

И.В. Баскаков, В.Л. Евсеев,
А.В. Пролетарский, А.М. Суровов

Защита информации в информационных системах

*Допущено Учебно-методическим объединением вузов
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших
учебных заведений, обучающихся по направлению
«Информатика и вычислительная техника»
и слушателей программ профессиональной переподготовки
и повышения квалификации специалистов
Российской Федерации и стран СНГ
по новым направлениям развития техники и технологии*

УДК 681.322.067
ББК 32.973-018.2
Б27



Издание осуществлено при поддержке
Межгосударственного фонда гуманитарного
сотрудничества государств-участников Содружества
Независимых Государств

Баскаков И.В., Евсеев В.Л., Пролетарский А.В., Суровов А.М.

Б27 Защита информации в информационных системах: Учебное пособие. М.: Изд-во «Рудомино», 2011. 362 с.

ISBN 978-5-905017-16-2

В учебном пособии освещаются вопросы защиты информации в информационных системах. Дается понятийный аппарат, анализируются и классифицируются возможные угрозы безопасности информации, излагаются математические основы криптографии, рассматриваются методы и средства защиты информации в информационных системах, раскрываются подходы к построению и эксплуатации систем защиты информации.

Содержание учебного пособия соответствует курсам лекций, читаемым авторами в МГТУ имени Н.Э.Баумана, а также в Межотраслевом институте повышения квалификации кадров (МИПК) по новым направлениям развития техники и технологии МГТУ им. Н.Э. Баумана.

Учебное пособие подготовлено в соответствии с учебными планами, утвержденными в МИПК МГТУ им. Н.Э. Баумана.

Для слушателей, студентов высших технических учебных заведений, специалистов в области информационных технологий и защиты информации, а также преподавателей, осуществляющих образовательную деятельность в сфере защиты информации.

Рецензенты: зав. кафедрой «Компьютерные системы и сети» МГТУ им. Н.Э.Баумана, д.т.н., проф. В.В.Сюзев; зав. кафедрой «Эксплуатация флота и АСУ водным транспортом» Московской академии водного транспорта, к.т.н., доцент, Ю.М.Миронов.

УДК 681.322.067
ББК 32.973-018.2

© МИПК МГТУ им. Н.Э. Баумана, 2011

© Баскаков И.В., Евсеев В.Л.,

Пролетарский А.В., Суровов А.М., 2011

ISBN 978-5-905017-16-2

СОДЕРЖАНИЕ

Список принятых сокращений.....	6
Введение.....	7
1. Основные понятия и положения защиты информации в информационных системах.....	9
1.1. Понятийный аппарат, предмет и объект защиты.....	9
1.2. Анализ угроз безопасности информации в информационных системах.....	18
1.2.1. Виды угроз.....	18
1.2.2. Случайные и преднамеренные искусственные угрозы.....	19
2. Теоретико-числовые методы в криптографии.....	29
2.1. Введение в теорию чисел.....	29
2.1.1. Простые и взаимно простые числа.....	29
2.1.2. Арифметика в классах вычетов.....	31
2.1.3. Теоремы Ферма и Эйлера	34
2.1.4. Проверка: является ли число простым.....	37
2.1.5. Алгоритм Евклида	38
2.1.6. Китайская теорема об остатках.....	39
2.1.7. Дискретные логарифмы.....	41
3. Методы и средства защиты информации в информационных системах.....	44
3.1. Правовые и организационные методы защиты информации в информационных системах.....	44
3.1.1. Правовое регулирование в области безопасности информации	44
3.1.2. Концептуальные документы в области защиты информации.....	47
3.1.3. Правонарушения и преступления в информационной сфере.....	59
3.1.4. Организационные меры по защите информации.....	60
3.2. Технические каналы утечки информации.....	61

3.2.1. Технические каналы утечки информации в информационных системах.....	61
3.2.2. Способы перехвата информации, передаваемой по каналам связи.....	78
3.3. Защита компьютерной информации от несанкционированного доступа.....	108
3.3.1. Компьютерная безопасность: современные требования, подходы.....	108
3.3.1.1. Введение.....	108
3.3.1.2. Основные требования к защите компьютерной информации и анализ защищенности современных операционных систем.....	109
3.3.1.3. Подходы к проектированию систем защиты компьютерной информации.....	135
3.3.2. Архитектурные принципы построения систем защиты информации.....	165
3.3.2.1. Системный подход в проектировании систем защиты.....	166
3.3.2.2. Архитектура системы защиты.....	172
3.3.2.3. Особенности архитектуры сетевой системы защиты.....	184
3.3.3. Авторизация, методы идентификации и авторизации пользователя.....	202
3.3.3.1. Авторизация.....	202
3.3.3.2. Парольная защита.....	208
3.3.3.3. Методы добавочных механизмов усиления парольной защиты.....	224
3.3.3.4. Сетевая авторизация.....	229
3.3.4. Управление доступом к ресурсам.....	231
3.3.4.1. Основные требования и задачи управления доступом.....	231
3.3.4.2. Механизм обеспечения замкнутости программной среды.....	243

3.3.4.3. Оценка влияния системы защиты на загрузку вычислительного ресурса информационной системы.....	249
3.3.4.4. Особенности реализации механизмов добавочной защиты.....	260
3.4. Криптографические методы защиты информации в информационных системах.....	263
3.4.1. Симметричное шифрование.....	263
3.4.2. Криптография с открытым ключом.....	300
3.4.3. Аутентификация.....	306
3.4.4. Электронные цифровые подписи.....	310
4. Построение и организация функционирования комплексных систем защиты информации в информационных системах.....	313
4.1. Построение систем защиты информации в информационных системах.....	313
4.1.1. Концепция и этапы создания защищенных информационных систем.....	313
4.1.2. Техническое задание на проектирование защищенной информационной системы.....	317
4.1.3. Моделирование, выбор показателей эффективности и критериев оптимальности защищенной информационной системы.....	321
4.1.4. Математическая постановка задачи разработки защищенной информационной системы.....	331
4.1.5. Оценка эффективности и создание организационной структуры системы защиты информации.....	332
4.2. Организация функционирования защищенной информационной системы.....	345
4.2.1. Применение защищенной информационной системы по назначению.....	345
4.2.2. Техническая эксплуатация защищенной информационной системы.....	355
Список литературы.....	358

Список принятых сокращений

АС - автоматизированная система
АСОД - автоматизированная система обработки данных
АСУ - автоматизированная система управления
ВЗУ - внешнее запоминающее устройство
ВС - вычислительная система
ВСт - вычислительная сеть
ИС – информационная система
ЗИ – защита информации
ЗУ - запоминающее устройство
КМ - коммуникационный модуль
КПП - контрольно-пропускной пункт
КС - компьютерная система
КСЗИ - комплексная система защиты информации
ЛВС - локальная вычислительная сеть
НИС - несанкционированное изменение структур
НСДИ - несанкционированный доступ к информации
ОБИ - обеспечение безопасности информации
ООП - объектно-ориентированное программирование
ОП - оперативная память
ОС - операционная система
ПЗУ - постоянное запоминающее устройство
ПЦ - процессор
ПЭМИН - побочные электромагнитные излучения и наводки
РКС - распределенная компьютерная система
СВЧ - сверхвысокая частота
СВТ - средства вычислительной техники
СЗИ - система защиты информации
СЗИК - система защиты от излучения и копирования
СКВУ - система контроля вскрытия устройств
СОО - система охраны объекта
СПД - система передачи данных
СРД - система разграничения доступа
СУБД - система управления базой данных
ТС - техническое средство
ТСВ - телевизионная система видеоконтроля
УОКВ - устройство обработки и коммутации видеoinформации
УРИ - устройство регистрации информации
ЭВТ - электронно-вычислительная техника

ВВЕДЕНИЕ

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Хотя, если уж быть точным, новые проблемы - это всего лишь обновленная форма старых. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий в первой половине 21 века, сделали проблему защиты информации настолько актуальной и острой. Насколько актуальна сегодня информатизация для всего общества. Главная тенденция, характеризующая развитие современных информационных технологий - рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь. По результатам одного исследования, посвященного вопросам компьютерных преступлений, около 58% опрошенных пострадали от компьютерных взломов в течение года. Свыше 22% атак были нацелены на промышленные секреты или документы, представляющие интерес прежде всего для конкурентов. Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированным доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Однако по данным, опубликованным в сети Internet, общие потери от несанкционированного доступа к информации в компьютерных системах в 2009 году оценивались в 400 миллионов долларов. Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются:

переход от традиционной «бумажной» технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Любое современное предприятие независимо от вида деятельности и формы собственности не в состоянии успешно развиваться и вести хозяйственную деятельность без создания на нем условий для надежного функционирования системы защиты собственной информации. Отсутствие у многих руководителей предприятий и компаний четкого представления по вопросам защиты информации приводит к тому, что им сложно в полной мере оценить необходимость создания надежной системы защиты информации на своем предприятии и тем более сложно бывает определить конкретные действия, необходимые для защиты тех или иных конфиденциальных сведений. В общем случае руководители предприятий идут по пути создания охранных служб, полностью игнорируя при этом вопросы информационной безопасности. Отрицательную роль при этом играют и некоторые средства массовой информации, публикуя «панические» статьи о состоянии дел по защите информации, формирующие у читателей представление о невозможности в современных условиях обеспечить требуемый уровень защиты информации.

Роль различных технических и организационных мер по охране и защите информации весьма велика и по некоторым оценкам составляет от 75 до 80% от всех проводимых защитных мероприятий.

Ориентировочно весь объем мероприятий (в денежном исчислении) по охране и защите информации можно разделить в следующем соотношении:

1. Правовые меры (законы, ведомственные акты, инструкции) - 5%;
2. Физические меры (ограда по периметру, службы охраны, разграничение полномочий и др.) - (15...20)%;
3. Технические меры (различные технические и программные средства защиты) - (25...30)%;
4. Организационные меры (разработка политики в области безопасности, процедур ее внедрения, кадровая политика, обучение персонала, контроль и др.) - 50%.

Можно с уверенностью утверждать, что создание эффективной системы защиты информации сегодня вполне реально. Надежность защиты информации, прежде всего, будет определяться полнотой решения целого комплекса задач, речь о которых будет продолжена дальше.

1. ОСНОВНЫЕ ПОНЯТИЯ И ПОЛОЖЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1.1. Понятийный аппарат, предмет и объект защиты

В Федеральном законе РФ «Об информации, информационных технологиях и о защите информации», принятом 27 июля 2006 года [8], даны основные понятия:

информация – сведения (сообщения, данные), независимо от формы их представления;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть – техническая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации – лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора разрешать или ограничивать доступ к информации, определяемой по каким-то признакам;

доступ к информации – возможность получения информации и ее использования;

конфиденциальная информация – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация – зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель;

оператор информационной системы – гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Информация имеет ряд особенностей [5]:

- ♦ она нематериальна;
- ♦ информация хранится и передается с помощью материальных носителей;
- ♦ любой материальный объект содержит информацию о самом себе или о другом объекте.

Нематериальность информации понимается в том смысле, что нельзя измерить ее параметры известными физическими методами и приборами. Информация не имеет массы, энергии и т. п.

Информация хранится и передается на материальных носителях. Такими носителями являются мозг человека, звуковые и электромагнитные волны, бумага, машинные носители (магнитные и оптические диски, магнитные ленты и барабаны) и др.

Информации присущи следующие свойства [5].

1. *Информация доступна человеку, если она содержится на материальном носителе.* Поэтому необходимо защищать материальные носители информации, так как с помощью материальных средств можно защищать только материальные объекты.

2. *Информация имеет ценность.* Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной или достоверной информацией является информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках.

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют *дезинформацией*.

Законом «Об информации, информационных технологиях и о защите информации» гарантируется право обладателя информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничивается, то такая информация является *конфиденциальной*. Конфиденциальная информация может содержать государственную или коммерческую тайну. *Коммерческую тайну* могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. *Государственную тайну* могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней секретности. В порядке возрастания ценности (важности) информации ей может быть присвоена степень (гриф) «*секретно*», «*совершенно секретно*» или «*особой важности*». В государственных учреждениях менее важной информации может присваиваться гриф «*для служебного пользования*».

Для обозначения ценности конфиденциальной коммерческой информации используются три категории:

- ♦ «коммерческая тайна - строго конфиденциально»;
- ♦ «коммерческая тайна - конфиденциально»;
- ♦ «коммерческая тайна».

Используется и другой подход к градации ценности коммерческой информации:

- ♦ «строго конфиденциально - строгий учет»;
- ♦ «строго конфиденциально»;
- ♦ «конфиденциально».

3 Ценность информации изменяется во времени.

Как правило, со временем ценность информации уменьшается. Зависимость ценности информации от времени приближенно определяется в соответствии с выражением:

$$C(t) = C_0 e^{-2,3t/\tau}, \quad (1.1)$$

где C_0 - ценность информации в момент ее возникновения (получения);

t - время от момента возникновения информации до момента определения ее стоимости;

τ - время от момента возникновения информации до момента ее устаревания.

Время, через которое информация становится устаревшей, меняется в очень широком диапазоне. Так, например, для пилотов

реактивных самолетов, автогонщиков информация о положении машин в пространстве устаревает за доли секунд. В то же время информация о законах природы остается актуальной в течение многих веков.

4. Информация покупается и продается.

Ее правомочно рассматривать как товар, имеющий определенную цену. Цена, как и ценность информации, связаны с полезностью информации для конкретных людей, организаций, государств. Информация может быть ценной для ее владельца, но бесполезной для других. В этом случае информация не может быть товаром, а, следовательно, она не имеет и цены. Например, сведения о состоянии здоровья обычного гражданина являются ценной информацией для него. Но эта информация, скорее всего, не интересует кого-то другого, а, следовательно, не станет товаром, и не будет иметь цены.

Информация может быть получена тремя путями:

- ◆ проведением научных исследований;
- ◆ покупкой информации;
- ◆ противоправным добыванием информации.

Как любой товар, информация имеет себестоимость, которая определяется затратами на ее получение. Себестоимость зависит от выбора путей получения информации и минимизации затрат при добывании необходимых сведений выбранным путем. Информация добывается с целью получения прибыли или преимуществ перед конкурентами, противоборствующими сторонами. Для этого информация:

- ◆ продается на рынке;
- ◆ внедряется в производство для получения новых технологий и товаров, приносящих прибыль;
- ◆ используется в научных исследованиях;
- ◆ позволяет принимать оптимальные решения в управлении.

5. Сложность объективной оценки количества информации.

Существует несколько подходов к измерению количества информации.

а) Энтропийный подход.

В теории информации количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество информации тем больше, чем ниже вероятность события. Энтропийный подход широко используется при определении

количества информации, передаваемой по каналам связи. Выбор при приеме информации осуществляется между символами алфавита в принятом сообщении. Пусть сообщение, принятое по каналу связи, состоит из N символов (без учета связи между символами в сообщении). Тогда количество информации в сообщении может быть подсчитано по формуле Шеннона [14]:

$$I = N \sum_{i=1}^k P_i \log_2 P_i, \quad (1.2)$$

где P_i - вероятность появления в сообщении символа i ;
 k - количество символов в алфавите языка.

Анализ формулы Шеннона показывает, что количество информации в двоичном представлении (в битах или байтах) зависит от двух величин: количества символов в сообщении и частоты появления того или иного символа в сообщениях для используемого алфавита. Этот подход абсолютно не отражает насколько полезна полученная информация, а позволяет определить лишь затраты на передачу сообщения.

б) Тезаурусный подход.

Этот подход предложен Ю.А. Шрейдером [15]. Он основан на рассмотрении информации как знаний. Согласно этому подходу количество информации, извлекаемое человеком из сообщения, можно оценить степенью изменения его знаний. Структурированные знания, представленные в виде понятий и отношений между ними, называются тезаурусом. Структура тезауруса иерархическая. Понятия и отношения, группируясь, образуют другие, более сложные понятия и отношения.

Знания отдельного человека, организации, государства образуют соответствующие тезаурусы. Тезаурусы организационных структур образуют тезаурусы составляющих их элементов. Так тезаурус организации образуют, прежде всего, тезаурусы сотрудников, а также других носителей информации, таких как документы, оборудование, продукция и т. д.

Для передачи знаний требуется, чтобы тезаурусы передающего и принимающего элемента пересекались. В противном случае владельцы тезаурусов не поймут друг друга.

Тезаурусы человека и любых организационных структур являются их капиталом. Поэтому владельцы тезаурусов стремятся сохранить и увеличить свой тезаурус. Увеличение тезауруса осуществляется за счет обучения, покупки лицензии, приглашения квалифицированных сотрудников или хищения информации.

В обществе наблюдаются две тенденции: развитие тезаурусов отдельных элементов (людей, организованных структур) и выравнивание тезаурусов элементов общества.

Выравнивание тезаурусов происходит как в результате целенаправленной деятельности (например, обучения), так и стихийно. Стихийное выравнивание тезаурусов происходит за счет случайной передачи знаний, в том числе и незаконной передачи.

в) Практический подход.

На практике количество информации измеряют, используя понятие «объем информации». При этом количество информации может измеряться в количестве бит (байт), в количестве страниц текста, длине магнитной ленты с видео- или аудиозаписью и т.п. Однако очевидно, что на одной странице информации может содержаться больше или меньше, по крайней мере, по двум причинам. Во-первых, разные люди могут разместить на странице различное количество сведений об одном и том же объекте, процессе или явлении материального мира. Во-вторых, разные люди могут извлечь из одного и того же текста различное количество полезной, понятной для них информации. Даже один и тот же человек в разные годы жизни получает разное количество информации при чтении книги.

В результате копирования без изменения информационных параметров носителя количество информации не изменяется, а цена снижается. Примером копирования без изменения информационных параметров может служить копирование текста с использованием качественных копируемых устройств. Текст копии, при отсутствии сбоев копируемого устройства, будет содержать точно такую же информацию, как и текст оригинала. Но при копировании изображений уже не удастся избежать искажений. Они могут быть только большими или меньшими.

В соответствии с законами рынка, чем больше товара появляется, тем он дешевле. Этот закон полностью справедлив и в отношении копий информации. Действие этого закона можно проследить на примере пиратского распространения программных продуктов, видеопродукции и т. п.

В качестве предмета защиты рассматривается информация, хранящаяся, обрабатываемая и передаваемая в информационных системах. Особенности этой информации являются:

♦ двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;

♦ высокая степень автоматизации обработки и передачи информации;

♦ концентрация большого количества информации в ИС.

Объектом защиты информации является информационная система или автоматизированная система обработки данных (АСОД). В работах, посвященных защите информации в автоматизированных системах, до последнего времени использовался термин АСОД, который все чаще заменяется термином ИС. Что же понимается под этим термином?

Информационная система – совокупность содержащейся в базах данных информации, технологий её обработки и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [8].

Понятие ИС очень широкое и оно охватывает следующие системы:

♦ ЭВМ всех классов и назначений;

♦ вычислительные комплексы и системы;

♦ вычислительные сети (локальные, региональные и глобальные).

Такой широкий диапазон систем объединяется одним понятием по двум причинам: во-первых, для всех этих систем основные проблемы защиты информации являются общими; во-вторых, более мелкие системы являются элементами более крупных систем. Если защита информации в каких-либо системах имеет свои особенности, то они рассматриваются отдельно.

Предметом защиты в ИС является информация. Материальной основой существования информации в ИС являются электронные и электромеханические устройства (подсистемы), а также машинные носители. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в ИС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ) и выводится из системы с помощью устройств вывода или СПД. В качестве машинных носителей используются - бумага, магнитные ленты, диски

различных типов. Ранее в качестве машинных носителей информации использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов машинных носителей информации являются съёмными, т.е. могут сниматься с устройств и использоваться (бумага) или храниться (ленты, диски, бумага) отдельно от устройств.

Таким образом, для защиты информации (обеспечения безопасности информации) в ИС необходимо защищать устройства (подсистемы) и машинные носители от несанкционированных (неразрешенных) воздействий на них.

Однако такое рассмотрение ИС с точки зрения защиты информации является неполным. Компьютерные системы относятся к классу человеко-машинных систем. Такие системы эксплуатируются специалистами (обслуживающим персоналом) в интересах пользователей. Причем, в последние годы пользователи имеют самый непосредственный доступ к системе. В некоторых ИС (например, ПЭВМ) пользователи выполняют функции обслуживающего персонала. Обслуживающий персонал и пользователи являются также носителями информации. Поэтому от несанкционированных воздействий необходимо защищать не только устройства и носители, но также обслуживающий персонал и пользователей.

При решении проблемы защиты информации в ИС необходимо учитывать также противоречивость человеческого фактора системы. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Понятие «*объект защиты*» или «*объект*» чаще трактуется в более широком смысле. Для сосредоточенных ИС или элементов распределенных систем понятие «объект» включает в себя не только информационные ресурсы, аппаратные, программные средства, обслуживающий персонал, пользователей, но и помещения, здания, и даже прилегающую к зданиям территорию.

Одними из основных понятий теории защиты информации являются понятия «безопасность информации» и «защищенные ИС». *Безопасность (защищенность) информации в ИС* - это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Информационные системы, в которых обеспечивается безопасность информации, называются

защищенными. Защита информации [8] представляет собой принятие правовых, организационных и технических мер, направленных на:

1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2. Соблюдение конфиденциальности информации ограниченного доступа;

3. Реализацию права на доступ к информации.

Безопасность информации в ИС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня *политики информационной безопасности*. Основным документом, на основе которого проводится политика информационной безопасности, является *программа информационной безопасности*. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в ИС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в ИС.

Под *системой защиты информации в ИС* понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

1.2. Анализ угроз безопасности информации в информационных системах

1.2.1. Виды угроз

С позиции обеспечения безопасности информации в ИС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

- ♦ информация;
- ♦ технические и программные средства;
- ♦ обслуживающий персонал и пользователи.

Целью создания любой ИС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным «продуктом потребления» в ИС и выступает в виде центральной компоненты системы. Безопасность информации на уровне ИС обеспечивают две другие компоненты системы. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий.

Особенности взаимодействия компонент заключаются в следующем:

Внешние воздействия чаще всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы;

Возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего персонала и пользователей.

В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в ИС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз).

Под *угрозой безопасности информации* понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

1.2.2. Случайные и преднамеренные искусственные угрозы

Все множество потенциальных угроз безопасности информации в ИС может быть разделено на два класса (рис 1.1).



Рис. 1.1. Угрозы безопасности информации в компьютерных системах

Случайные угрозы.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют *случайными* или *непреднамеренными*.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам ИС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние

подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке ИС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы ИС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) до 65% случаев нарушения безопасности информации происходит в результате *ошибок пользователей и обслуживающего персонала*. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в ИС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации ИС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Преднамеренные угрозы.

Второй класс угроз безопасности информации в ИС составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- ◆ традиционный или универсальный шпионаж и диверсии;
- ◆ несанкционированный доступ к информации;
- ◆ электромагнитные излучения и наводки;
- ◆ модификация структур ИС;
- ◆ вредительские программы.

Традиционный шпионаж и диверсии. В качестве источников нежелательного воздействия на информацию по-прежнему актуальны *методы и средства шпионажа и диверсий*, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих ИС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в ИС, а также для хищения и уничтожения информации.

К методам шпионажа и диверсий относятся:

- ◆ подслушивание;
- ◆ визуальное наблюдение;
- ◆ хищение документов и машинных носителей информации;
- ◆ хищение программ и атрибутов системы защиты;
- ◆ подкуп и шантаж сотрудников;
- ◆ сбор и анализ отходов машинных носителей информации;
- ◆ поджоги;
- ◆ взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами [12]. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное

расстояние подслушивания с помощью направленных микрофонов составляет от 50 до 100 метров[12].

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен от 50 до 100 см [12]. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал, может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации, может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в ИС малопригодна и носит, как правило, вспомогательный характер. Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из ИС

информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г) [5].

Для вербовки сотрудников и физического уничтожения объектов ИС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект ИС, может использовать любой из методов традиционного шпионажа. Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео- и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов ИС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий признак - излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде

радиосигнала на дальность до 8 км [5]. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний от 50 до 800 метров.

Для некоторых объектов ИС существует *угроза вооруженного нападения террористических или диверсионных групп*. При этом могут быть применены средства огневого поражения.

Несанкционированный доступ к информации. Термин «несанкционированный доступ к информации» (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем [7].

Под правилами разграничения доступа (ПРД) понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам ИС определяется руководством организации для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы иницируются в ИС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в ИС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- ♦ отсутствует система разграничения доступа;
- ♦ сбой или отказ в ИС;
- ♦ ошибочные действия пользователей или обслуживающего персонала компьютерных систем;
- ♦ ошибки в СРД;
- ♦ фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в ИС, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств ИС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

Электромагнитные излучения и наводки. Процесс обработки и передачи информации техническими средствами ИС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок*. С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в ИС присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км [5]. Восстановление данных возможно также путем анализа сигналов излучения незранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств ИС.

«Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки ИС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

Несанкционированная модификация структур. Большую угрозу безопасности информации в ИС представляет *несанкционированная модификация алгоритмической, программной и технической структур системы.* Несанкционированная модификация структур может осуществляться на любом жизненном цикле ИС. Несанкционированное изменение структуры ИС на этапах разработки и модернизации получило название «закладка». В процессе разработки ИС «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные ИС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки ИС во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных ИС.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на ИС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на ИС осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т.д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название «люки».

Вредительские программы. Одним из основных источников угроз безопасности информации в ИС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- ◆ «логические бомбы»;
- ◆ «черви»;
- ◆ «троянские кони»;
- ◆ «компьютерные вирусы».

«Логические бомбы» - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход ИС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони» - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы» - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к ИС. Злоумышленником может быть:

- ◆ разработчик ИС;
- ◆ сотрудник из числа обслуживающего персонала;
- ◆ пользователь;

♦ постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных средствах ИС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты ИС. Пользователь имеет общее представление о структурах ИС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения «закладок* пользователями очень ограничены. Постороннее лицо, не имеющее отношения к ИС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект ИС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если ИС является распределенной.

Большие возможности оказания вредительских воздействий на информацию ИС имеют *специалисты, обслуживающие эти системы*. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

2. ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

2.1. Введение в теорию чисел

Для разработки алгоритмов шифрования с открытым ключом используется целый ряд понятий теории чисел. Понятия и методы теории чисел являются совершенно абстрактными, и их часто трудно понять интуитивно без использования примеров. Поэтому надо приводить примеры.

2.1.1. Простые и взаимно простые числа

Делители.

Главным объектом теории чисел являются простые числа. Говорят, что b , отличное от нуля, делит a , если $a = m \cdot b$ для некоторого m , где a , b и m являются целыми числами. Таким образом, b делит a , то есть b/a . Если b/a , то b называют делителем a (например, положительными делителями числа 24 являются числа: 1, 2, 3, 4, 6, 8, 12, 24).

Имеют место следующие соотношения:

- если $a / 1$, то $a = \pm 1$;
- если b/a и a/b , то $a = \pm b$;
- любое b , отличное от нуля, делит 0;
- если b/g и b/h , то $b/(mg+nh)$ для произвольных целых m и n .

Чтобы убедиться в истинности последнего утверждения, надо обратить внимание на следующее:

- если b/g , то g имеет вид $g = b \cdot g_1$, для некоторого целого g_1 ;
- если b/h , то h имеет вид $h = b \cdot h_1$, для некоторого целого h_1 .

Поэтому $mg+nh = m \cdot b \cdot g_1 + n \cdot b \cdot h_1 = b \cdot (m \cdot g_1 + n \cdot h_1)$, следовательно, b делит $mg+nh$ (например, $b = 7$, $g = 14$, $h = 63$, $m = 3$, $n = 2$, $7/14$, $7/63$. Требуется доказать, что $7/(3 \cdot 14 + 2 \cdot 63)$. Имеем $3 \cdot 14 + 2 \cdot 63 = 7 \cdot (3 \cdot 2 + 2 \cdot 9)$. Тогда очевидно, что $7(3 \cdot 14 + 2 \cdot 63)$).

Простые числа.

Целое число $p > 1$ называется простым, если его делителями являются только числа ± 1 и $\pm p$. Простые числа играют основную роль в теории чисел и в ее методах.

Любое целое число $a > 1$ может быть разложено на множители и единственным способом представлено в виде $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_i^{a_i}$, где $p_1 < p_2 < \dots < p_i$ являются простыми числами, и где каждое $a_i > 0$ (например, $91 = 7 \cdot 13$, $11011 = 7 \cdot 112 \cdot 13$).

В теории простых чисел полезно следующее немного отличное от приведенного выше представление числа. Если P обозначает множество всех простых чисел, то любое положительное целое число может быть единственным способом записано в форме $a = \prod_p p^{a_p}$, где все $a_p \geq 0$. В этой формуле выражение справа от знака равенства означает произведение по всем возможным простым числам p . Для каждого конкретного значения a большинство значений показателя a_p будет равно 0 (например, $3600 = 2^4 \cdot 3^2 \cdot 5^2$).

Значение любого положительного целого числа может быть однозначно задано простым перечислением всех ненулевых показателей в предыдущей формуле (например, целое число 12 можно представить как $(a_2 = 2, a_3 = 1)$).

Умножение двух чисел эквивалентно сложению значений соответствующих показателей: $k = mn$, отсюда $k_p = m_p + n_p$ для всех p (например, $k = 12 \cdot 18 = 216$, $k_2 = 2 + 1 = 3$, $k_3 = 1 + 2 = 3$, $216 = 2^3 \cdot 3^3$).

Что же тогда означает a / b ? Любое целое число вида p^k может делиться только на целое число, которое является степенью того же простого числа p с показателем, не превышающим k , то есть на p^j , где $j \leq k$. Таким образом, a / b это есть $a_p \leq b_p$ для всех p (например, $a = 12$, $b = 36$, тогда $12/36$, $12 = 2^2 \cdot 3$, $36 = 2^2 \cdot 3^2$, $a_2 = 2$, $b_2 = 2$, $a_3 = 1 \leq 2 = b_3$).

Взаимно простые числа.

Пусть НОД (a , b) – это наибольший общий делитель чисел a и b . Говорят, что положительное целое число c является наибольшим общим делителем чисел a и b , если:

1. c - является делителем a и b ;
2. Любой делитель a и b является делителем c .

Эквивалентным этому оказывается определение:

$$\text{НОД}(a, b) = \max \{k \text{ таких, что } k/a \text{ и } k/b\}.$$

Поскольку требуется, чтобы НОД был положительным, то имеем: $\text{НОД}(a, b) = \text{НОД}(a, -b) = \text{НОД}(-a, b) = \text{НОД}(-a, -b)$. Вообще $\text{НОД}(a, b) = \text{НОД}(|a|, |b|)$ (например, $\text{НОД}(60, 24) = \text{НОД}(60, -24) = 12$).

А поскольку все ненулевые целые числа делят 0, имеем $\text{НОД}(a, 0) = |a|$.

Легко определить НОД двух положительных целых чисел, если эти числа представлены в виде произведения простых множителей (например, $300 = 2^2 \cdot 3^1 \cdot 5^2$, $18 = 2^1 \cdot 3^2$, тогда $\text{НОД}(18, 300) = 2^1 \cdot 3^1 \cdot 5^0$).

В общем случае: $k = \text{НОД}(a, b) \longrightarrow k_p = \min(a_p, b_p)$ для

всех p .

Определение простых множителей больших чисел является непростой задачей, так что представленное выше соотношение не дает непосредственной практической возможности вычислить НОД двух чисел (для этого служит алгоритм Евклида).

Целые числа a и b являются взаимно простыми, если они не имеют общих простых делителей, то есть если их единственным общим делителем является 1. Другими словами, a и b являются взаимно простыми, если $\text{НОД}(a, b) = 1$ (например, числа 8 и 15 являются взаимно простыми, так как делителями числа 8 являются 1, 2, 4, и 8, а делителями числа 15 – являются 1, 3, 5, и 15, поэтому 1 оказывается единственным числом, присутствующим в обоих списках).

2.1.2. Арифметика в классах вычетов

Для любого положительного целого числа n и любого целого a при делении a на n получаем некоторое частное q и остаток r , удовлетворяющие соотношению $a = qn + r$, $0 \leq r < n$; $q = \lfloor a/n \rfloor$, где $\lfloor x \rfloor$ обозначает наибольшее целое число, не превышающее x . Для заданного a и положительного n всегда можно найти q и r , удовлетворяющие вышеприведенному соотношению. В представлении целых чисел на числовой a , оказывается некоторой точки на этой оси (рассмотрим для положительного a). Начиная от значения 0, рассматриваются значения n , $2n$ и так далее вплоть до такого qn , что $qn \leq a$ и $(q+1)n > a$. Пусть расстояние от qn до a равно r , и, таким образом, уникальные значения q и r оказываются найденными. Остаток r часто называют *вычетом* (например, $a=11$; $n=7$; $11=1 \cdot 7+4$, тогда $r=4$).

Если a является целым, а n – положительным целым, то $a \bmod n$ определяется как остаток от деления a на n . Таким образом, для любого целого числа a можно записать $a = \lfloor a/n \rfloor \cdot n + (a \bmod n)$. (например, $11 \bmod 7 = 4$, $-11 \bmod 7 = 3$).

Говорят, что два целых числа a и b являются *сравнимыми* по модулю n , если $(a \bmod n) = (b \bmod n)$. Что записывается в таком виде $a \equiv b \bmod n$ (например, $73 \equiv 4 \bmod 23$ и $21 \equiv -9 \bmod 10$).

Следует обратить внимание на то, что если $a \equiv 0 \bmod n$, то n/a .

Свойства операции сравнения по модулю:

1. $a \equiv b \bmod n$, когда $n/(a - b)$;

2. Из $(a \bmod n) = (b \bmod n)$ следует $a \equiv b \bmod n$;
3. Из $a \bmod n$ следует $b \equiv a \bmod n$;
4. Из $a \equiv b \bmod n$ и $b \equiv c \bmod n$ следует $a \equiv c \bmod n$.

Эти свойства доказываются легко, например, первое: из соотношения $n/(a - b)$ следует, что $(a - b) = kn$ для некоторого k . Поэтому $a = b + kn$. Таким образом, $(a \bmod n) = (\text{остаток от деления } (b + kn) \text{ на } n) = (\text{остаток от деления } b \text{ на } n) = (b \bmod n)$.

Операции арифметики в классах вычетов.

По определению (п.2.1.1), при сравнении по модулю n множество всех целых чисел отображается во множество $\{0, 1, \dots, (n-1)\}$. При этом возникает вопрос: можно ли определить арифметические операции в рамках данного множества? Оказывается, можно, и соответствующий набор операций называется арифметикой в классах вычетов. Операции арифметики в классах вычетов обладают следующими свойствами:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$;
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$;
3. $[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$.

Свойства доказываются легко, например, первое: Пусть $(a \bmod n) = r_a$, и $(b \bmod n) = r_b$. Тогда $a = r_a + jn$ для некоторого целого числа j и $b = r_b + kn$ для некоторого целого числа k . Поэтому $(a + b) \bmod n = (r_a + jn + r_b + kn) \bmod n = (r_a + r_b + (j + k)n) \bmod n = (r_a + r_b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$. (Например, пусть $11 \bmod 8 = 3$, $15 \bmod 8 = 7$, тогда $[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$).

Возведение в степень выполняется с помощью повторного умножения, как и в обычной арифметике. (Например, найти $11^7 \bmod 13$. Будем действовать так: $11^2 = 121 \equiv 4 \bmod 13$, $11^4 \equiv 4^2 \equiv 3 \bmod 13$, $11^7 \equiv 11 \cdot 4 \cdot 3 \equiv 132 \equiv 2 \bmod 13$).

Таким образом, правила выполнения обычных арифметических операций – сложения, вычитания и умножения – можно применять и в арифметике классов вычетов.

Свойства арифметики в классах вычетов.

Пусть Z_n обозначает множество всех неотрицательных целых чисел, которые меньше n : $Z_n = \{0, 1, \dots, (n-1)\}$.

Это множество называют еще множеством вычетов (остатков) по модулю n . Для арифметических операций по модулю n в этом множестве выполняются следующие свойства:

1. Коммутативные законы:

$$(w + x) \bmod n = (x + w) \bmod n;$$

$$(w \cdot x) \bmod n = (x \cdot w) \bmod n.$$

2. Ассоциативные законы:

$$[(w + x) + y] \bmod n = [(w + (x + y))] \bmod n;$$

$$[(w \cdot x) \cdot y] \bmod n = [(w \cdot (x \cdot y))] \bmod n.$$

3. Дистрибутивный закон:

$$[(w \cdot x) \cdot y] \bmod n = [(w \cdot x) \cdot (x \cdot y)] \bmod n.$$

4. Тожества:

$$(0 + w) \bmod n = w \bmod n;$$

$$(1 \cdot w) \bmod n = w \bmod n.$$

5. Аддитивный обратный $(-w)$:

Для любого $w \in Z_n$, существует такое z , что:

$$w + z \equiv 0 \bmod n.$$

Существует одна особенность арифметики в классах вычетов, которая делает ее отличной от обычной арифметики. Следует отметить, что, как и в обычной арифметике, имеет место следующее свойство:

$$\text{если } (a + b) \equiv (a + c) \bmod n, \text{ то } b \equiv c \bmod n \quad (2.1)$$

(например, $(5 + 23) \equiv (5 + 7) \bmod 8$, $23 \equiv 7 \bmod 8$).

Свойство (2.1) согласуется с существованием аддитивного обратного. Прибавив к обеим частям равенства (2.1) аддитивное обратное элемента a , получаем выражение:

$$((-a) + a + b) \equiv ((-a) + a + c) \bmod n \text{ и тогда } b \equiv c \bmod n.$$

Однако, следующее утверждение выполняется только при указанном условии:

$$\text{если } (a \cdot b) \equiv (a \cdot c) \bmod n, \text{ то } b \equiv c \bmod n \quad (2.2)$$

при условии, что a и n взаимно просты.

(Например, когда данное условие выполнено: $6 \cdot 3 = 18 \equiv 2 \bmod 8$, и $6 \cdot 7 = 42 \equiv 2 \bmod 8$. Однако $3 \not\equiv 7 \bmod 8$).

Причиной такого странного результата является то, что для произвольного модуля сравнения n в результате умножения чисел от 0 до $(n - 1)$ на множитель a не получается полного набора всех вычетов, когда a и n имеют общие множители.

Наконец, отметим, что если p является простым, то все элементы Z_p будут взаимно простыми с p . Это дает нам возможность добавить еще одно свойство к тем, которые были приведены выше:

Мультипликативный обратный (w^{-1}): для любого $w \in Z_p$ существует такое z , что $w \cdot z \equiv 1 \bmod p$.

В связи с тем, что w и p являются простыми, при умножении каждого элемента Z_p на w будет получен набор всех элементов множества Z_p в несколько измененном порядке. Поэтому, по крайней мере, один из остатков будет иметь значение 1. Таким образом, найдется некоторое число в Z_p , при умножении которого на w получается значение 1. Это число и будет мультипликативным обратным для w , обозначаемым w^{-1} . Итак, свойство (2.2) согласуется с существованием мультипликативного обратного. Умножая обе части равенства (2.2) на мультипликативное обратное значения a , получаем $((a^{-1}) \cdot a \cdot b) \equiv ((a^{-1}) \cdot a \cdot c) \pmod n$, $b \equiv c \pmod n$.

Тогда, следует окончательное заключение: некоторые (но не все) целые числа будут иметь мультипликативные обратные, даже если модуль сравнения не является простым числом. В частности, если НОД $(a, n) = 1$, можно найти такое значение b в Z_n , что $a \cdot b \equiv 1 \pmod n$. Аргументацию здесь можно привести ту же, что и в п.2.1.2. Поскольку a и n являются взаимно простыми, при умножении всех элементов Z_n на a , результирующее множество остатков будет включать все элементы Z_n в другом порядке. Поэтому и найдется некоторое такое значение b в Z_n , что $a \cdot b \equiv 1 \pmod n$.

2.1.3. Теоремы Ферма и Эйлера

Теоремы Ферма и Эйлера играют очень важную роль в криптографии с открытым ключом.

Теорем Ферма.

Теорема Ферма: если p является простым и a является положительным целым числом, которое не делится p , то

$$a^{p-1} \equiv 1 \pmod p. \quad (2.3)$$

Доказательство. Нам известно (ранее), что если все элементы Z_p умножить на a по модулю p , то в результате получаются все элементы Z_p в некоторой перестановке. Кроме того, $a \cdot 0 \equiv 1 \pmod p$. Поэтому набор $(p - 1)$ чисел $\{a \pmod p, 2a \pmod p, \dots, (p - 1) \pmod p\}$ представляет собой тот же набор чисел $\{1, 2, \dots, (p - 1)\}$ в ином порядке. Перемножим все эти числа: $a \cdot 2a \cdot \dots \cdot ((p - 1) a) \equiv [(a \pmod p) \cdot (2a \pmod p) \cdot \dots \cdot ((p - 1) a \pmod p)] \pmod p \equiv (p - 1)! \pmod p$.

Но $a \cdot 2a \cdot \dots \cdot ((p - 1) a) = (p - 1)! a^{p-1}$, поэтому $(p - 1)! a^{p-1} \equiv (p - 1)! \pmod p$. Здесь можно сократить на $(p - 1)!$,

поскольку это значение и p являются взаимно простыми (см. (2.2)). Отсюда вытекает формула (2.3). (Например, $a = 7$, $p = 19$, $7^2 = 49 \equiv 11 \pmod{19}$, $7^4 \equiv 121 \equiv 7 \pmod{19}$, $7^8 - 49 \equiv 11 \pmod{19}$, $7^{16} \equiv 121 \equiv 7 \pmod{19}$, $a^{p-1} = 7^{18} = 7^{16} \cdot 7^2 \equiv 7 \cdot 11 \equiv 1 \pmod{19}$).

Альтернативная формулировка теоремы тоже может оказаться полезной: если p является простым и a является положительным целым числом, то

$$a^p \equiv a \pmod{p} \quad (2.4)$$

(например, $p = 5$, $a = 3$, $3^5 = 243 \equiv 3 \pmod{5}$).

Функция Эйлера.

Прежде чем представить теорему Эйлера, необходимо определить одну важную функцию, именуемую в теории чисел и называемую функцией Эйлера. Она обозначается символом $\phi(n)$ и представляет собой число положительных целых значений, которые меньше n и являются взаимно простыми с n .

Ясно, что для простого p : $\phi(p) = p - 1$.

Предположим, что имеется два простых числа p и q . Тогда для $n = p \cdot q$ получаем $\phi(n) = \phi(pq) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1)$.

Чтобы увидеть это, рассмотрим множество значений Z_n , представляющее собой $\{0, 1, \dots, (pq - 1)\}$. Значениями, не являющимися взаимно простыми с n , будут значения множества $\{p, 2p, \dots, (q-1)p\}$ и $\{q, 2q, \dots, (p-1)q\}$, а также 0. Соответственно имеем: $\phi(n) = pq - [(q-1) + (p-1) + 1] = pq - (p+q) + 1 = (p-1) \cdot (q-1) = \phi(p) \cdot \phi(q)$.

(Например, $\phi(21) = 12 = \phi(3) \cdot \phi(7) = 2 \cdot 6 = (3-1) \cdot (7-1)$, и эти 12 целых чисел образуют множество $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$).

Теорема Эйлера.

Теорема Эйлера утверждает, что для любых взаимно простых чисел a и n :

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (2.5)$$

(например, $a = 3$, $n = 10$, $\phi(10) = 4$, $3^4 = 81 \equiv 1 \pmod{10}$).

Доказательство. Равенство (2.5) верно, если n является простым, так как в таком случае $\phi(n) = (n - 1)$ и выполняется теорема Ферма. Однако, то же самое равенство выполняется и для целого числа n вообще. Напомним, что $\phi(n)$ равно числу положительных целых значений, меньших n и взаимно простых с n . Рассмотрим множество таких целых чисел, пронумеровав их так: $R = \{x_1, x_2, \dots$

$x_{\varphi(n)}\}$. Теперь умножим каждый элемент этого множества на a по модулю n . $S = \{(ax_1 \bmod n), (ax_2 \bmod n), \dots, (ax_{\varphi(n)} \bmod n)\}$.

Приведенное выше множество представляет перестановку элементов множества R по следующим причинам:

1. Поскольку a , как и x_1 , является взаимно простым с n , ax_i тоже должно быть взаимно простым с n . Таким образом, все элементы S являются целыми числами, меньшими n и взаимно простыми с n .

2. Во множестве S нет повторов. Посмотрите на утверждение (2.2). Если $ax_i \bmod n$, то $x_i = x_j$. Поэтому:

$$\prod_{i=1}^{\varphi(n)} ax_i \bmod n = \prod_{i=1}^{\varphi(n)} x_i, \prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod{n},$$

$$a^{\varphi(n)} + \prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod{n}, a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Полезной оказывается и альтернативная формулировка теоремы:

$$a^{\varphi(n)+1} \equiv a \pmod{n} \quad (2.6)$$

Из теоремы Эйлера можно вывести следствие, с помощью которого демонстрируется эффективность алгоритма RSA. Для любых двух простых чисел p и q и целых чисел $n=p \cdot q$ и m (здесь $0 < m < n$) выполняется следующее условие:

$$m^{\varphi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n \quad (2.7)$$

Если $\text{НОД}(m, n) = 1$, то есть если m и n являются взаимно простыми, то указанное условие выполняется в силу теоремы Эйлера (согласно (2.5)). Предположим, что $\text{НОД}(m, n) \neq 1$. Что это означает? Поскольку $n = p \cdot q$, равенство $\text{НОД}(m, n) = 1$ эквивалентно логическому выражению $[(m \text{ не кратно } p) \text{ И } (m \text{ не кратно } q)]$. Если m кратно p , то m и n имеют общий простой множитель p и поэтому не будут взаимно простыми, а если m кратно q , то m и n имеют общий простой множитель q и поэтому не будут взаимно простыми. Таким образом, выражение $\text{НОД}(m, n) \neq 1$ оказывается эквивалентным отрицанию вышеуказанного логического выражения. Поэтому $\text{НОД}(m, n) \neq 1$ эквивалентно логическому выражению $[(m \text{ не кратно } p) \text{ ИЛИ } (m \text{ не кратно } q)]$.

Рассмотрим случай, когда m кратно p , так что $m = cp$ для некоторого положительного целого числа c . В этом случае мы должны иметь $\text{НОД}(m, n) = 1$, поскольку иначе m кратно p , m кратно q и $m < pq$. Если $\text{НОД}(m, n) = 1$, то применима теорема Эйлера, и

поэтому $m^{\varphi(q)} \equiv 1 \pmod q$. Но по правилам арифметики в классах вычетов $[m^{\varphi(q)}]^{q(p)} \equiv 1 \pmod q$, $m^{\varphi(n)} \equiv 1 \pmod q$.

Поэтому найдется такое целое число k , что $m^{\varphi(n)} = 1 + kq$.

Умножив обе части этого равенства на $m \equiv sp \pmod n$, получим $m^{\varphi(n)+1} = m + kspq \equiv m + ksp \pmod n$, $m^{\varphi(n)+1} \equiv m \pmod n$.

Подобный ряд аргументов используется для случая, когда m является кратным q . Таким образом, равенство (2.7) оказывается доказанным. Полезной будет и следующая альтернативная форма того же следствия:

$$[m^{\varphi(n)}]^k \equiv 1 \pmod n, \quad m^{k\varphi(n)} \equiv 1 \pmod n, \quad (2.8)$$

$$m^{k\varphi(n)+1} \equiv m^{k(p-1)(q-1)+1} \equiv m \pmod n.$$

2.1.4. Проверка: является ли число простым

К сожалению, не существует доступных и в то же время эффективных средств, позволяющих выяснить, является ли простым произвольное большое число. Рассмотрим один из наиболее удачных подходов к решению подобной задачи. Но сначала необходимо сформулировать определенные теоретические результаты, которые потребуются в дальнейшем. Вот первый из них.

Если p является нечетным простым числом, то уравнение $x^2 \equiv 1 \pmod p$ имеет только два решения: $x = 1$ и $x = -1$.

Доказательство. Имеем $x^2 - 1 \equiv 0 \pmod p$,
 $(x + 1)(x - 1) \equiv 0 \pmod p$.

По правилам арифметики в классах вычетов последнее равенство требует, чтобы p делило либо $(x + 1)$, либо $(x - 1)$, либо и то, и другое. Предположим, что p делит и $(x+1)$, и $(x - 1)$. Тогда $(x + 1) = kp$ и $(x - 1) = jp$ для некоторых целых чисел k и j . При вычитании одного равенства из другого получаем $2 = (k-j)p$. Это равенство может выполняться только для $p = 2$. По условию теоремы рассматриваются только нечетные простые числа. Поэтому для любого решения x в результате получается либо $p/(x+1)$, либо $p/(x-1)$, но никак не одновременно. Предположим, что $p \nmid (x - 1)$. Тогда $x - 1 = kp$ для некоторого k .

Следовательно, $x \equiv 1 \pmod p$. Точно так же получается другое решение: $x \equiv -1 \pmod p$.

Эту теорему формулируют и в противоположном виде: если существуют решения уравнения $x^2 \equiv 1 \pmod p$, отличные от ± 1 , то p не является простым числом.

2.1.5. Алгоритм Евклида

Одной из основных процедур теории чисел является алгоритм Евклида, представляющий собой простую процедуру определения наибольшего общего делителя двух положительных целых чисел. Обобщенный алгоритм Евклида определяет наибольший общий делитель двух положительных целых чисел и, если эти числа оказываются взаимно простыми, мультипликативное обратное одного из них по модулю другого.

Поиск наибольшего общего делителя.

Алгоритм Евклида опирается на следующую теорему: для любого неотрицательного целого числа a и любого положительного целого числа b справедливо следующее[^]

$$\text{НОД}(a, b) = \text{НОД}(b, a \bmod b) \quad (2.9)$$

(например, $\text{НОД}(55, 22) = \text{НОД}(22, 55 \bmod 22) = \text{НОД}(22, 11) = 11$).

Чтобы убедиться в этом, заметим, что $d = \text{НОД}(a, b)$. Тогда, по определению, НОД имеем $d|a$ и $d|b$. Для любого положительного целого числа b значение a можно представить в форме $a = kb + r = r \bmod b$, $a \bmod b = r$.

Поэтому, $(a \bmod b) = a - kb$ для некоторого целого числа k . Но, поскольку $d|b$, d делит и kb . Из условия $d|a$ следует также $d|(a \bmod b)$. Это доказывает, что d является общим делителем для b и $(a \bmod b)$. И наоборот, если d является общим делителем для b и $(a \bmod b)$, то $d|kb$ и, таким образом, $d|[kb + (a \bmod b)]$, что эквивалентно $d|a$. Итак, множество общих делителей a и b совпадает с множеством общих делителей b и $(a \bmod b)$. Поэтому и наибольший общий делитель первой пары чисел будет равен наибольшему общему делителю второй, что завершает доказательство.

Чтобы определить наибольший общий делитель, равенство (2.9) можно использовать повторно.

(Например, $\text{НОД}(18, 12) = \text{НОД}(12, 6) = \text{НОД}(6, 0) = 6$).

В алгоритме Евклида многократно применяется равенство (2.9) для определения наибольшего общего делителя следующим образом. В алгоритме предполагается, что $d > f > 0$. Можно ограничить рассмотрение только положительными целыми числами, так как $\text{НОД}(a, b) = \text{НОД}(|a|, |b|)$.

Вычисление мультипликативного обратного.

Если $\text{НОД}(d, f) = 1$, то d имеет мультипликативное обратное по модулю f . Это значит, что для положительного целого числа $d < f$

существует такое $d^{-1} < f$, что $d(d^{-1}) = 1 \bmod f$. Алгоритм Евклида можно расширить так, чтобы в дополнение к вычислению наибольшего общего делителя d и f (если наибольший общий делитель оказывается равным 1) алгоритм возвращал и мультипликативное обратное d .

2.1.6. Китайская теорема об остатках

Одним из наиболее полезных результатов теории чисел является так называемая китайская теорема об остатках (такое название данная теорема получила из-за того, что, как считается, она была открыта китайским математиком Сунь-Цзе, доказавшим ее примерно в 100 г. до н.э.). По существу, эта теорема утверждает, что можно восстановить целое число из определенного диапазона чисел по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел.

(Например, любое из десяти целых чисел в множестве $Z_{10}(0, 1, \dots, 9)$ может быть восстановлено всего по двум вычетам по модулю 2 и 5 (эти числа являются простыми делителями числа 10). Пусть известными вычетами однозначного десятичного числа x являются $r_2 = 0$ и $r_5 = 3$, т.е. $x \bmod 2 = 0$ и $x \bmod 5 = 3$. Тогда x является четным целым числом в множестве Z_{10} , остаток от деления которого на 5 равен 3. Единственным решением является $x = 8$).

Существует несколько формулировок китайской теоремы об остатках. Представим здесь формулировку, которая оказывается наиболее полезной с точки зрения материала, который потребует в дальнейшем. Пусть $M = \prod_{i=1}^k m_i$, где m_i является попарно взаимно простыми числами, то есть $\text{НОД}(m_i, m_j) = 1$ для $1 \leq i, j \leq k$ и $i \neq j$. Любое целое значение из множества Z_M можно представить с помощью набора k чисел, используя следующее соответствие:

$$A \leftrightarrow (a_1, a_2, \dots, a_k). \quad (2.10)$$

где: $A \in Z_M$, $a_i \in Z_{m_i}$ и $a_i = A \bmod m_i$ для $1 \leq i \leq k$.

Китайская теорема об остатках утверждает следующее.

1. Отображение (2.10) задает взаимно однозначное соответствие (называемое биекцией) между Z_M и декартовым произведением $Z_{m_1} \cdot Z_{m_2} \cdot \dots \cdot Z_{m_k}$. Это значит, что для каждого такого целого числа A , что $0 \leq A < M$, найдется ровно один представляющий его набор k чисел $(a_1, a_2, \dots, a_k)$, где $0 \leq a_i < m_i$ и для

каждого такого набора k чисел $(a_1, a_2, \dots, a_k)$ найдется единственное соответствующее A из множества Z_M .

2. Операции, выполняемые с элементами множества Z_M , имеют соответствующие эквиваленты во множестве наборов k чисел, где эти операции проводятся независимо по каждой из координат в некоторой подходящей системе.

Второе из представленных выше утверждений может быть доказано следующим образом.

Если $A \leftrightarrow (a_1, a_2, \dots, a_k)$, $B \leftrightarrow (b_1, b_2, \dots, b_k)$, то:
 $(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, \dots, (a_k + b_k) \bmod m_k),$
 $(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, \dots, (a_k - b_k) \bmod m_k),$
 $(A \cdot B) \bmod M \leftrightarrow ((a_1 \cdot b_1) \bmod m_1, \dots, (a_k \cdot b_k) \bmod m_k),$

Докажем первое утверждение.

Переход от A к $(a_1, a_2, \dots, a_k)$ очевидно однозначен - необходимо просто взять $a_i = A \bmod m_i$. Вычислить A по заданному $(a_1, a_2, \dots, a_k)$ можно следующим образом. Пусть $M_i = M/m_i$ для $1 \leq i \leq k$. Заметим, что $M_i = m_1 \cdot m_2 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_k$, так что $M_i \equiv 0 \pmod{m_j}$ для всех $j \neq i$. Теперь пусть:

$$c_i = M_i \cdot (M_i^{-1} \bmod m_i) \text{ для } 1 \leq i \leq k \quad (2.11)$$

По определению M_i должно быть взаимно простым с m_i и, таким образом, иметь мультипликативное обратное по модулю m_i . Поэтому равенство (2.11) оказывается вполне определенным и задает уникальное значение c_i . Теперь мы можем вычислить:

$$A \equiv (\sum_{i=1}^k a_i c_i) \bmod M \quad (2.12)$$

Чтобы показать, что значение, получаемое с помощью равенства (2.12), оказывается правильным, мы должны убедиться в том, что $a_i = A \bmod m_i$ для $1 \leq i \leq k$. Заметим, что $c_j \equiv M_j \equiv 0 \pmod{m_i}$, если $j \neq i$, и что $c_i \equiv 1 \pmod{m_i}$. Отсюда следует, что $a_i = A \bmod m_i$.

Второе утверждение китайской теоремы об остатках, касающееся арифметических операций, непосредственно вытекает из правил арифметики в классах вычетов.

Польза китайской теоремы об остатках определяется, в частности, и тем, что она указывает способ выполнения арифметических операций по модулю M над (потенциально очень большими) числами для наборов некоторых меньших по величине чисел. Это может оказаться весьма полезным, когда M имеет,

например, 150 или еще больше разрядов.

2.1.7. Дискретные логарифмы

Дискретные логарифмы составляют основу целого ряда алгоритмов криптографии с открытым ключом, в том числе алгоритма обмена ключами по Диффи - Хеллману и алгоритма цифровой подписи RSA. Представим краткий обзор теории дискретных логарифмов.

Степень целого числа по модулю n .

Нам известно, что в силу теоремы Эйлера (п.2.1.3) для любых взаимно простых a и n выполняется соотношение (2.5) $a^{\varphi(n)} \equiv 1 \pmod{n}$, где $\varphi(n)$ обозначает функцию Эйлера, значение которой равно числу положительных целых значений, меньших n и взаимно простых с n . Далее рассмотрим более общее соотношение:

$$a^m \equiv 1 \pmod{n} \quad (2.13)$$

Если a и n являются взаимно простыми, то существует по крайней мере одно целое число m , удовлетворяющее соотношению (2.13), число $m = \varphi(n)$. Для наименьшего из положительных m , при которых выполняется условие (2.13), используются следующие названия:

- порядок числа a по модулю n ;
- показатель, которому принадлежит a по модулю n ;
- длина периода последовательности, генерируемой степенями a .

В общем случае можно сказать, что наивысшим из показателей, которому может принадлежать число a по модулю n , является $\varphi(n)$. Числа, принадлежащие показателю $\varphi(n)$, называются первообразными корнями по модулю n . Важность этого понятия определяется тем фактом, что, когда a является первообразным корнем n , его степени $a, a^2, \dots, a^{\varphi(n)}$ оказываются различными по модулю n и взаимно простыми с n . В частности, для простого числа p , если a является первообразным корнем p , то $a, a^2, \dots, a^{p-1}$ оказываются различными по модулю p . (Например, для простого числа 19 его первообразными корнями являются числа 2, 3, 10, 13, 14 и 15.

Не все целые числа имеют первообразные корни. На самом деле целыми числами с первообразными корнями будут только числа $2, 4, p^a$ и $2p^a$, где p – любое нечетное простое число.

Индексы.

Для обычных положительных действительных чисел логарифм является функцией, обратной возведению в степень. Аналогичная функция существует и в арифметике классов вычетов.

Перечислим основные свойства обычного логарифмирования. Логарифм числа определяется как степень, в которую нужно возвести значение определенного положительного основания (не равного 1), чтобы получить данное число, то есть для заданного основания x и произвольного y : $y = x^{\log_x(y)}$.

Основные свойства логарифмов:

$$\log_x(1) = 0 \quad (2.14)$$

$$\log_x(x) = 1 \quad (2.15)$$

$$\log_x(yz) = \log_x(y) + \log_x(z) \quad (2.16)$$

$$\log_x y^r = r \cdot \log_x(y) \quad (2.17)$$

Рассмотрим первообразный корень некоторого простого числа p (подобные аргументы могут быть использованы и в случае с числами, не являющимися простыми). В этом случае мы знаем, что степени числа a с показателями от 1 до $(p - 1)$ порождают каждое целое число от 1 до $(p - 1)$ в точности по одному разу. Нам также известно, что любое целое число b можно представить в форме $b \equiv g \pmod{p}$, где $1 \leq g \leq (p - 1)$ в классах вычетов. Отсюда вытекает, что для любого целого числа b и любого первообразного корня a простого числа p можно найти ровно один показатель степени i , для которого

$$b \equiv a^i \pmod{p}, \text{ где } 1 \leq i \leq (p - 1).$$

Значение этого показателя (i) называют индексом числа b по модулю p при основании a . По другому это значение записываю как $\text{ind}_{a,p}(b)$.

Обратите внимание на следующий момент:

$$\text{ind}_{a,p}(1) = 0, \text{ поскольку } a^0 \pmod{p} = 1 \pmod{p} = 1 \quad (2.18)$$

$$\text{ind}_{a,p}(a) = 1, \text{ поскольку } a^1 \pmod{p} = a \quad (2.19)$$

Теперь рассмотрим:

$$\begin{aligned} x &= a^{\text{ind}_{a,p}(x)} \pmod{p}, \\ y &= a^{\text{ind}_{a,p}(y)} \pmod{p}, \\ xy &= a^{\text{ind}_{a,p}(xy)} \pmod{p}. \end{aligned}$$

Воспользовавшись правилами умножения по модулю сравнения, получим

$$a^{\text{inda},p(xy)} \bmod p = (a^{\text{inda},p(x)} \bmod p)(a^{\text{inda},p(y)} \bmod p) = \\ = (a^{\text{inda},p(x)+\text{inda},p(y)} \bmod p).$$

Теперь применим теорему Эйлера, которая утверждает, что для любых взаимно простых каждого a и n имеет место формула $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Любое положительное целое число z может быть представлено в виде $z = q + k\varphi(n)$. Поэтому по теореме Эйлера имеем $a^z \equiv a^q \pmod{n}$, если $z = q \bmod \varphi(n)$.

Используя это соотношение с предыдущим, получим равенство $\text{ind}_{a,p}(xy) = [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \bmod \varphi(p)$, обобщив которое, получаем

$$\text{ind}_{a,p}(y^r) = [r \cdot \text{ind}_{a,p}(y)] \bmod \varphi(p).$$

Это указывает на аналогию между обычными логарифмами и индексами. По этой причине последние часто называют дискретными логарифмами.

Следует иметь в виду, что однозначно дискретные логарифмы по модулю m при основании a определяются, только когда a является первообразным корнем m .

Вычисление дискретных логарифмов.

Рассмотрим уравнение $y = g^x \bmod p$.

Вычисление y при заданных g , x и p является простым делом. В самом худшем случае придется выполнить x повторных умножений, для чего имеются достаточно эффективные алгоритмы. Но если заданы y , g и p , то вычисление x из указанного выше соотношения (дискретное логарифмирование) является, вообще говоря, очень непростой задачей. По сложности эта задача сравнима с задачей разложения больших чисел на простые множители, что требуется для RSA. Сейчас сложность асимптотически наиболее быстрого из известных алгоритмов вычисления дискретных логарифмов по модулю простого числа оценивалась величиной порядка $e^{((\ln p)^{1/3} \cdot \ln(\ln p)^{2/3})}$, что для больших простых чисел оказывается за пределами практических возможностей современных вычислительных средств.

3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. Правовые и организационные методы защиты информации в ИС

3.1.1. Правовое регулирование в области безопасности информации

Безопасность является качественной характеристикой системы, ее нельзя измерить в каких-либо единицах, более того, нельзя даже с однозначным результатом сравнивать безопасность двух систем - одна будет обладать лучшей защитой в одном случае, другая - в другом. Кроме того, у каждой группы специалистов, занимающихся проблемами безопасности информационных технологий, имеется свой взгляд на безопасность и средства ее достижения, а следовательно, и свое представление о том, что должна представлять собой защищенная система. Разумеется, любая точка зрения имеет право на существование и развитие, но для того, чтобы объединить усилия всех специалистов в направлении конструктивной работы над созданием защищенных систем, все-таки необходимо определить, что является целью исследования, что мы хотим получить в результате и чего в состоянии достичь.

Для ответа на эти вопросы и согласования всех точек зрения на проблему создания защищенных систем разработаны и продолжают разрабатываться *стандарты информационной безопасности, принимаются международные, государственные ведомственные нормативные акты*. Эти документы регламентируют основные понятия и концепции информационной безопасности на государственном и межгосударственном уровне, определяют понятие «защищенная система» посредством стандартизации требований и критериев безопасности, образуют шкалу оценки степени защищенности информационных систем.

В соответствии с этими документами ответ на поставленный вопрос в общем виде звучит так: *защищенная система обработки информации* - это система, отвечающая тому или иному стандарту информационной безопасности. Конечно, это условная характеристика, она зависит от критериев, по которым оценивается безопасность, но у нее есть одно неоспоримое преимущество - объективность.

Государство должно обеспечить в стране защиту информации, как в масштабах всего государства, так и на уровне организаций и отдельных граждан [8]. Для решения этой проблемы государство обязано:

1. Выработать государственную политику безопасности в области информационных технологий;

2. Законодательно определить правовой статус информационных систем, информации, систем защиты информации, обладателей информации и т. д.;

3. Создать иерархическую структуру государственных органов, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;

4. Создать систему стандартизации, лицензирования и сертификации в области защиты информации;

5. Обеспечить приоритетное развитие отечественных защищенных информационных технологий;

6. Повышать уровень образования граждан в области информационных технологий, воспитывать у них патриотизм и бдительность;

7. Установить ответственность граждан за нарушения законодательства в области информационных технологий.

На рис. 3.1 представлена обобщенная схема нормативно-справочного обеспечения информационной безопасности (ИБ) информационных технологий (ИТ).

В соответствии с Конституцией России международные документы, подписанные от имени Российской Федерации, имеют приоритет над соответствующими документами федерального уровня. Документы, не подписанные от имени России, могут использоваться, если они не противоречат законодательству страны.

К числу международных актов относят:

- декларации;
- конвенции;
- рекомендации;
- соглашения;
- стандарты.

Разработкой этих документов занимаются различные структурные подразделения международных организаций, такие как:

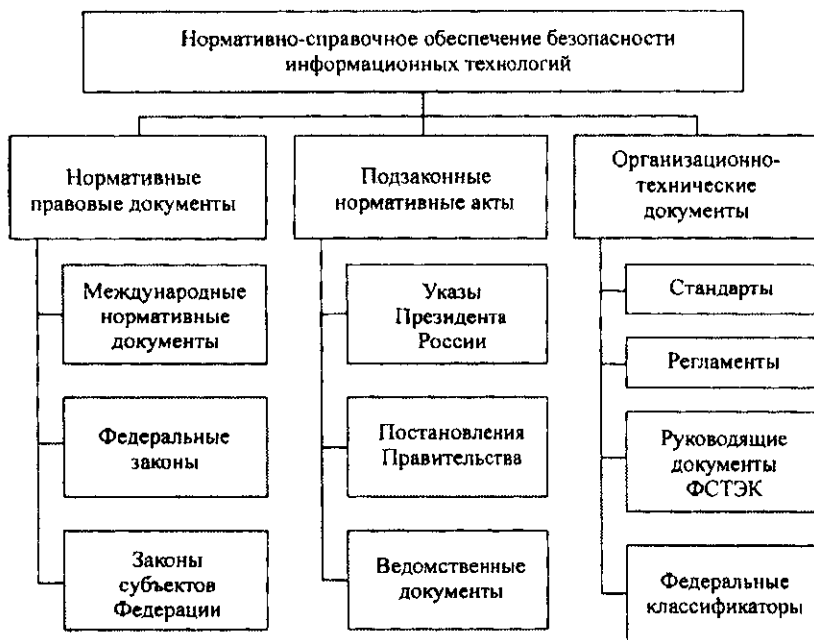


Рис. 3.1. Обобщенная схема нормативно-справочного обеспечения информационной безопасности информационных технологий

- Совет Европы (комитет министров);
- Европейский комитет по проблемам преступности;
- Комитет экспертов по преступности в киберпространстве (КЭ-ПК);
- Международная электротехническая комиссия (МЭК/IEC);
- Международная организация по стандартизации (ИСО/ISO);
- Британский институт стандартов (BSI);
- Американский институт AICPA;
- Канадский институт CICA и др.

Все это привело к тому, что сформировалось единое международное мнение о том, что эффективное обеспечение ИБ может быть достигнуто не только технологическими мерами, но для этого потребуются усилия по правовому регулированию в данной сферы и выработке соответствующих национальных политик.

Целями использования соответствующих международных документов являются:

1. Предоставление отечественным разработчикам ИТ документов, средств и методов, с помощью которых можно создавать

системы, удовлетворяющие требованиям гарантированной защищенности;

2. Предоставление государственным органам страны правил для приемки и оценки защищенности систем, предназначенных для обработки конфиденциальной и другой ценной информации;

3. Обеспечение базы для исследования требований к выбору аппаратных и программных средств для защищенных систем;

4. Приведение отечественных нормативных документов в соответствие с международными документами, если это не противоречит интересам национальной безопасности России.

Среди всех международных нормативных актов в области информационной безопасности в нашей стране чаще всего применяются организационно-технические документы, в частности стандарты.

По своему назначению и содержанию отечественную федеральную и ведомственную нормативную базу по защите информации можно разделить на три группы:

1. Документы, определяющие концептуальную основу защиты информации в Российской Федерации;

2. Пакет федеральных законов, определяющих систему защиты информации в России;

3. Вспомогательные нормативные акты в виде указов Президента РФ, постановлений Правительства РФ, межведомственных и ведомственных руководящих документов и стандартов, регулирующих процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства.

3.1.2. Концептуальные документы в области защиты информации

К основным нормативным документам, определяющим концептуальные основы обеспечения информационной безопасности в России, относятся:

1. Конституция Российской Федерации 1993 года;

2. Концепция национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 10 января 2000 г. № 24 (предыдущая редакция Концепции была утверждена Указом от 17 декабря 1997 г. № 1300);

3. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № РП-1895 г.;

4. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 г., одобренная Распоряжением Правительства Российской Федерации от 27 сентября 2004 г. №1244-р.

Конституция Российской Федерации определяет базовые принципы отношений в информационной сфере. Этому вопроса касаются, в частности, следующие статьи.

Статья 15: Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

Статья 23: Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права осуществляется только на основании судебного решения.

Статья 24: Сбор, хранение, использование и распространение информации о личной жизни лица без его согласия не допускается. Органы государственной власти, органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29: Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 44: Интеллектуальная собственность охраняется законом.

Концепция национальной безопасности Российской Федерации - политический документ, отражающий совокупность официально принятых взглядов на цели и государственную стратегию в области обеспечения безопасности личности, общества, государства от внешних и внутренних угроз политического, экономического, социального, военного, техногенного, экологического, информационного и иного характера с учетом имеющихся ресурсов и возможностей.

В Концепции сформулированы важнейшие направления и принципы государственной политики. Концепция является основой для разработки конкретных программ и организационных документов в области обеспечения национальной безопасности Российской Федерации.

Данный документ определяет, что национальные интересы России в информационной сфере обуславливают необходимость сосредоточения усилий общества, государства на решении таких задач, как:

- соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею;
- защита национальных духовных ценностей;
- пропаганда национального культурного наследия, норм морали и общественной нравственности;
- обеспечение права граждан на получение достоверной информации;
- развитие современных телекоммуникационных технологий.

В то же время объявляется недопустимым использование информации для манипулирования массовым сознанием. Декларируется необходимость защиты государственного информационного ресурса от утечки важной политической, экономически научно-технической и военной информации.

В качестве важнейших задач обеспечения национальной безопасности Российской Федерации в информационной сфере определены:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную структуру;
- разработка соответствующей нормативно-правовой базы и координация деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

• защита государственного информационного ресурса, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Доктрина информационной безопасности [10] представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны применительно к информационной сфере.

Доктрина информационной безопасности включает в себя четыре раздела:

1. Информационная безопасность Российской Федерации;
2. Методы обеспечения информационной безопасности России;
3. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации;
4. Организационная основа системы обеспечения информационной безопасности Российской Федерации.

Рассмотрим кратко их основное содержание.

В первом разделе «Информационная безопасность Российской Федерации» определены *национальные интересы* страны в информационной сфере, *угрозы* национальным интересам, их *причины и источники*, сформулированы стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре составляющие национальных интересов России в информационной сфере.

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления страны, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала России.

2. Информационное обеспечение государственной политики России, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по всем видам внутренней и международной жизни.

3. Развитие современных информационных технологий, отечественной индустрии информации.

4. Защита информационных ресурсов от НСД, обеспечение безопасности информационных и телекоммуникационных систем.

В соответствии с национальными интересами определены и все виды угроз информационной безопасности России, дана их классификация, в соответствии с которой выделяются четыре вида угроз:

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

2. Угрозы информационному обеспечению государственной политики Российской Федерации;

3. Угрозы развитию отечественной индустрии информатизации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования качественных информационных ресурсов;

4. Угрозы безопасности информационных и телекоммуникационных сред систем, как уже развернутых, так и создаваемых на территории России.

Для каждого вида угроз в Доктрине указываются их причины.

Второй раздел «Методы обеспечения информационной безопасности России» посвящен общим методам обеспечения ИБ и ее особенностям в различных сферах общественной жизни, а также международному сотрудничеству нашей страны в области обеспечения ИБ. Подробно рассмотрены методы обеспечения ИБ в сфере экономики, внутренней и внешней политики, в области науки и техники, в сфере духовной жизни, в общегосударственных информационных и телекоммуникационных системах, в сфере обороны, в правоохранительной и судебной сферах и в условиях чрезвычайных ситуаций.

Все методы обеспечения ИБ, согласно Доктрине, делятся на три группы (рис. 3.2):

- 1) Правовые;
- 2) Организационно-технические;
- 3) Экономические.



Рис. 3.2. Методы обеспечения информационной безопасности

Третий раздел «Основные положения государственной политики обеспечения ИБ России и первоочередные мероприятия по ее реализации» определяет направления деятельности органов власти всех уровней, порядок закрепления их обязанностей по защите интересов страны в информационной сфере и базируется на соблюдении баланса интересов личности, общества и государства.

Здесь рассмотрены основные принципы этой политики в сфере ИБ, которые включают:

- соблюдение Конституции РФ, законодательства РФ, общепризнанных норм и правил международного права;
- открытость в реализации функции органов власти всех уровней по информированию общества об их деятельности;

- правовое равенство всех участников процесса информационного взаимодействия, основанное на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов России.

На государство в сфере информационной безопасности возложено выполнение некоторых функций.

1. Проведение объективного и всестороннего анализа и прогнозирования в области ИБ России и выработка мер по ее обеспечению.

2. Организация работы органов власти всех уровней по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз ИБ страны.

3. Поддержка деятельности общественных объединений, направленная на объективную информированность населения о всех сторонах жизни общества, его защиты от искаженной и недостоверной информации.

4. Осуществление контроля за разработкой, созданием, развитием, использованием, экспортом и импортом средств ЗИ посредством их сертификации и лицензирования деятельности в области ЗИ.

5. Проведение необходимой протекционистской политики в отношении производителей средств информатизации и ЗИ на территории России и защиту внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов.

6. Способствование доступа юридическим и физическим лицам к мировым информационным ресурсам, глобальным информационным сетям.

7. Формирование и реализация государственной информационной политики России.

8. Организация разработки федеральной программы обеспечения ИБ.

9. Способствование интернационализации глобальных информационных систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Четвертый раздел «Организационная основа системы обеспечения ИБ России» определяет основные функции системы обеспечения ИБ, а также компетенцию территориальных органов власти, органов власти субъектов РФ, государственных организаций, входящих в систему обеспечения ИБ. Система обеспечения ИБ является частью системы обеспечения национальной безопасности страны.

Основными элементами организационной основы системы обеспечения ИБ Российской Федерации являются:

- Президент Российской Федерации;
- Совет Федерации;
- Государственная Дума РФ;
- Правительство РФ;
- Совет безопасности РФ;
- федеральные органы исполнительной власти;
- межведомственные комиссии по защите гостайны и по информационной безопасности;
- органы исполнительной власти субъектов; органы местного самоуправления, органы судебной власти;
- общественные объединения, граждане.

Примечание. ФАПСИ реорганизовано и вошло в МО РФ и ФСБ России, а Государственная техническая комиссия преобразована в ФСТЭК России.

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют государственные органы, структура которых приведена на рис.3.3.

Возглавляет государственные органы обеспечения информационной безопасности Президент РФ. Он руководит Советом Безопасности и утверждает указы, касающиеся обеспечения безопасности информации в государстве.

Общее руководство системой информационной безопасности, наряду с другими вопросами государственной безопасности страны, осуществляют Президент и Правительство Российской Федерации.

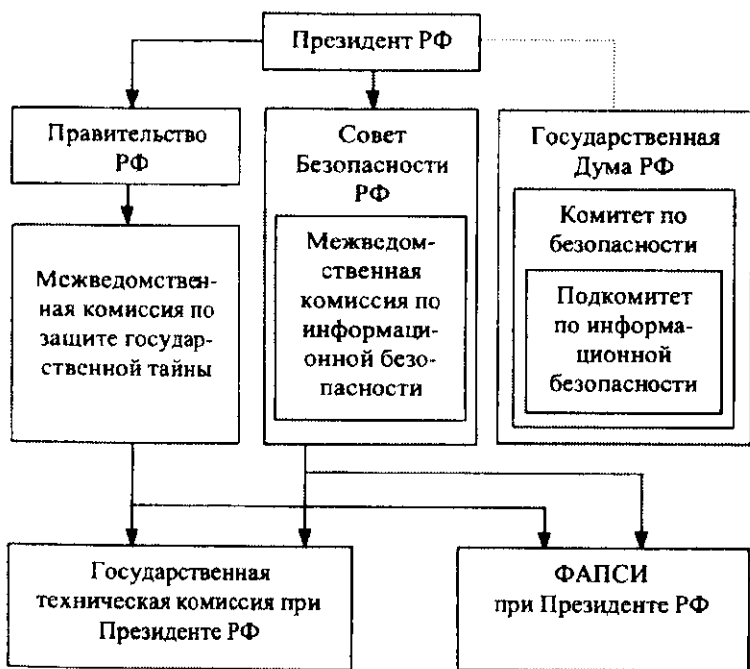


Рис. 3.3. Структура государственных органов, обеспечивающих проведение политики информационной безопасности в РФ

Органом исполнительной власти, непосредственно занимающимся вопросами государственной безопасности, является Совет Безопасности при Президенте РФ. В состав Совета Безопасности входит Межведомственная комиссия по информационной безопасности. Комиссия готовит указы Президента, выступает с законодательной инициативой, координирует деятельность руководителей министерств и ведомств в области информационной безопасности государства.

Рабочим органом Межведомственной комиссии по информационной безопасности является Государственная техническая комиссия при Президенте РФ. Эта комиссия осуществляет подготовку проектов законов, разрабатывает нормативные документы (Решения Государственной технической комиссии, ныне ФСТЭК России), организует сертификацию средств защиты информации (за исключением криптографических средств), лицензирование деятельности в области производства средств

защиты и обучения специалистов по защите информации [5]. Гостехкомиссия руководит аттестацией ИС, предназначенных для обработки информации, представляющей государственную тайну, или управляющих экологически опасными объектами. Она координирует и направляет деятельность государственных научно-исследовательских учреждений, работающих в области защиты информации, обеспечивает аккредитацию органов лицензирования и испытательных центров (лабораторий) по сертификации. Эта комиссия обеспечивает также работу Межведомственной комиссии по защите государственной тайны.

На Межведомственную комиссию по защите государственной тайны возложена задача руководства лицензированием предприятий, учреждений и организаций, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также оказанием услуг по защите гостайны. Кроме того, эта комиссия осуществляет координацию работы по организации сертификации средств защиты информации.

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) обеспечивает правительственную связь и информационные технологии государственного управления. Агентство осуществляет сертификацию всех средств, используемых для организации правительственной связи и информатизации государственного управления, а также лицензирует все предприятия, учреждения и организации, занимающиеся производством таких средств. Кроме того, в исключительном ведении ФАПСИ находятся вопросы сертификации и лицензирования в области криптографической защиты информации.

В министерствах и ведомствах создаются иерархические структуры обеспечения безопасности информации, которые, как правило, совпадают с организационной структурой министерства (ведомства). Называясь они могут по-разному, но функции выполняют сходные

Концепция использования информационных технологий в деятельности федеральных органов государственной власти России разработана Министерством информационных технологий и связи. Ее целью является определение основных приоритетов, принципов и направлений реализации единой государственной политики в сфере использования ИТ в деятельности федеральных органов государственной власти. В результате реализации Концепции

ожидается формирование эффективной системы предоставления государственных услуг на основе использования ИТ.

В Концепции поставлен ряд *задач*, решение которых позволит повысить эффективность использования ИТ. Среди этих задач имеются и связанные с защитой информации:

1. Обеспечение информационной безопасности деятельности федеральных органов государственной власти (ОГВ) и элементов информационно-технологической инфраструктуры;

2. Развитие единой защищенной телекоммуникационной инфраструктуры для государственных нужд, системы удостоверяющих центров в области электронной цифровой подписи (ЭЦП) и электронной среды взаимодействия, обеспечивающей эффективный межведомственный информационный обмен;

3. Разработка стандартов в сфере использования ИТ в деятельности федеральных органов государственной власти, создание государственных ИС, их интеграция и совместное использование в рамках создания общего информационного пространства федеральных органов власти.

4. Защита интеллектуальной собственности, недопущение использования в деятельности федеральных органов власти программного обеспечения, не имеющего соответствующей лицензионной поддержки.

Концепция определяет основные *приоритеты* в следующих областях:

- социально-экономического развития;
- государственного управления;
- обеспечения информационной открытости;
- информационной безопасности;
- формирования информационного пространства и защищенной информационной среды федеральных органов власти;
- разработки единых требований к основным элементам информационно-технологического обеспечения;
- создания общегосударственных информационных ресурсов;
- совершенствования нормативной правовой базы в области ИТ и др.

Пакет федеральных нормативных правовых актов, касающихся информационной безопасности, распространения информации в целом и сил и средств обеспечения ее защиты на государственном уровне, включает несколько десятков документов. Это: кодексы; законы, регулирующие отдельные аспекты нескольких

видов деятельности; регулирующие отдельные видов деятельности; законы о деятельности органов государственной власти; законы, непосредственно касающиеся защиты информации.

Высокие темпы информатизации, а также социально-экономические изменения в обществе, происшедшие в последние годы, требовали законодательного регулирования отношений, складывающихся в области информационных технологий. Эта проблема во многом была решена Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ [8]. В законе даны определения основных терминов: информация; информационная технология; информационно-телекоммуникационная сеть; информационные системы; обладатель информации; доступ к информации; конфиденциальная информация; предоставление информации; распространение информации; электронное сообщение; документированная информация; оператор информационной системы. Государство гарантирует права обладателя информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом. Обладатель информации имеет право разрешать или ограничивать доступ к информации. В законе определены права и обязанности граждан и государства по доступу к информации. В этом законе дано определение защите информации.

Другим важным правовым документом, регламентирующим вопросы защиты информации в ИС, является закон РФ «О государственной тайне» от 21.07.1993 г. №5485-1 (с изменениями и дополнениями, вступившими в силу с 15.07.2007 г. Закон определяет уровни секретности государственной информации (грифы секретности) и соответствующую степень важности информации. Руководствуясь данным законом и «Перечнем сведений, отнесенных к государственной тайне», введенным в действие Указом Президента РФ от 30 ноября 1995 года, соответствующие государственные служащие устанавливают гриф секретности информации.

На основании приведенных правовых документов ведомства (министерства, объединения, корпорации и т. п.) разрабатывают нормативные документы (приказы, директивы, руководства, инструкции и др.), регламентирующие порядок использования и защиты информации в подведомственных организациях.

Очень важным правовым вопросом является установление юридического статуса ИС и особенно статуса информации, получаемой с применением ИС. Статус информации или ее

правомочность служит основанием для выполнения (невыполнения) определенных действий. Например, в одних АСУ соответствующее должностное лицо имеет юридическое право принимать решения только на основании информации, полученной из АСУ. В других АСУ для принятия решения необходимо получить подтверждающую информацию по другим каналам. В одной и той же АСУ решение может приниматься как с получением подтверждающей информации, так и без нее. Примером может служить организация перевода денег с помощью АСУ. До определенной суммы перевод осуществляется автоматически при поступлении соответствующей заявки. Для перевода крупной суммы выполняются дополнительные процедуры проверки правомочности такой операции. Для этого может быть затребована дополнительная информация, в том числе и по дублирующей системе, а окончательное решение о переводе денег может принимать должностное лицо.

Правовой статус информации устанавливается с учетом ее стоимости (важности) и степени достоверности, которую способна обеспечить компьютерная система.

3.1.3. Правонарушения и преступления в информационной сфере

Важной составляющей правового регулирования в области информационных технологий является установление ответственности граждан за противоправные действия при работе с ИС. Преступления, совершенные с использованием ИС или причинившие ущерб владельцам компьютерных систем, получили название компьютерных преступлений. В нашей стране 1 января 1997 года введен в действие новый Уголовный кодекс РФ. В него впервые включена глава № 28, в которой определена уголовная ответственность за преступления в области компьютерных технологий.

В статье 272 предусмотрены наказания за неправомерный доступ к компьютерной информации. За данное деяние предусмотрены наказания, лежащие в диапазоне от денежного штрафа в размере 200 минимальных зарплат до лишения свободы на срок до 5 лет. Отягощающими вину обстоятельствами являются совершение преступления группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных (вредительских) программ для ЭВМ. По этой статье предусмотрено наказание от штрафа в размере заработной платы или иного дохода осужденного за два месяца до лишения свободы на срок до семи лет (в зависимости от последствий).

В статье 274 определена ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Нарушение правил эксплуатации лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от ста восьмидесяти до двухсот часов. Если те же деяния повлекли тяжкие последствия, то предусмотрено лишение свободы на срок до 4 лет.

3.1.4. Организационные меры по защите информации

Законы и нормативные акты особенно эффективны в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности информации такая деятельность относится к организационным методам защиты информации.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации ИС для обеспечения заданного уровня безопасности информации.

Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации. В соответствии с законами и нормативными актами в министерствах, ведомствах, на предприятиях (независимо от форм собственности) для защиты информации создаются специальные службы безопасности (на практике они могут называться и иначе). Эти службы подчиняются, как правило, руководству учреждения. Руководители служб организуют создание и функционирование систем защиты информации. На организационном уровне решаются следующие задачи обеспечения безопасности информации в ИС:

- ♦организация работ по разработке системы защиты информации;

- ♦ ограничение доступа на объект и к ресурсам ИС;
- ♦ разграничение доступа к ресурсам ИС;
- ♦ планирование мероприятий;
- ♦ разработка документации;
- ♦ воспитание и обучение обслуживающего персонала и пользователей;
- ♦ сертификация средств защиты информации;
- ♦ лицензирование деятельности по защите информации;
- ♦ аттестация объектов защиты;
- ♦ совершенствование системы защиты информации;
- ♦ оценка эффективности функционирования системы защиты информации;
- ♦ контроль выполнения установленных правил работы в ИС.

Организационные методы являются стержнем комплексной системы защиты информации в ИС. Только с помощью этих методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему. Наибольшее внимание организационным мероприятиям уделено в главе 4 при изложении вопросов построения и организации функционирования систем защиты информации в информационных системах.

3.2. Технические каналы утечки информации

3.2.1. Технические каналы утечки информации в информационных системах

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры и субъектов, осуществляющих сбор, формирование, распространение и использование информации.

Под информацией понимаются сведения (сообщения, данные) независимо от формы их представления [8].

К *защищаемой информации* относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации [8]. Это, как правило, *информация ограниченного доступа*, содержащая

сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации часто называют обобщенным термином *обработка информации* [9].

К *техническим средствам передачи, обработки, хранения и отображения информации* ограниченного доступа (ТСПИ) относятся [10]: технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы, в дальнейшем именуемые средствами вычислительной техники (СВТ); средства изготовления и размножения документов; аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода; системы внутреннего телевидения; системы видеозаписи и видеовоспроизведения; системы оперативно-командной связи; системы внутренней автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д. Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС) [11].

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях устанавливаются и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуют. К ним относятся: системы и средства городской автоматической телефонной связи; системы и средства передачи данных в системе радиосвязи; системы и средства охранной и пожарной сигнализации; системы и средства оповещения и сигнализации; контрольно-измерительная аппаратура; системы и средства кондиционирования; системы и средства проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, телевизоры и радиоприемники и т.д.); средства электронной оргтехники; системы и средства электрочасофикации и иные технические средства и системы. Такие технические средства и системы называются *средствами обеспечения объекта информатизацией* или *вспомогательными техническими средствами и системами* (ВТСС) [10, 11].

Электропитание ТСПИ и ВТСС осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной

подстанцией городской электросети. Все технические средства и системы, питающиеся от электросети, должны быть заземлены. Типовая система заземления включает общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с техническими средствами.

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, как правило, проходят провода и кабели, не относящиеся к ТСПИ и ВТСС, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, которые называются *посторонними проводниками (ПП)* [11].

Совокупность информационных ресурсов, средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации (вспомогательных технических средств и систем), помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, называется *объектом информатизации* или *объектом ТСПИ* [9, 10].

Некоторые соединительные линии ВТСС, а также посторонние проводники могут выходить за пределы не только объекта информатизации, но и *контролируемой зоны (КЗ)*, под которой понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц (посетителей, работников различных технических служб, не являющихся сотрудниками организации), а также транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации, а также ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории [11].

Таким образом, при рассмотрении объекта информатизации, как объекта разведки, его необходимо рассматривать как систему, включающую:

технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа, вместе с их соединительными линиями (под соединительными линиями понимают совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами);

вспомогательные технические средства и системы вместе с их соединительными линиями;

посторонние проводники;

систему электропитания объекта;
систему заземления объекта.

Для добывания информации, обрабатываемой техническими средствами, «противник» (лицо или группа лиц, заинтересованных в получении этой информации) может использовать широкий арсенал портативных технических средств разведки (ТСР).

Совокупность объекта разведки (в данном случае - объекта информатизации), технического средства разведки, с помощью которого добывается информация, и физической среды, в которой распространяется информационный сигнал, называется *техническим каналом утечки информации* (рис. 3.4).

Технические каналы утечки информации можно разделить на естественные и специально создаваемые.

Естественные каналы утечки информации возникают за счет побочных электромагнитных излучений, возникающих при обработке информации техническими средствами (электромагнитные каналы утечки информации), а также вследствие наводок информационных сигналов в линиях электропитания ТСПИ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации).

К специально создаваемым каналам утечки информации относятся каналы, создаваемые путем внедрения в ТСПИ электронных устройств перехвата информации (закладных устройств) и путем высокочастотного облучения ТСПИ

Электромагнитные каналы утечки информации.

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно [12]:

- побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;
- побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
- побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

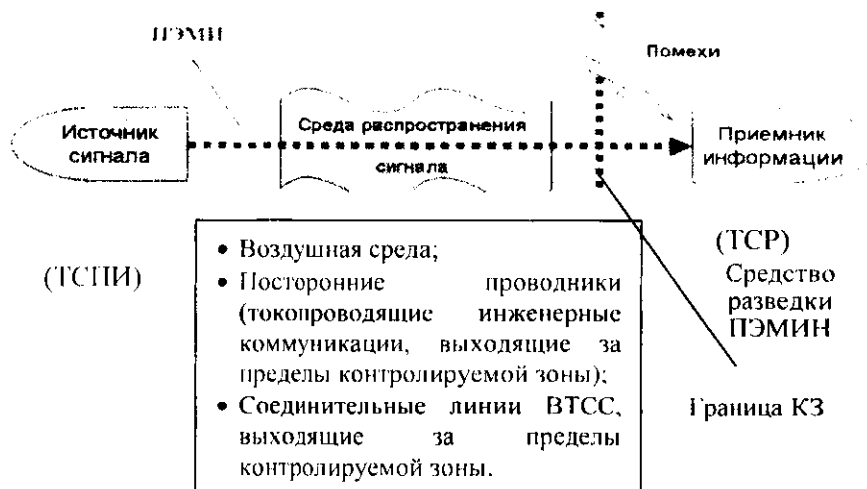


Рис. 3.4.Схема технического канала утечки информации

В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Источниками ПЭМИ могут являться различного рода высокочастотные генераторы, например: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов.

Наиболее характерные ПЭМИ, вызванные работой генераторов тактовой частоты, наблюдаются у средств вычислительной техники (СВТ). Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники: вывод информации на экран монитора; ввод данных с клавиатуры; запись информации на накопители; чтение информации с накопителей;

передача данных в каналы связи: вывод данных на периферийные печатные устройства - принтеры, плоттеры; запись данных от сканера на магнитный носитель (ОЗУ).

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Поэтому более подробно рассмотрим этот режим работы СВТ [12].

В формировании видеоизображения на экране монитора участвует видеоподсистема, которая состоит из двух основных частей: монитора и видеоадаптера (часто видеоадаптер называют видеокартой).

Видеоадаптер предназначен для формирования видеосигнала, которое происходит следующим образом.

Прежде чем стать изображением на мониторе, цифровые данные об изображении обрабатываются центральным процессором ПЭВМ, затем из его оперативной памяти через шину данных они поступают в специализированный процессор видеоадаптера, где обрабатываются и сохраняются в видеопамяти. В видеопамяти создается цифровой образ изображения, которое должно быть выведено на экран монитора. Затем, все еще в цифровом формате, данные, образующие образ изображения, из видеопамяти передаются в цифроаналоговый преобразователь (Digital Analog Converter, DAC), который часто называют RAMDAC, где они преобразуются в аналоговый вид и только после этого передаются в монитор с электронно-лучевой трубкой (ЭЛТ).

С появлением жидкокристаллических дисплеев (ЖК) потребность в цифроаналоговом преобразователе исчезла, но этот компонент всё равно присутствует в видеокартах на случай подключения аналоговых мониторов через разъем VGA.

Экран монитора отображает информацию в виде точек - пикселей. Слово пиксель («Pixel») расшифровывается как "picture element" - элемент изображения. Он представляет собой крошечную точку на дисплее, яркость и цвет которой изменяется в зависимости от выводимого на экран изображения (рис. 3.5).

Все вместе пиксели и составляют изображение. Картинка на экране обновляется от 65 до 120 раз в секунду в зависимости от типа дисплея и данных, выдаваемых выходом видеокарты. Данная характеристика называется частотой обновления (или регенерации) экрана. Согласно современным эргономическим стандартам частота обновления экрана должна составлять не менее 85 Гц, в противном

случае человеческий глаз замечает мерцание, что отрицательно влияет на зрение.

Мониторы с ЭЛТ обновляют дисплей строчка за строчкой, а плоские ЖК-мониторы могут обновлять каждый пиксель по отдельности.



Рис. 3.5. Увеличенный фрагмент изображения на экране монитора

Количество точек в изображении зависит от установленного режима отображения (количество точек по горизонтали N_x и количество точек по вертикали N_y). Наиболее часто используемые следующие режимы отображения: 1024 пикселей по горизонтали и 768 по вертикали или 1280 пикселей по горизонтали и 1024 по вертикали.

В электронно-лучевых мониторах информация об изображении передается видеокарты последовательно, пиксель за пикселем, начиная с самой верхней левой точки экрана - до правой нижней. Во многом временные диаграммы формирования изображения на экране ПЭВМ аналогичны работе телевизора. Цвет и яркость изображения каждого пикселя будут определяться уровнем сигналов, синхронно передаваемых по трем проводам R, G и B. На отображение каждого пикселя (точки изображения) тратится строго определенное время, которое обозначим t . Данное время часто называют пиксельной скоростью заполнения (pixel fill rate). Пиксельная скорость заполнения соответствует скорости выдачи пикселей. Она рассчитывается как число растровых операций, помноженное на тактовую частоту. На отображение всей строки тратится время $t = N_x \cdot \tau$, где N_x - число пикселей в строке. После отображения всей строки следует строчный синхроимпульс. Далее во времени отображается вторая строка, третья строка и т.д. После последней строки следует кадровый синхроимпульс.

Любой текст или любая картинка передается на экран в виде цифровых импульсов разной длительности. Длительность импульсов τ_i зависит от вида текста или картинки, отображаемой на экране. Минимальная длительность импульса будет равна $\tau_{\min} = t$, а максимальная $\tau_{\max} = N_x \cdot \tau$.

При прохождении по проводникам импульсных сигналов возникают побочные электромагнитные излучения (ПЭМИ).

Следовательно, источником ПЭМИ является видеокарта, а в качестве антенны выступают отрезки проводников, по которым распространяется сигнал: внутренние жгуты проводов, связывающие между собой отдельные платы, разъемы и элементы конструкции, а также внешние кабели, соединяющие отдельные устройства и т.п. Данное положение подтверждено экспериментально: при отключении монитора от видеокарты побочные электромагнитные излучения не исчезают, уменьшается лишь их уровень. Мощность информативного сигнала ПЭМИ зависит от амплитуды генерируемых импульсов и качества антенны, которое оценивается ее коэффициентом усиления.

Коэффициент усиления антенны во многом зависит от длины излучающего кабеля (проводника). Длина излучающего кабеля (проводника) СВТ всегда значительно меньше длины волны излучения первой гармоники информативного сигнала (частота излучения первой гармоники сигнала зависит от установленного режима отображения и, как правило, находится в диапазоне частот от

12 до 75 МГц), так как длина самых длинных кабелей (кабелей, соединяющих системный блок с монитором и принтером) обычно не превышает 1,5 м, а длина внутренних проводов не превышает нескольких десятков сантиметров. Следовательно, резонансные частоты таких антенн будут находиться в диапазоне частот от 200 до 800 МГц.

Вследствие этого на практике сначала амплитуда сигналов ПЭМИ с возрастанием номера гармоники уменьшается, затем на определенных частотах (как правило, в диапазоне частот от 150 до 600 МГц) возрастает, а затем опять снижается.

Разведывательный приемник, предназначенный для перехвата ПЭМИ видеосистемы, должен иметь полосу пропускания $\Delta F_n \geq 1/\tau$. При использовании полосы пропускания приемника $\Delta F_n < 1/\tau$ импульсы с длительностью $\tau_n = \tau$ будут восстанавливаться с искажениями, что приведет к искажениям мелких деталей изображения (например, искажению букв, см. рис. 3.6).



Рис. 3.6. Увеличенное изображение слова «Сигнал», написанное 14 кеглем шрифта Arial при разрешении экрана 1280x1024 (а) и его изображение, полученное с более низким разрешением (б)

Последовательность импульсов черных и белых точек тестового сигнала периодически прерывают импульсы строчной и кадровой развертки, поэтому излучаемый сигнал ПЭМИ будет периодически «прерываться» на время действия данных импульсов.

Паразитная генерация в элементах ТСПИ, в том числе самовозбуждение усилителей низкой частоты (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.), возможна за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается

модулированным информационным сигналом. Самовозбуждение наблюдается в основном при переводе усилителя в нелинейный режим работы, т.е. в режим перегрузки.

Перехват информации осуществляется путем приема и детектирования средством разведки побочных электромагнитных излучений, возникающих при работе ТСПИ.

Для перехвата побочных электромагнитных излучений ТСПИ используются специальные перевозимые и переносимые средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Данные средства могут развертываться в машинах или близлежащих зданиях, расположенных за пределами контролируемой зоны объекта (рис.3.7).

Зная характеристики приемного устройства и антенной системы, средства разведки можно рассчитать допустимое (нормированное) значение напряженности электромагнитного поля в точке размещения средства разведки, при котором отношение «информационный сигнал/помеха» на входе приемного устройства будет равно некоторому (нормированному) значению, обеспечивающим или обнаружение средством разведки информационных сигналов с требуемой вероятностью, или измерение их параметров с допустимыми ошибками, а значит, и выделение полезной информации.

Пространство вокруг ТСПИ, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного) значения, называется опасной зоной 2 (R_2) [11] (рис. 3.7).

Зона R_2 для каждого ТСПИ определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий (рис. 3.8):

- первое - расстояние от ТСПИ до границы контролируемой зоны должно быть менее зоны R_2 ;

- второе - за пределами зоны R_2 , в пределах зоны R_2 возможно размещение портативных (переносимых, перевозимых или стационарных) средств разведки ПЭМИН.

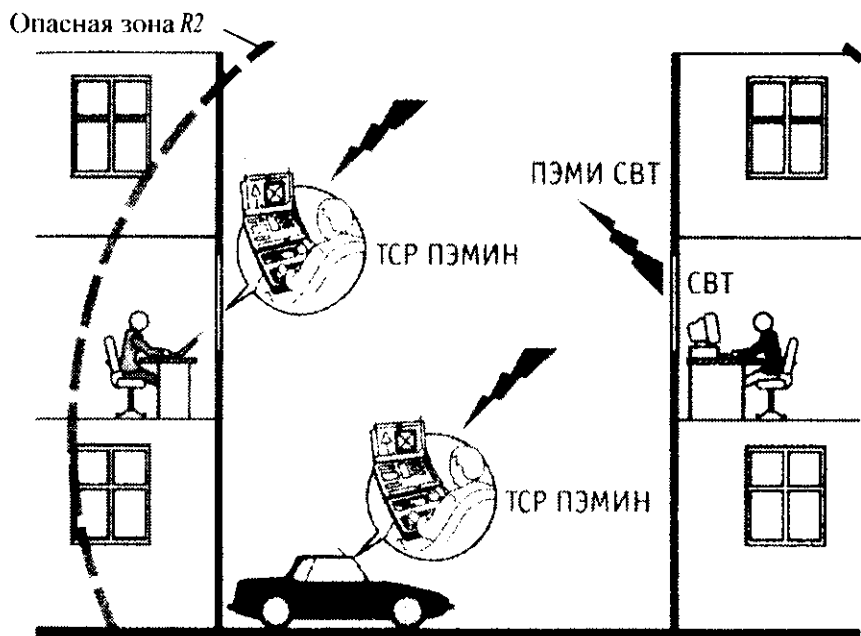


Рис. 3.7. Перехват побочных электромагнитных излучений СВТ средствами разведки ПЭМИИ

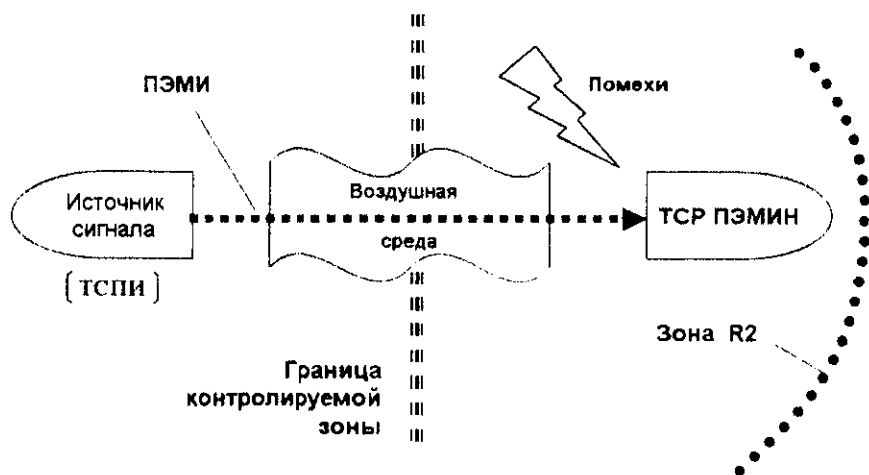


Рис. 3.8. Схема перехвата побочных электромагнитных излучений ТСПИ (электромагнитный канал утечки информации)

Электрические каналы утечки информации.

Причинами возникновения электрических каналов утечки информации являются наводки информационных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, емкостными и индуктивными связями [9].

Наводки информационных сигналов могут возникать [12]:

- в линиях электропитания ТСПИ;
- в линиях электропитания и соединительных линиях ВТСС;
- в цепях заземления ТСПИ и ВТСС;
- в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

Появление информационных сигналов в цепи электропитания ТСПИ возможно как за счет ПЭМИ, так и при наличии внутренних паразитных емкостных и (или) индуктивных связей выпрямительного устройства блока питания ТСПИ. Например, в усилителе низкой частоты токи усиливаемых сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. Кроме того, среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает

электромагнитное поле, которое также является источником информации.

Различные вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления являются как бы случайными антеннами, при непосредственном (через токосъемник или индукционный датчик) подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов.

Случайные антенны могут быть сосредоточенными и распределенными.

Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т.д.), подключенное к линии, выходящей за пределы контролируемой зоны.

К *распределенным случайным антеннам* относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны. Уровень наводимых в них сигналов в значительной степени зависит не только от мощности излучаемых сигналов, но и расстояния от линий ТСПИ до линий ВТСС или посторонних проводников, а также длины их совместного пробега.

При распространении по случайной антенне наведенный информационный сигнал затухает. Коэффициент затухания информационного сигнала можно рассчитать, зная расстояние от места возможного подключения ТСП к случайной антенне до объекта ТСПИ и частоты побочных электромагнитных излучений. При известном коэффициенте затухания легко рассчитать значение наведенного информационного сигнала в случайной антенне, при котором на входе приемного устройства средства разведки уровень информационного сигнала будет равен некоторому пороговому (нормированному) значению, при котором еще возможно или обнаружение средством разведки информационных сигналов с требуемой вероятностью, или измерение их параметров с допустимыми ошибками.

Пространство вокруг ТСПИ, на границе и за пределами которого уровень наведенного от ТСПИ информативного сигнала в сосредоточенных антеннах не превышает допустимого

(нормированного) значения, называется зоной I (r_1), а в распределенных антеннах - зоной 1 (r_1) [11].

В отличие от зоны R_2 размер зоны r_1 (r_1) зависит не только от уровня побочных электромагнитных излучений ТСПИ, но и от длины случайной антенны (от помещения, в котором установлено ТСПИ, до места возможного подключения к ней средства разведки).

Зоны r_1 (r_1) для каждого ТСПИ определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия. При этом для возникновения электрического канала утечки информации необходимо, чтобы:

соединительные линии ВТСС, линии электропитания ТСПИ, посторонние проводники и т.д., выполняющие роль случайных антенн, имели выход за пределы контролируемой зоны;

расстояние от ТСПИ до ВТСС было менее r_1 , либо расстояние от ТСПИ до соединительных линий ВТСС или посторонних проводников, выходящих за пределы контролируемой зоны, должно быть менее r_1 ;

за пределами контролируемой зоны должна существовать возможность непосредственного подключения или к линиям электропитания и заземления ТСПИ, или к соединительным линиям ВТСС, или к посторонним проводникам портативных средств разведки ПЭМИН.

Перехват наведенных сигналов с линий электропитания и заземления ТСПИ возможен в случае, если трансформаторная подстанция или заземлитель находятся за пределами контролируемой зоны объекта.

Специально создаваемые технические каналы утечки информации

Наряду с пассивными способами перехвата информации, обрабатываемой ТСПИ, рассмотренными выше, возможно использование и активных способов, в частности, способа «высокочастотного облучения», при котором ТСПИ облучается мощным высокочастотным гармоническим сигналом (для этих целей используется высокочастотный генератор с направленной антенной, имеющей узкую диаграмму направленности). При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит модуляция вторичного излучения информационным

сигналом. Переизлученный сигнал принимается приемным устройством средства разведки и детектируется.

Для перехвата информации, обрабатываемой ТСПИ, также возможно использование электронных устройств перехвата информации (*закладных устройств*), скрытно внедряемых в технические средства и системы.

Закладные устройства представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается в специальное запоминающее устройство, а уже затем по команде управления передается по радиоканалу на приемный пункт. Для передачи информации также могут использоваться линии электропитания ТСПИ или инфракрасный канал.

Наиболее вероятна установка закладных устройств в ТСПИ иностранного производства. Закладные устройства, внедряемые в ТСПИ, по виду перехватываемой информации можно разделить на:

- аппаратные закладки для перехвата изображений, выводимых на экран монитора;
- аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ;
- аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер);
- аппаратные закладки для перехвата информации, записываемой на жесткий диск ПЭВМ.

Аппаратные закладки для перехвата изображений, выводимых на экран монитора, состоят из блока перехвата и компрессии, передающего блока, блока управления и блока питания (преобразователя AC/DC). Они скрытно устанавливаются, как правило, в корпусе монитора (возможна установка закладки и в системном блоке ПЭВМ) и контактно подключаются к кабелю монитора.

Перехваченная информация (видеоизображение) в цифровом виде передается по радиоканалу, линии электросети 220 В или выделенной линии на приемный пункт, где перехваченное изображение восстанавливается и отображается на экране компьютера в реальном масштабе времени, создавая «копию экрана», а дополнительная информация может записываться на жесткий диск для дальнейшей обработки.

Блок дистанционного управления предназначен для приема сигналов дистанционного включения и выключения закладного устройства и установления параметров работы передающего устройства.

Питание закладного устройства осуществляется от сети 220 В через блок питания.

Приемный комплекс состоит из радиоприемного устройства, модема, ПЭВМ типа notebook и специального программного обеспечения.

Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ, скрытно устанавливаются в корпусе клавиатуры или внутри системного блока и подключаются к интерфейсу клавиатуры. Они состоят из модуля перехвата, передающего блока и блока управления. Питание закладок осуществляется от интерфейса клавиатуры.

Модуль перехвата осуществляет перехват сигналов, передаваемых от клавиатуры в системный блок при нажатии клавиши. Перехваченные сигналы в цифровом виде передаются по радиоканалу на приемный пункт, где в реальном масштабе времени восстанавливаются и отображаются на экране компьютера в виде символов, набираемых на клавиатуре.

Блок дистанционного управления предназначен для приема сигналов дистанционного включения и выключения закладного устройства и установления параметров работы передающего устройства.

Приемный комплекс состоит из радиоприемного устройства, специального модемного модуля (модема), ПЭВМ типа notebook и специального программного обеспечения.

Данные закладные устройства предназначены в основном для перехвата паролей пользователей и текстовых документов, набираемых с использованием ПЭВМ.

Аппаратные закладки для перехвата информации, выводимой на принтер, устанавливаются в корпусе принтера, и по принципу работы аналогичны аппаратным закладкам, рассмотренным выше.

Аппаратные закладки для перехвата информации, записываемой на жесткий диск ПЭВМ, являются наиболее сложными из рассмотренных выше. Они состоят из блока перехвата, блока обработки, передающего блока, блока управления и блока питания (преобразователя AC/DC). Они скрытно устанавливаются в системном блоке ПЭВМ и контактно подключаются через

специальный блок перехвата к интерфейсу, соединяющему жесткий диск с материнской платой. Перехватываемые сигналы поступают в блок специальной обработки, включающий специализированный процессор, где осуществляется их обработка по специальной программе. Файлы с заданным расширением (например, *.doc) записываются в оперативную или flash память. По команде управления записанная в памяти информация в цифровом виде по радиоканалу или сети 220 В передается на приемный пункт, где в виде отдельных файлов записывается на жесткий диск для дальнейшей обработки.

Питание закладного устройства осуществляется от сети 220 В через блок питания.

Приемный комплекс состоит из радиоприемного устройства, модема, ПЭВМ типа notebook и специального программного обеспечения.

Таким образом, перехват информации, обрабатываемой техническими средствами, может осуществляться путем (рис. 3.9):



Рис. 3.9. Классификация способов перехвата информации, обрабатываемой техническими средствами

- перехвата побочных электромагнитных излучений, возникающих при работе технических средств;
- перехвата наводок информационных сигналов с соединительных линий ВТСС и посторонних проводников;
- перехвата наводок информационных сигналов с линий электропитания и заземления ТСПИ;
- «высокочастотного облучения» ТСПИ;
- внедрения в ТСПИ закладных устройств.

3.2.2. Способы перехвата информации, передаваемой по каналам связи

Способы перехвата информации, передаваемой по каналам проводной связи

До настоящего времени телефонная связь превалирует среди многих видов электрорадиосвязи, поэтому телефонный канал является основным, на базе которого строятся узкополосные и широкополосные каналы для других видов связи. На передающей стороне телефонного канала в качестве передатчика используется микрофон, который преобразует акустические сигналы в полосе частот от 0,3 до 3,4 кГц в электрические сигналы таких же частот. На приемной стороне телефонный канал заканчивается телефонным капсюлем (телефоном), преобразующим электрическую энергию в акустические сигналы в этой же полосе частот.

Для передачи информации используются аналоговый и дискретный (цифровой) каналы.

Аналоговый канал чаще называют каналом тональной частоты (ТЧ). Он используется для передачи речи, электронной почты, данных, телеграфирования, факсимильной связи и т.п. Пропускная способность канала ТЧ составляет $C_x = 25$ кбит/с [13].

Стандартный цифровой канал (ЦЦК) с пропускной способностью $C_x = 64$ кбит/с разработан прежде всего для передачи речи в реальном времени, т.е. для обычной телефонии с целью передачи сигналов частот 0,3-3,4 кГц [13].

Чтобы полосу частот 0,3 - 3,4 кГц (аналоговый сигнал - речь) преобразовать в цифровой поток со скоростью 64 кбит/с, осуществляют три операции: дискретизацию, квантование и кодирование.

В современной многоканальной аппаратуре имеется возможность создания каналов с более высокой пропускной

способностью, чем у каналов ТЧ и СЦК. Увеличение пропускной способности достигается расширением эффективно передаваемой полосы частот. Все каналы используют одну линию передачи, поэтому оконечная часть аппаратуры должна осуществлять разделение каналов.

Среди возможных методов разделения каналов преимущественное распространение получили два - частотный и временной [13]. При частотном методе каждому из каналов отводится определенный участок частотного диапазона в пределах полосы пропускания линии связи. Отличительными признаками каналов являются занимаемые ими полосы частот в пределах общей полосы пропускания линии связи. При временном методе разделения каналы подключаются к линии связи поочередно, так что для каждого канала отводится определенный временной интервал в течение общего времени передачи группового сигнала. Отличительным признаком канала в этом случае является время его подключения к линии связи.

Современная многоканальная аппаратура строится по групповому принципу. При построении оконечной аппаратуры используется многократное преобразование частоты. Сущность многократного преобразования частоты заключена в том, что в передающей части аппаратуры спектр каждого первичного сигнала преобразуется несколько раз прежде, чем занять свое место в линейном спектре. Такое же многократное преобразование, но в обратном порядке осуществляется в приемной части аппаратуры.

Большинство типов многоканальной аппаратуры рассчитано на число каналов, кратное двенадцати. При формировании первичной группы (ПГ) спектр каждого из двенадцати первичных сигналов, занимающих полосы 0,3 - 3,4 кГц, с помощью соответствующих несущих частот переносится в полосу 60 - 108 кГц. Оборудование 12-канальной группы является индивидуальным оборудованием для большинства типов многоканальной аппаратуры. Общая полоса частот 60 - 108 кГц подается дальше на групповое оборудование передачи [13].

Последующие ступени преобразования предназначены для создания более крупных групп каналов: 60-канальной (вторичной) группы (ВГ), 300-канальной (третичной) группы (ТГ) и т.д. Полосы частот 60 - 108 кГц каждой из пяти первичных групп при помощи групповых преобразователей частоты перемещаются в соответствующую данной группе полосу 60-канальной группы. Полосовые фильтры образуют общую полосу частот ВГ 312 - 552

кГц. По аналогии с ВГ строится схема 300-канальной группы, занимающей полосу от 812 до 2044 кГц [13].

Типовая абонентская телефонная линия состоит из пары проводов, проложенных от телефонной розетки до распределительной коробки (РК). От нее она идет далее по многопарному кабелю до распределительного щита (РЩ), а затем - по многопарному бронированному кабелю до АТС. Между АТС прокладываются симметричные или коаксиальные высокочастотные кабели.

Использование тех или иных средств для перехвата информации, передаваемой по телефонным линиям связи, будет определяться возможностью доступа к линии связи.

Для перехвата информации с различных типов кабелей используются разные типы устройств:

для симметричных высокочастотных кабелей - устройства с индукционными датчиками;

для коаксиальных высокочастотных кабелей - устройства непосредственного (гальванического) подключения;

для низкочастотных кабелей - устройства непосредственного (гальванического) подключения, а также устройства с индукционными датчиками, подключаемыми к одному из проводов.

Перехват информации с обычных абонентских двухпроводных телефонных линий может осуществляться или путем непосредственного контактного подключения к линиям, или с использованием простых малогабаритных индуктивных датчиков, подключаемых к одному из проводов абонентской линии. Факт контактного подключения к линии связи легко обнаружить. При подключении индукционного датчика целостности оплетки кабеля не нарушается, параметры кабеля не изменяются и обнаружить факт подключения к линии в этом случае практически невозможно.

Информация, перехватываемая с телефонной линии, может записываться на диктофон или передаваться по радиоканалу с использованием телефонных передатчиков, которые часто называют телефонными закладками или телефонными ретрансляторами.

Телефонные закладки могут быть установлены последовательно в разрыв одного из телефонных проводов, параллельно или через индуктивный датчик.

При последовательном включении питание закладки осуществляется от телефонной линии, что обеспечивает неограниченное время ее работы. Однако закладку с

последовательным подключением довольно легко обнаружить за счет изменения параметров линии и в частности падения напряжения. В ряде случаев используется последовательное подключение с компенсацией падения напряжения, но реализация этого требует наличия дополнительного источника питания.

Телефонные закладки с параллельным подключением к линии могут питаться или от телефонной линии, или от автономных источников питания. Чем выше входное сопротивление закладки, тем незначительнее изменение параметров линии и тем труднее ее обнаружить. Особенно трудно обнаружить закладку, подключенную к линии через высокоомный адаптер сопротивлением более 18-20 МОм. Однако такая закладка должна иметь автономное питание.

Наряду с контактным подключением возможен и бесконтактный съем информации с телефонной линии. Для этих целей используются закладки с миниатюрными индукционными датчиками. Такие закладки питаются от автономных источников питания и установить факт подключения их к линии даже самыми современными средствами практически невозможно, так как параметры линии при подключении не меняются.

Перехваченную информацию телефонные закладки передают по радиоканалу. В качестве антенны может использоваться телефонный провод. Для передачи информации наиболее часто используются VHF (метровый), UHF (дециметровый) и GHz (ГГц) диапазоны длин волн и частотная широкополосная (WFM) или узкополосная (NFM) модуляция сигнала.

Для повышения скрытности используются цифровые сигналы с фазовой или частотной манипуляцией, передаваемая информация может кодироваться различными методами.

Дальность передачи информации при мощности излучения от 10 до 30 мВт в зависимости от вида модуляции и типа используемого приемника может составлять от 100 до 500 м [12].

Передача информации (работа на излучение) начинается в момент поднятия трубки абонентом. Однако встречаются закладки, производящие запись информации в цифровой накопитель и передающие ее по команде.

Телефонные закладки выполняются или в виде отдельного модуля, или камуфлируются под элементы телефонного аппарата, например, конденсатор, телефонный или микрофонный капсюли, телефонный штекер, розетку и т.д.

Телефонные закладки могут быть установлены: в корпусе телефонного аппарата, телефонной трубке или телефонной розетке, а также непосредственно в тракте телефонной линии [12].

Возможность установки телефонной закладки непосредственно в телефонной линии имеет важное значение, так как для перехвата телефонного разговора нет необходимости проникать в помещение, где находится один из абонентов. Телефонные закладки могут быть установлены или в тракте телефонной линии до распределительной коробки, находящейся, как правило, на одном этаже с помещением, где установлен контролируемый аппарат, или в тракте телефонной линии от распределительной коробки до распределительного щитка здания, располагаемого обычно на первом этаже или в подвале здания.

При питании от телефонной линии время работы закладки не ограничено. При использовании автономных источников питания время работы закладки составляет от нескольких десятков часов до нескольких недель.

Способы применения телефонных закладок определяются возможностью доступа в помещение, где установлен контролируемый телефонный аппарат.

Для перехвата факсимильных передач используются специальные комплексы типа РК1 1100, подключаемые к двухпроводной абонентской линии (рис. 3.10) [12].

Типовая система перехвата факсимильных передач размещается в стандартном дипломате, может питаться как от сети переменного тока, так и от встроенных батарей, подключается к линии через высокоомный адаптер, поэтому практически невозможно определить факт подключения, позволяет автоматически распознавать речевое и факсимильное сообщение, записывать передаваемые сообщения, обладает высокой помехоустойчивостью и адаптируется к изменению параметров линии и скорости передачи информации. Система позволяет непрерывно контролировать работу на прием и передачу нескольких факсов [12].

Регистрация перехваченных сообщений может осуществляться в нескольких видах: регистрация по строкам в реальном масштабе времени; распечатка по строкам с одновременной записью в запоминающее устройство; печать на выходные устройства записанной информации; запись информации в запоминающее устройство без печати.

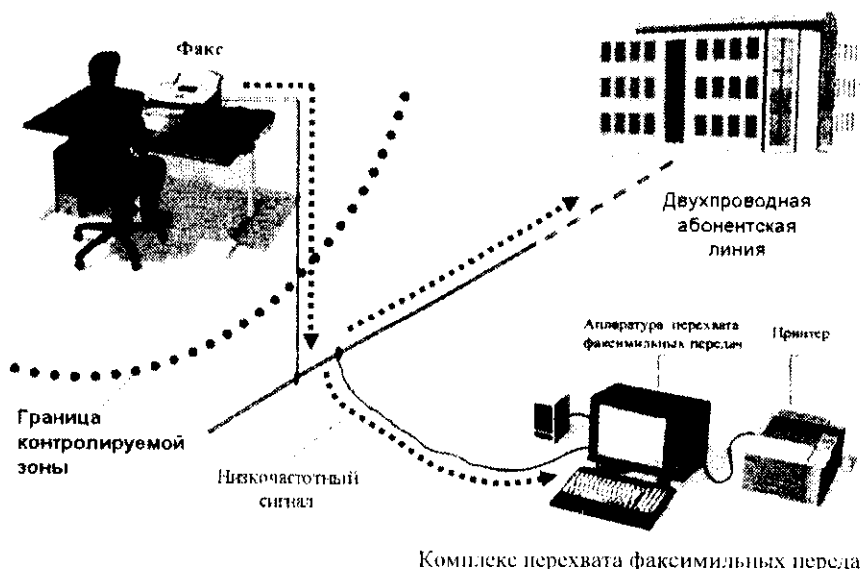


Рис. 3.10. Схема перехвата факсимильных передач

Кроме записи перехваченных сообщений такая система записывает служебную информацию о характере передаваемых сообщений, нестандартных режимах работы факса, поисках и методах (приемах) криптографии.

Программное обеспечение системы позволяет моделировать приемник факсимильного аппарата с расширенными возможностями по визуальному анализу регистрируемых сигналов и заданию параметров демодуляции в случаях, когда автоматическая демодуляция является неудовлетворительной.

Наряду с перехватом факсимильных передач возможен также перехват данных, передаваемых в сети Интернет [12].

При подключении к Интернету через абонентскую телефонную линию наиболее часто используются современные технологии DSL (доступ по *цифровой абонентской линии*).

При этом доступ организуется следующим образом (рис.3.11) [12]. Телефонный сигнал, пропущенный через фильтр с полосой 4 кГц, смешивается с компьютерным сигналом, прошедшим через модем. Модемы DSL отличаются от телефонных значительно большим диапазоном частот. Если телефонные модемы работают в полосе стандартного телефонного канала (0,3 - 3,4 кГц), то частотная

полоса, занимаемая DSL, составляет сотни кГц - единицы МГц. Суммарный сигнал (с телефона и с компьютера) поступает в абонентскую линию и передается на АТС. Там, в свою очередь, телефонный сигнал выделяется фильтром нижних частот (4 кГц) и подается на телефонный коммутатор, а компьютерный сигнал попадает на модем и затем направляется в мультимедийную сеть.

Существующие технологии DSL делятся на две подгруппы: симметричного и асимметричного доступа. Симметричные технологии применяются, как правило, в корпоративном секторе, тогда как асимметричные – предназначены для предоставления услуг доступа к мультимедийной сети отдельным абонентам. Различные технологии уплотнения абонентских линий обозначаются собственными аббревиатурами: ADSL, HDSL, RADSL, SHDSL, VDSL. Все они представляют собой разные способы передачи цифровых потоков (цифровизации), совместно с голосовыми сигналами, по абонентской линии (Subscriber Line, SL).

В зависимости от способа передачи линейного сигнала различают (см. табл. 3.1) [12]:

- системы DSL с последовательной передачей сигналов под названием «системы модуляции одной несущей» (Single Carrier Modulation, SCM), где используются способы кодирования 2B1Q, CAP и др.;

- системы с параллельной передачей сигналов на нескольких несущих частотах, так называемые «системы со многими несущими» (Discrete Multitone, DMT). Их применяют в асимметричных DSL.

Симметричные технологии DSL, такие, как HDSL, SDSL, SHDSL, являются системами с одной несущей (SCM). Асимметричные DSL, такие, как ADSL, ADSL2, ADSL2+, используют модуляцию нескольких несущих (DMT).

Система уплотнения HDSL обеспечивает режим передачи со скоростью около 2 Мбит/с в обе стороны по одной или двум парам проводов на расстояние до 10 км. Оборудование ADSL, наоборот, предназначено для асимметричной передачи со скоростями от 6 до 8 Мбит/с - в сторону абонента и 840 Кбит/с или меньше - в сторону узла связи. RADSL отличается от упомянутых выше технологий тем, что поддерживает либо симметричный режим со скоростью около 1 Мбит/с, либо асимметричный - при скорости к абоненту до 8 Мбит/с. SDSL обозначает, как правило, симметричную передачу по одной паре; IDSL - модификацию ISDN (цифровая сеть с интеграцией служб) [12].

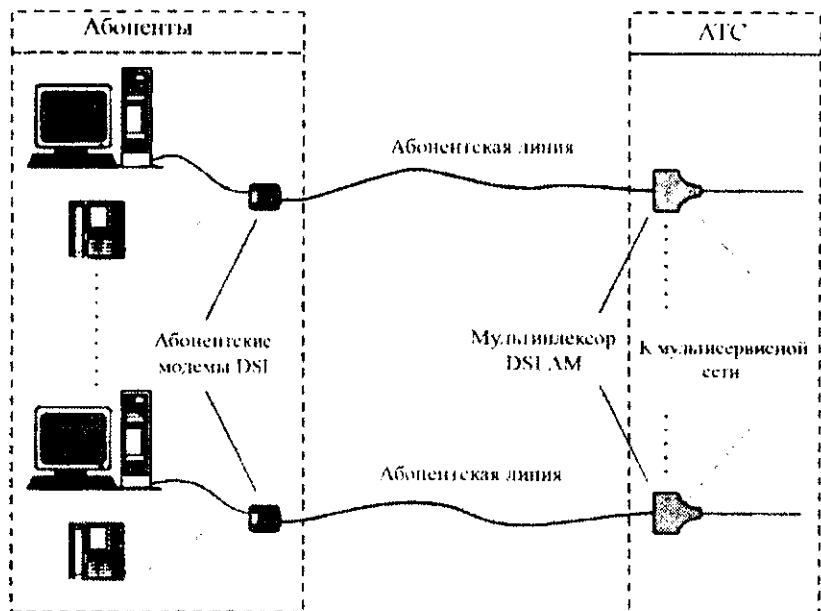


Рис. 3.11. Широкополосный доступ по DSL

Таблица 3.1

Виды систем DSL

Тип	Линейное кодирование	Количество используемых пар	Скорость (Мбит/с)
HDSL	2B1Q или CAP	1, 2 или 3	2
SDSL	2B1Q или CAP	1	От 0,384 до 2,3
SHDSL	TC-PAM	1 или 2	От 0,192 до 2,3
ADSL	DMT	1	До 0,8 - «восходящая», до 8 - «нисходящая»
VDSL	QAM или DMT	1	Для асимметричной до 6,5 - «восходящая», до 52 - «нисходящая»; для симметричной - от 13 до 26

Новый стандарт VDSL2 (Very-High-Bit rate DSL, сверхвысокоскоростная DSL) обеспечивает скорость передачи до 100 Мбит/с в обоих направлениях. Такая скорость реализуется в случае, когда расстояние от распределительного узла до пользователя не превышает 350 м. При больших расстояниях скорость VDSL2 падает, но не опускается ниже 12 Мбит/с [12].

С подобной скоростью VDSL2 может функционировать при таком удалении, на котором сегодня работает ADSL, т. е. от 4,5 до 5 км [12].

Для достижения скорости 100 Мбит/с на расстоянии 350 м частотный диапазон системы расширен с 12 до 30 МГц [12].

Способы перехвата информации, передаваемой по каналам радиосвязи

Одним из наиболее распространенных способов передачи больших объемов информации на значительные расстояния является многоканальная радиосвязь с использованием радиорелейных линий и космических систем связи. Радиорелейная связь представляет собой связь с использованием промежуточных усилителей-ретрансляторов. Трассы многоканальных радиорелейных линий, как правило, прокладываются вблизи автомобильных дорог, для облегчения обслуживания удаленных ретрансляторов, которые размещаются на господствующих высотах, мачтах и т.п. В космических системах связи информация передается через спутники-ретрансляторы, находящиеся на геостационарных и высоких эллиптических орбитах.

Для перехвата информации, передаваемой с использованием радиорелейных линий и космических систем связи, используются наземные центры и посты радиоразведки, космические системы радио- и радиотехнической разведки, а также стратегические самолеты-разведчики типа RC-135.

Наиболее оптимальным для передачи информации в настоящее время признано использование сетей подвижной радиосвязи общего пользования (транкинговых, сотовых), так как они предоставляют абонентам больше разнообразных услуг (от образования диспетчерской связи отдельных служб до автоматического выхода на абонентов городских и междугородных телефонных сетей), а также позволяют резко поднять пропускную способность сети. В этих сетях любой абонент имеет право доступа к любому незанятому каналу сети и подчиняется только дисциплине массового обслуживания.

Под термином «транкинг» понимается метод равного доступа абонентов сети к общему выделенному пучку каналов, при котором конкретный канал закрепляется для каждого сеанса связи индивидуально. В зависимости от распределения нагрузки в системе, связь между отдельными абонентами в такой сети осуществляется в основном через специальную приемопередающую базовую станцию. Радиус действия базовой станции в городских условиях в зависимости от частотного диапазона сети, расположения и мощности базовой и абонентских станций колеблется от 8 до 50 км [13].

Наиболее широко используемые транкинговые системы радиосвязи представлены в таблице 3.2 [12].

Таблица 3.2

Характеристики транкинговых систем радиосвязи

Система (стандарт)	Наименование характеристик			
	Полосы частот, МГц	Ширина полосы частот канала, кГц (разнос каналов)	Число каналов (вместе с каналами управления)	Примечание
Алтай	337 -341 301-305	25	180	Аналоговая
Smarttrunk	146-174 403 - 470	150/250	16	Однозоновая. Аналоговая
MPT 1327	146-174 300 -380 400 -520	12,5/25	24	Многозоновая. Аналоговая. Цифровое управление
EDACS	30-300 800;900	25/30 12,5	20	Аналоговая (речь). Цифровая (речь, данные)
TETRA	380-400	25	200	Цифровая (TDMA) π/4 DQPSK

Основные потребители услуг транкинговой связи - это правоохранительные органы, службы экстренного вызова, вооруженные силы, службы безопасности частных компаний, таможня, муниципальные органы, службы охраны и сопровождения.

банки и службы инкассации, аэропорты, энергетические подстанции, строительные фирмы, больницы, лесничества, транспортные компании, железные дороги, промышленные предприятия.

Особое место среди сетей связи общего пользования занимает сотовая радиотелефонная связь [13]. Сотовый принцип топологии сети с повторным использованием частот во многом решил проблему дефицита, частотного ресурса и в настоящее время является основным в создаваемых системах подвижной связи общего пользования.

Структура сотовых сетей представляет собой совокупность примыкающих друг к другу и имеющих различные частоты связи небольших зон обслуживания, которые могут охватывать обширные территории. Поскольку радиус одной такой зоны (ячейки, соты) не превышает, как правило, нескольких километров, в сотах, непосредственно не примыкающих друг к другу, возможно повторное использование без взаимных помех одних и тех же частот.

В каждой из ячеек размещается стационарная (базовая) приемопередающая радиостанция, которая связана проводной связью с центральной станцией сети. Число частотных каналов в сети обычно не превышает 7...10, причем один из них организационный. Переход абонентов из одной зоны в другую не сопряжен для них с какими-либо перестройками аппаратуры. Когда абонент пересекает границу зоны, ему автоматически предоставляется другая свободная частота, принадлежащая новой ячейке.

На федеральном уровне в основном используются цифровые стандарты GSM и CDMA.

Основные технические характеристики связи сотовых систем связи стандарта GSM представлены в табл. 3.3 [12].

Стандарт GSM тесно связан со всеми современными стандартами цифровых сетей, в первую очередь с ISDN (Integrated Services Digital Network) и IN (Intelligent Network).

В стандарте GSM применён дуплексный канал с разносом 45 МГц. Полоса частот, выделенных для сети, разделяется на частотные каналы, разнос каналов 200 кГц, это позволяет создать 124 частотных канала. Значения несущих частот для передачи $F_{\text{про}}$, МГц, и приёма $F_{\text{прм}}$, МГц, можно определить по формулам [12, 13]:

$$F_{\text{про}} = 890,2 + 0,2 (n - 1) \quad (3.1)$$

$$F_{\text{прм}} = F_{\text{про}} + 45, \quad (3.2)$$

где n – номер несущей частоты ($n = 1, 2, \dots, 124$).

Основные технические характеристики сотовых систем связи стандарта GSM

Система (стан- дарт)	Наименование характеристик				
	Полосы частот, МГц	Ширина полосы частот канала, кГц	Макси- мальная мощност ь, Вт	Число кана- лов	Класс сигналов, тип модуляции
GSM	890-915 (ПС) 935 - 960 (БС)	200	300 (БС)	124	200KF7W GMSK (манипуляция с минималь- ным частотным сдвигом)
DCS- 1800	1710-1785 (ПС) 1805-1880 (БС)	200	Менее 1 (ПС)	374	200KF7W GMSK

Примечание: ПС - подвижная станция, БС – базовая станция.

В стандарте GSM используется узкополосный многостанционный доступ с временным разделением каналов (TDMA). В структуре TDMA кадра содержится 8 временных позиций на каждой из 124 несущих [12].

Для защиты от ошибок в радиоканалах при передаче информационных сообщений применяется блочное и сверточное кодирование с перемежением. Повышение эффективности кодирования и перемежения при малой скорости перемещения подвижных станций достигается медленным переключением рабочих частот (SFH) в процессе сеанса связи со скоростью 217 скачков в секунду [12].

Для борьбы с интерференционными замираниями принимаемых сигналов, вызванными многолучевым распространением радиоволн в условиях города, в аппаратуре связи используются эквалайзеры, обеспечивающие выравнивание импульсных сигналов со среднеквадратическим отклонением времени задержки до 16 мкс. Система синхронизации рассчитана на компенсацию абсолютного времени задержки сигналов до 233 мкс,

что соответствует максимальной дальности связи или максимальному радиусу ячейки (соты) 35 км [12].

В стандарте GSM выбрана гауссовская манипуляция с минимальным сдвигом (GMSK) с величиной нормированной полосы, равной 0,3. Индекс частотной манипуляции - 0,5. При этих параметрах уровень излучения в соседнем канале не превысит минус 60 дБ.

Обработка речи осуществляется в рамках принятой системы прерывистой передачи речи (DTX), которая обеспечивает включение передатчика только при наличии речевого сигнала и отключение передатчика в паузах и в конце разговора. В качестве речепреобразующего устройства выбран речевой кодек с регулярным импульсным возбуждением, долговременным предсказанием и линейным предикативным кодированием с предсказанием (RPE/LTP-LTP-кодек). Общая скорость преобразования речевого сигнала - 13 кбит/с [12].

В стандарте GSM достигается высокая степень безопасности передачи сообщений, так как осуществляется шифрование сообщений по алгоритму шифрования с открытым ключом (RSA).

Система DCS-1800 работает в диапазоне 1800 МГц. Ядро стандарта DCS-1800 составляют более 60 спецификаций стандарта GSM, поэтому данный стандарт часто называют стандартом GSM-1800. Стандарт рассчитан на ячейки радиуса порядка 0,5 км в районах плотной городской застройки и до 8 км в условиях сельской местности [12].

Стандарт CDMA (Code Division Multiple Access) является стандартом систем сотовой связи на основе метода множественного доступа с кодовым разделением каналов. В системе используются шумоподобные сигналы с расширенным спектром.

В системах CDMA используются несколько стандартов [12].

Стандарт IS-95 является стандартом системы сотовой связи на основе метода множественного доступа с кодовым разделением каналов CDMA. Безопасность передачи информации являются свойством технологии CDMA, поэтому операторам этих сетей не требуется специального оборудования шифрования сообщений. Система CDMA построена по методу прямого расширения спектра частот на основе использования 64 видов последовательностей, сформированных по закону функций Уолша [12].

Основные характеристики стандарта IS-95 приведены в таблице 3.4. Структура CDMA-сетей отличается от GSM-сетей.

Таблица 3.4

Основные характеристики стандарта CDMA IS-95

<i>Наименование характеристики</i>	<i>Значение характеристики</i>
Диапазон частот передачи МС	824,040-848,860 МГц
Диапазон частот передачи БС	869,040-893,970 МГц
Вид модуляции несущей частоты	QPSK(BTS), O-QPSK(MS) (квадратурная фазовая модуляция)
Ширина спектра излучаемого сигнала: • по уровню минус 3 дБ • по уровню минус 40 дБ	1,25 МГц 1,50 МГц
Тактовая частота ПСП М-функции	1,2288 МГц
Количество каналов БС на 1 несущей частоте	1 пилот-канал 1 канал синхронизации 7 каналов персонального вызова 55 каналов связи
Количество каналов МС	1 канал доступа 1 канал связи
Скорость передачи данных: ♦ в канале синхронизации ♦ в канале перс. Вызова и доступа ♦ в каналах связи	1200 бит/с 9600, 4800 бит/с 9600, 4800, 2400, 1200 бит/с
Кодирование в каналах передачи БС	Сверточный код $R=1/2$, $K=9$
Кодирование в каналах передачи МС	Сверточный код $R=1/3$, $K=9$
Требуемое для приема отношение энергии бита информации	6 - 7 дБ
Максимальная эффективная излучаемая мощность БС	50 Вт
Максимально эффективная излучаемая мощность МС	6,3- 10 Вт

Каждая ячейка использует всю полосу частот, поэтому проблемы с повторным использованием частот не возникает. Использование секторизации, в отличие от обычных сотовых сетей, позволяет существенно увеличить количество абонентов, обслуживаемых одной

ячейкой, за счет увеличения соотношения сигнал/шум. Емкость CDMA-сетей превышает емкость аналоговых узкополосных сотовых сетей в 8-10 раз [12].

Система CDMA IS-95 рассчитана на работу в диапазоне частот 800 МГц. Одному оператору может быть выделен максимальный диапазон частот 12,5 МГц. Полоса частот канала связи составляет 1,25 МГц, в которой может разместиться 41 узкополосный канал (по 30 МГц) [12].

В пределах одного частотного канала организовано 64 кодовых канала. На линии базовая станция - абонентская станция адресным признаком кодового канала служит одна из 64 взаимно ортогональных функций Уолша, а на линии абонентская станция - базовая станция - квазиортогональные длинные псевдослучайные последовательности.

Особенностью стандарта является то, что для успешного осуществления связи необходимо, чтобы мощность на входе приёмника базовой станции и мощность на входе приёмника мобильной станции отличалась не более чем на ± 1 дБ. При не соблюдении этого требования сигналы одних абонентов будут маскироваться более мощными сигналами других.

Для того чтобы абонентская станция могла установить соединение с сетью, она должна обмениваться сигналами управления с базовой станцией на заранее определённой дуплексной паре частот.

Для передачи речевых сообщений выбрано речепреобразующее устройство с алгоритмом CELP со скоростью преобразования 8000 бит/с (9600 бит/с в канале). Возможны режимы работы на скоростях 4800, 2400, 1200 бит/с [12].

В стандарте IS-95 используется раздельная обработка отраженных сигналов, приходящих с разными задержками, и последующее их весовое суммирование, что значительно снижает отрицательное влияние явления многолучевости.

Стандарт CDMA2000 является дальнейшим развитием стандарта IS-95. В документах Lucent Technologies встречается обозначение IS- 2000.

Стандарты семейства CDMA2000 не требуют организации отдельной полосы частот и в ходе их эволюционного развития от IS-95 могут быть реализованы во всех частотных диапазонах, используемых системами сотовой подвижной связи (450, 700, 800, 900, 1700, 1800, 1900, 2100 МГц).

В России в настоящее время используется одна из разновидностей технологии CDMA - CDMA-450, использующая диапазон 450 МГц.

Потребителям уже сейчас предлагаются системы фиксированной связи, основанные на технологии широкополосной CDMA (В-CDMA), которая использует радиоканалы шириной 5, 10 и даже 20 МГц и рабочие радиочастоты в диапазонах 2, 3 и 4 ГГц.

Для перехвата информации в сетях сотовой и транкинговой связи используются стационарные, перевозимые и переносимые комплексы радиоразведки.

Стационарные и перевозимые пассивные комплексы перехвата сотовой связи могут перехватывать и записывать до 100 и более телефонных абонентов одновременно, а портативные (переносимые) - до 4-х [12].

Дальность перехвата переговоров абонентов может составлять до 10 км и более.

Комплексы радиоразведки и специальные комплексы перехвата систем сотовой связи находятся на вооружении специальных служб ведущих иностранных государств и обеспечивают перехват и декодирование сообщений, передаваемых с использованием любых систем связи, включая стандарты GSM и CDMA. При этом перехват информации в сетях сотовой связи может осуществляться как пассивными, так и активными комплексами разведки.

Типовой пассивный портативный комплекс перехвата сотовой связи стандарта GSM позволяет осуществлять перехват и прослушивание как открытых, так и зашифрованных голосовых каналов [12].

Активный комплекс перехвата представляет собой виртуальную базовую станцию (ВБС) внутри сети GSM, использующую для работы перехваченные из реальной сети параметры соты, которая мобильными телефонами аутентифицируется в качестве обычной базовой станции [12].

При включении ВБС на сравнительно небольшом расстоянии от контролируемого мобильного аппарата (не более 500 м), последний регистрируется ею согласно стандарту GSM. При регистрации определяются идентификаторы IMSI и IMEI, которые заносятся в базу данных комплекса перехвата.

Наряду с системами транкинговой и сотовой связи для передачи информации широко используются системы беспроводных телефонов (БПТ).

На первоначальном этапе своего развития они предназначались для замены шнура телефонной трубки беспроводной линией радиосвязи с целью обеспечения большей мобильности абонента. Дальнейшее развитие этого вида связи, особенно переход на цифровые методы обработки информации, значительно расширило область применения БПТ [13].

В системах БПТ аналогового (стандарты CT-OR, CT-1R) и цифрового (стандарты CT-2R, DECT) типов, наиболее часто используемых в жилых помещениях и небольших учреждениях, применяются БПТ индивидуального пользования, состоящие из базовой станции (БС), подключенной к городской телефонной сети, и переносного радиотелефонного аппарата (РТА) [13]. При использовании БПТ в крупных компаниях в качестве внутриучрежденческого средства связи организуются разветвленные сети маломощных радиотелефонов, принцип работы которых аналогичен сотовым сетям. В этих системах используются в основном цифровые методы обработки сигнала (наиболее часто используется стандарт DECT), обеспечивающие более стойкое шифрование передаваемых сообщений.

Как аналоговые, так и цифровые беспроводные телефоны работают в дуплексном режиме по нескольким каналам, причем выбор канала осуществляется автоматически из числа незанятых. Дальность действия сертифицированных радиопередатчиков БПТ, мощность излучения которых не превышает 10 мВт, в зависимости от типа аппаратуры и условий эксплуатации составляет 25 - 50 м.

Мощность несертифицированных передатчиков БПТ может составлять 0,35 - 1,2 Вт и более, при этом дальность их действия может составлять до нескольких километров.

Перечень частотных полос, выделенных для БПТ на условии ограничения максимальной выходной мощности 10 мВт и на вторичной основе, т.е. без каких либо гарантий чистоты эфира, представлены в таблице 3.5.

Стандарт DECT получил наиболее широкое применение в сетях и системах радиотелефонной связи. Основные параметры стандарта приведены в таблице 3.6 [12].

Таблица 3.5

Перечень частотных полос, выделенных для беспроводных телефонов мощностью до 10 мВт

<i>Стандарт</i>	<i>Частотный диапазон, МГц</i>
CT-0R	30-31/39-40
CT-1R	814-815/904-905
CT-2R	864 - 868,2
DECT	1880- 1900

Таблица 3.6

Характеристики стандарта DECT

<i>Наименование характеристики</i>	<i>Значение характеристики</i>
Диапазон частот, МГц	1880-1900
Полоса пропускания канала, МГц	1,728
Количество несущих частот	10
Вид разделения каналов	12TDMA/10FDMA
Вид разделения дуплекса	временное разделение каналов
Скорость модуляции в канале, кбод	1152
Скорость передачи речи, кбит/с	32
Пиковая мощность, мВт	250
Вид модуляции	GMSK, $\pi/2$ - DBPSK, $\pi/4$ - DQPSK, $\pi/8$ -DBPSK
Скорость передачи основным видом модуляции (GMSK), кбит/с R=300 м R=3 км R=30 км	516,8 508 436
Полоса частот сигнала по уровню, МГц, -30 дБ -26 дБ -20 дБ	3,0 2,3 1,7
Защитный интервал, мкс	54
Количество дуплексных каналов в системе	120

Стандарт допускает использование 10 частотных каналов с центральными частотами 1881,792; 1883,52; 1885,248; 1886,976; 1888,704; 1890,432; 1892,16; 1893,888; 1895,616 и 1897,344 МГц, определяемыми выражением [12]

$$f_{II} = 1897,334 - 1,728 \cdot N, \quad (3.3)$$

где $N=0,1...9$.

В каждом из десяти частотных каналов для организации 12 телефонных каналов используется кадр множественного доступа к каналу с временным разделением сигналов. Разделение дуплексных каналов происходит по времени, поэтому кадр содержит 24 временных интервала, 12 из которых используются на передачу, 12 - на приём данных. Соответственно, общее количество каналов связи 120 [12].

Основным видом модуляции принята гауссовская частотная модуляция с минимальным сдвигом. Для расширения возможностей стандарта предусмотрены дополнительные виды модуляции: относительная двоичная фазовая модуляция ($\pi/2$ -DBPSK), относительная квадратурная фазовая ($\pi/4$ -DQPSK), относительная фазовая ($\pi/4$ -DBPSK).

Дополнительные виды модуляции обеспечивают увеличение скорости передачи при той же занимаемой полосе частот, однако обладают меньшей помехоустойчивостью.

При пиковой мощности 250 мВт средняя мощность излучения с учётом защитных интервалов составляет 10 мВт.

На базе стандарта DECT возможно создание микросотовых систем связи и прежде всего для применения совместно с учрежденческими АТС (УАТС) в офисах с высокой плотностью размещения персонала и интенсивным трафиком.

Микросотовая система DECT включает в себя абонентские терминалы, базовые станции и контроллер и позволяет осуществлять телефонные вызовы, передавать голосовые и факсимильные сообщения, предоставлять услуги ISDN. Стандарт предусматривает также возможность передачи данных с базовой скоростью 32 кбит/с, а путем объединения нескольких радиоканалов можно передавать трафик приложений реального времени (например, видеoinформацию) с общей скоростью до 640 кбит/с [12].

Контроллер системы беспроводного доступа стандарта DECT обеспечивает управление работой базовых станций (до нескольких десятков БС), преобразует аналоговые или цифровые (64 кбит/с) сигналы телефонии в сжатый поток 32 кбит/с и направляет их к

базовым станциям, а также обеспечивает подключение к проводной сети (например, УАТС) с помощью цифровых потоков 2 Мбит/с.

В зависимости от платформы, на которой реализована система DECT, одновременно может обеспечиваться от 120 до 20000 речевых каналов. Одна БС может одновременно поддерживать голосовые соединения на 4-12 абонентских терминалах [12].

Дальность связи внутри зданий может составлять от 20 до 50 м, а на открытой местности - до 300 м. Максимальное удаление базовой станции от АТС составляет 600 - 2000 м [12].

Перехват информации, передаваемой с использованием радиотелефонов, работающих в аналоговых стандартах CT-0R, CT-1R, может осуществляться обычным сканирующим приемником. Для перехвата информации, передаваемой с использованием радиотелефонов, работающих в цифровых стандартах CT-2R, DECT, используются специальные комплексы радиоразведки (см. рис. 3.12). При этом дальность перехвата переговоров абонентов может составлять более 5 км.

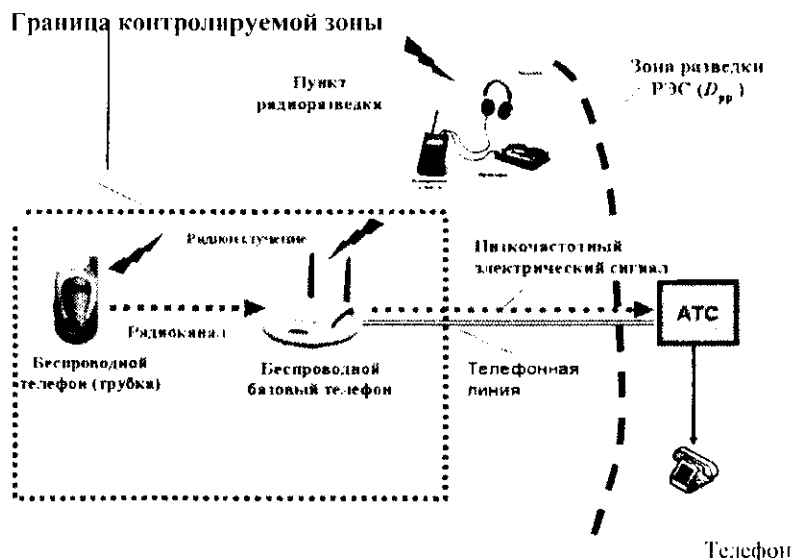


Рис. 3.12. Перехват информации, передаваемой с использованием радиотелефона, портативными комплексами радиоразведки

Таблица 3.7

**Полосы частот, выделяемые для систем
беспроводного доступа**

<i>Полосы радиочастот, МГц</i>	<i>Ширина полосы, МГц</i>
1275 – 1527	252
2200 - 2483,5	283,5
2500 – 2700	200
3400-3450; 3500- 3550	100
5150- 5350	200
5470 – 6425	955
10150- 10300; 10500- 10650	300
24549-25109; 25557-26117	1120
28052.5 - 28444,5; 29060,5 - 29425,5	784
40500 - 43500	3000

Таблица 3.8

**Полосы частот, одобренные для использования
в системах беспроводного доступа решениями ГКРЧ**

<i>Полосы радиочастот, МГц</i>	<i>Ширина полосы, МГц</i>	<i>Решение ГКРЧ</i>
1787,5 - 1802,5	15	От 23.10.2006 № 06-17-03-001
2400 - 2483,5	83,5	Внутриофисные СБД - от 6.12.2004 № 04-03-04-003. Уличные СБД - от 28.11.2005 №05-10-01 -001
2500-2530; 2560-2570 2620-2630; 2660-2670 2680 - 2690	70	От 4.09.2006 № 06-16-03-001
3400 – 3450 3500 - 3550	100	От 23.12.2002 №23/3. От 1.12.2003 №30/4. От 28.11.2005 №05-10-01 -001
5150 – 5350 5650 - 6425	975	От 23.12.2002 №23/5. От 28.11.2005 № 05-10-01-001

В последние годы для передачи информации все более широко используются сети радиодоступа.

Полосы частот, выделяемые на территории РФ для систем беспроводного доступа, представлены в табл. 3.7 и 3.8 [12].

Наиболее широкое распространение из беспроводных сетей радиодоступа нашли сети радиодоступа стандартов Wi-Fi и WiMax.

Wi-Fi (Wireless Fidelity) - или стандарт 802.11 используется для организации беспроводных компьютерных сетей и точек высокоскоростного доступа в Интернет.

Сети Wi-Fi строятся на основе небольших базовых станций (точек доступа или хот-спотов), присоединенных к сети фиксированной связи. Радиус покрытия одной точки доступа достигает 100 м. Для работы с Wi-Fi необходимо иметь ноутбук, КПК или смартфон, поддерживающие эту технологию, либо специальную Wi-Fi-карту для мобильных компьютеров и телефонов. Скорость передачи данных в сетях Wi-Fi достигает 54 Мбит/с. В стандарте IEEE 802.11 используется диапазон частот 2.40 - 2.4835 (см. таблицу 3.9) [12].

Разновидностями стандарта 802.11 являются стандарты 802.11a, 802.11b и 802.11g. Их сравнительные характеристики приведены в табл. 3.10 [12].

WiMAX (Worldwide Interoperability for Microwave Access) – или стандарт 802.16-2004 обеспечивает широкополосную связь на площади радиусом более 30 км и пропускной способностью, сравнимой с кабельными соединениями - до 10 Мбит/с и более. Технология WiMAX позволяет работать в любых условиях, в том числе – в условиях плотной городской застройки.

Таблица 3.9

Частоты каналов IEEE 802.11 (Wi-Fi)

Номер канала	Центральная частота, ГГц	Диапазон частот, ГГц
1	2,412	2,401-2,423
2	2,417	2,406-2,428
3	2,422	2,411-2,433
4	2,427	2,416-2,438
5	2,432	2,421-2,443
6	2,437	2,426-2,448
7	2,442	2,431-2,453

Примечание: Каждый канал занимает частотный диапазон в 22 МГц

Оборудование сетей WiMAX функционирует в нескольких частотных каналах шириной 10 МГц в пределах диапазона от 2 до 11 ГГц.

Столь широкий разброс диапазонов выбран для учета специфики большинства стран мира. Так, в Северной Америке для WiMAX используются участки в диапазонах 2,5 и 5 ГГц, а в Западной и Восточной Европе - 3,5 и 5 ГГц [12].

Таблица 3.10

**Характеристики стандартов беспроводных сетей
стандартов 802.11**

<i>Наименование характеристики</i>	<i>Стандарт</i>			
	<i>802.11</i>	<i>802.11b</i>	<i>802.11a</i>	<i>802.11g</i>
Полоса частот, МГц	83,5	83,5	300	83,5
Диапазон частот, ГГц	2,40-2,4835	2,40-2,4835	5,15-5,35 5,725 -5,825	2,40-2,4835
Количество не- пересекающихся каналов	3	3	12	3
Скорость передачи, Мбит/с	1,2	1,2,5,5, 11,22	6,9,12,18,24 36,48,54	1,2,5,5,11, 22, 6, 9, 12, 18, 24, 36, 48, 54
Метод	DSSS	DSSS	OFDM	DSSS, OFDM
Тип модуляции	DBPSK, DQPSK	DBPSK, DQPSK	BPSK, QPSK, QAM	BPSK, QPSK, QAM

В целом базовые характеристики следующего стандарта 802.16 предусматривают дальность действия до 50 км, покрытие с возможностью работы вне прямой зоны видимости, в перспективе - пиковую скорость обмена данными до 70 Мбит/с на сектор одной базовой станции при том, что типовая базовая станция будет иметь до 6 секторов покрытия [12].

Для соединения базовой станции с пользователем необходимо лишь устанавливаемое в помещении абонентское оборудование. С него сигнал поступает по стандартному Ethernet-кабелю либо непосредственно на один компьютер, либо на точку доступа

стандарта 802.11, или в локальную проводную сеть стандарта Ethernet.

Одна базовая станция в сети стандарта IEEE 802.16 может обслуживать большое количество пользователей и предоставлять им разного рода услуги.

В настоящее время на стадии разработки находится стандарт IEEE 802.16e, который рассматривает вопросы роуминга между сетями различных беспроводных стандартов, чтобы пользователь без ущерба для сеанса связи мог переходить из беспроводных сетей стандарта IEEE 802.11 в сети IEEE 802.16 и обратно.

Основные характеристики стандартов 802.16 приведены в табл. 3.11 [12].

Таблица 3.11

Характеристики стандартов 802.16

<i>Наименование характеристики</i>	<i>Стандарт</i>	
	<i>802.16-2004</i>	<i>802.16e</i>
Частотный диапазон	2-12 ГГц	2-6 ГГц
Тип сети	Стационарная	Подвижная
Зона покрытия	Вне зоны прямой видимости	Вне зоны прямой видимости
Радиус зоны покрытия	4-6 км	4-6 км
Скорость передачи данных	До 75 Мбит/с при полосе 20 МГц	До 15 Мбит/с при полосе 5 МГц
Модуляция	OFDM 256, OFDMA, BPSK, QPSK, 16QAM, 64QAM	OFDM 256, OFDMA, BPSK, QPSK, 16QAM, 64QAM
Ширина канала	Избирательная ширина от 1.25 до 20 МГц	Избирательная ширина от 1.25 до 20 МГц

В стандарте 802.16 были выделены три типа физического уровня соединений, различающихся методом модуляции сигнала:

WirelessMAN-SC - физический уровень с одной несущей частотой; WirelessMAN-OFDM - ортогональное частотное разделение на 256 каналов с мультиплексированием. Реализация множественного доступа к среде передачи данных происходит за счет технологии временного разделения (Time Division Multiple Access, TDMA);

WirelessMAN-OFDMA - ортогональное масштабируемое частотное разделение каналов с мультиплексированием. Используется разделение на 2048 поднесущие частоты. Коллективный доступ к среде передачи данных реализуется за счет объединения нескольких поднесущих частот в один канал передачи и его выделения конкретному получателю (OFD Multiple Access, OFDMA).

Физический уровень WirelessMAN-SC предназначен для применения в зоне прямой видимости приемника и получателя сигналов. Остальные два уровня, основанные на ортогональном частотном разделении каналов, могут использоваться для построения сетей по топологии «точка-многоточие» в условиях отсутствия прямой видимости.

Из двух OFDM-уровней уровень WirelessMAN-OFDM несколько проще для реализации с технической точки зрения и потому пользуется большей поддержкой со стороны производителей оборудования.

В случае ортогонального частотного разделения на 256 каналов с мультиплексированием (WirelessMAN-OFDM) используется 256 отсчетов IFFT, из которых 192 поднесущие являются информационными, то есть применяются для передачи данных, 8 поднесущих предназначены для измерения характеристик канала связи и используются для передачи пилотных символов (pilot symbols), а остальные 56 поднесущих частот могут применяться для организации защитных интервалов, длительность которых составляет $1/4$, $1/8$, $1/16$ или $1/32$ длительности OFDM-сигнала.

Ширина канала связи может быть различной и изменяется от 1,25 до 20 МГц.

Ортогональное частотное разделение каналов с мультиплексированием типа WirelessMAN-OFDMA представляет собой масштабируемое частотное разделение каналов, то есть количество поднесущих в данном случае, не фиксировано и может составлять 512, 1024 и 2048. В зависимости от количества поднесущих, меняется и ширина канала, и количество подканалов (таблица 3.12) [12].

Базовые станции (Base Station, BS), как правило, применяют мультиплексирование с разделением по времени (TDM), при котором каждой абонентской станции (Subscriber Station, SS) последовательно выделяются временные слоты. Абоненты же разделяют общий канал

посредством схемы множественного доступа с разделением по времени (Time Division Multiple Access, TDMA).

Таблица 3.12

Характеристики OFDMA

Наименование характеристик	Значение характеристик		
Ширина канала	5 МГц	10 МГц	20 МГц
Количество поднесущих	512	1024	2048
Количество подканалов	32	64	128
Ширина подканала	156 кГц	156 кГц	156 кГц
Длительность символа	101 мкс	101 мкс	101 мкс
Расстояние между поднесущими	11,2 кГц	11,2 кГц	11,2 кГц
Длительность циклического префикса	11,2 мкс	11,2 мкс	11,2 мкс

Еще один новый стандарт для мобильного доступа к данным - 802.20. В отличие от WiMax, рассчитанного на работу в городах при ограниченном числе базовых станций, стандарт 802.20 имеет больше сходства с обычными сотовыми системами и предназначен для быстродействующих мобильных подключений на скоростях свыше 1 Мбит/с [12].

Беспроводное соединение становится все более популярным и на бытовом уровне. Соединения между двумя мобильными устройствами (например, телефонами и КПК) поддерживают стандарты IrDA и Bluetooth [12].

IrDA (инфракрасную связь) начали использовать для беспроводного соединения бытовых устройств в начале 90-ых. В 1993 г. была создана организация IrDA (Infrared Data Association), выработавшая общий стандарт инфракрасной связи IrDA (Infrared Direct Access).

Собственно ИК-порт, расположенный на устройствах, внешне выглядит как окошко из темной прозрачной пластмассы, за которым находятся светодиод и фотодиод. Цифровой сигнал направляется на светодиод одного устройства и посылается в виде инфракрасного излучения на фотодиод другого устройства. Скорость передачи данных составляет от 2,4 кбит/с до 115 кбит/с, а между компьютерными ИК-портами может увеличиваться до 4 Мбит/с.

ИК-порт позволяет связывать только два устройства. При этом есть целый ряд условий: расстояние между устройствами не

должно быть более 1 м, между ними не должно быть никаких преград, угол, под которым устройства находятся по отношению друг к другу, не должен превышать 60 градусов.

Стандарт Bluetooth (IEEE 802.15.1) помогает соединять между собой самые разные бытовые приборы, включая мобильные телефоны, КПК, персональные компьютеры и т.д. От IrDA отличается принципиально тем, что в нем для соединения используются радиосредства. Основные характеристики стандарта IEEE 802.15.1 (Bluetooth) приведены в табл. 3.13 [12].

Таблица 3.13

Характеристики стандарта IEEE 802.15.1 (Bluetooth)

<i>Наименование характеристики</i>	<i>Значение характеристики</i>
Диапазон частот, МГц	2400...2483,5
Максимальная эквивалентная изотропно излучаемая мощность для наружных устройств с малым радиусом действия, мВт	Менее 2,5
Максимальная эквивалентная изотропно излучаемая мощность для внутриофисных устройств, мВт	Менее 100
Способ расширения спектра сигнала	Псевдослучайная перестройка частоты
Номиналы несущих частот, МГц	2402+N, где N=0,...,76

Bluetooth-устройство содержит небольшой чип - приемопередатчик, работающий в диапазоне 2,4 ГГц. Соединение двух Bluetooth- устройств позволяет передавать данные на скоростях от 420 до 720 кбит/с на расстояние до 10/100 м. Всего Bluetooth может одновременно связать до восьми устройств.

На территории России без разрешения и регистрации разрешено использование оборудования мощностью излучения, не превышающую 2,5 мВт.

Для реализации множественного доступа к каналу в стандарте применена псевдослучайная перестройка частоты. Общая полоса частот 2,4 - 2,483 ГГц делится на 79 каналов шириной 1 МГц. Перестройка частоты происходит путём изменения частоты несущей с номинала одного канала на номинал другого в соответствии с

задаваемой в стандарте псевдослучайной последовательностью. Скорость изменения частоты 1600 скачков в секунду (длительность передачи на одной частоте, соответственно, 0,625 мс). В стандарте применяется временное разделение каналов [12].

Для перехвата информации, передаваемой в сетях беспроводного доступа, используются специальные активные комплексы перехвата, включающие приемопередающий модуль, ноутбук (или карманный ПК) и специальное программное обеспечение. Перехват может вестись со стационарных и подвижных постов радиоразведки, а также отдельными лицами с использованием портативных средств (см. рис. 3.13).

Типовой портативный комплекс перехвата сетей беспроводного доступа позволяет проводить идентификацию РЭС, работающих в любых стандартах, и осуществлять перехват информации, передаваемой в сети.

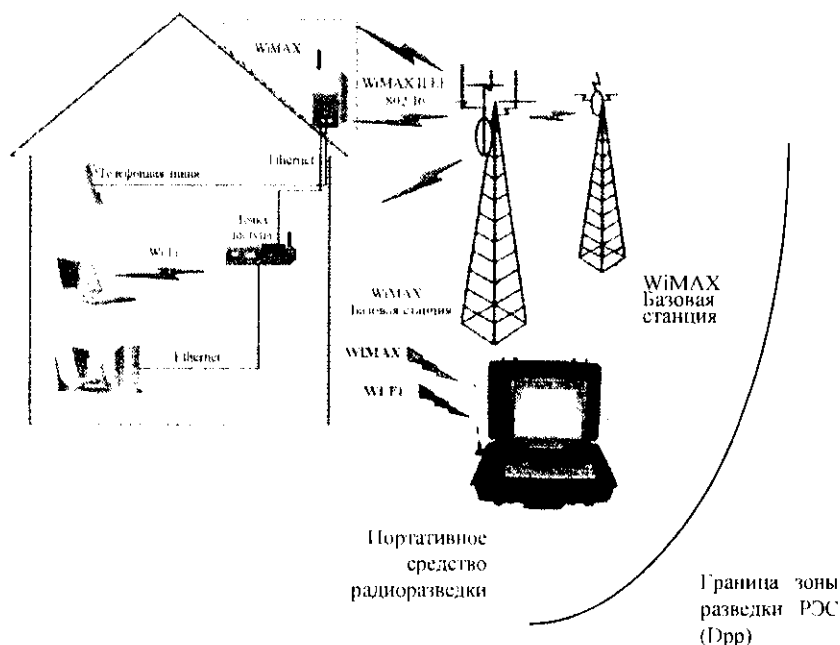


Рис. 3.13. Перехват информации, передаваемой в сетях беспроводного доступа

При ведении радиоразведки осуществляется не только перехват и анализ сообщений (информационных потоков), передаваемых по каналам радиосвязи, но и измерение характеристик сигналов РЭС, а при необходимости - и определение их местоположения.

Определение местоположения РЭС осуществляется угломерным (триангуляционным) и разностно-дальномерным методами.

Способы скрытого видеонаблюдения и съемки

Специальные службы иностранных государств давно и широко применяют различные оптические и оптико-электронные приборы, позволяющие вести скрытое наблюдение и регистрировать информацию днем и ночью при различных метеоусловиях.

Основная задача видеонаблюдения - слежение за действиями отдельных лиц и передвижением транспортных средств, а также проводимых с их участием мероприятий. Но средства видеонаблюдения и съемки могут использоваться и в целях добывания информации, обрабатываемой на объектах информатизации и в выделенных помещениях. При этом могут решаться следующие задачи разведки:

- перехват (видеозапись) информации, выводимой на экран монитора ПЭВМ или демонстрируемой с использованием видеопроектора;
- видеозапись действий оператора при вводе информации с клавиатуры (например, с целью вскрытия паролей доступа к автоматизированной системе);
- перехват информации, содержащейся на плакатах и стендах, вывешенных в помещении;
- перехват информации, содержащейся в документах, находящихся на рабочих столах в помещении;
- документирование (видеозапись) действий лиц в помещении; документирование (видеозапись) переговоров, ведущихся в помещении и т.д.

Аппаратура видеонаблюдения и съемки может быть установлена в автомашинах или близлежащих зданиях, находящихся за пределами контролируемой зоны, а также непосредственно на объекте информатизации или в помещении. Для съемки объектов

могут привлекаться малогабаритные беспилотные дистанционно - управляемые вертолеты (ПБВ).

При ведении разведки из-за пределов контролируемой зоны используется длиннофокусная аппаратура. Для видеонаблюдения в дневное время используются традиционные оптические приборы, такие, как бинокли, бинокюляры, подзорные трубы и телескопы, а для съемки - цифровые камеры. Для ведения разведки ночью применяются специальные телевизионные камеры, работающие при низком уровне освещения, приборы ночного видения и тепловизоры.

Для скрытой установки внутри помещений используются миниатюрные видеокамеры с объективами типа пинхоул (pin-hole). Пинхоулы бывают двух типов - «игольное ушко» и «вынесенный зрачок». В качестве приемников оптического излучения (ПОИ) используются матрицы на базе приборов с зарядовой связью (ПЗС). Объектив и приемник излучения, как правило, конструктивно объединяются в одно устройство.

Видеоизображения с телевизионных камер могут записываться на цифровые накопители или передаваться на приемный пункт по радиоканалу с использованием специальных видеопередатчиков. Как правило, одновременно с видеоизображением передается и звук.

3.3. Защита компьютерной информации от несанкционированного доступа

3.3.1. Компьютерная безопасность: современные требования, подходы

3.3.1.1. Введение

Современными тенденциями развития информационных технологий является ярко выраженный переход в сторону создания корпоративных информационных систем. При этом основной характеристикой этих систем является разграничение доступа сотрудникам корпорации к информационным и иным ресурсам ИС. Причем данные тенденции проявляются практически для всех уровней иерархии современных информационных технологий, начиная с архитектурного уровня в целом (Internet и Intranet), включая сетевые технологии (например, IP v.6.0 и IP Sec), и заканчивая уровнем общесистемных средств (ОС, СУБД) и приложений [18].

Масштабы применения и приложения информационных технологий стали таковы, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем, остро встает проблема защиты циркулирующей в системах информации от несанкционированного доступа. Статистика фактов несанкционированного доступа к информации (НСД) показывает, что большинство современных информационных систем достаточно уязвимо с точки зрения безопасности. И это несмотря на устойчивую тенденцию к усилению встроенных в них механизмов защиты.

Другой аспект — это возможность локализации угроз корпоративной информации, так как большая их часть связана с угрозой НСД, исходящей от самих сотрудников компании. При этом следует учитывать и сетевые ресурсы (прежде всего в составе ЛВС), к которым сотрудник имеет доступ со своего компьютера в рамках своей служебной деятельности.

В связи с этим именно компьютер (особенно находящийся в составе сети) следует в первую очередь рассматривать в качестве объекта защиты, а конечного пользователя — в качестве ее наиболее вероятного потенциального нарушителя. Как следствие, *под сомнение ставится обоснованность концепции реализованной системы защиты в современных универсальных ОС*. Эта система защиты заключается в

построении распределенной схемы администрирования механизмов защиты, элементами которой, помимо администратора, выступают пользователи, имеющие возможность назначать и изменять права доступа к создаваемым ими файловым объектам.

На практике сегодня существует два подхода к обеспечению компьютерной безопасности:

1. Использование только встроенных в ОС и приложения средств защиты.

2. Применение, наряду со встроенными, дополнительных механизмов защиты. Этот подход заключается в использовании так называемых технических средств добавочной защиты - программных, либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты.

Существующая статистика ошибок, обнаруженных в ОС, а также сведения о недостаточной эффективности встроенных в ОС и приложения механизмов защиты, заставляет специалистов сомневаться в достижении гарантированной защиты от НСД, при использовании встроенных механизмов, и все большее внимание уделять средствам добавочной защиты информации.

Поэтому требуется системное изложение проблем защиты компьютерной информации, а также теоретических основ применения добавочных средств защиты компьютерной информации.

Факт очевиден - *важнейшим условием защищенности компьютерной информации является квалификация администраторов безопасности и сотрудников эксплуатирующих служб*, которая, по крайней мере, не должна уступать квалификации злоумышленников. В противном случае не помогут никакие средства защиты (то же относится и к разработчикам средств защиты и защищенных информационных систем).

3.3.1.2. Основные требования к защите компьютерной информации и анализ защищенности современных операционных систем

Основные требования к защите компьютерной информации

Используемые в настоящее время на практике подходы к защите компьютерной информации определяются следующими характеристиками:

- формализованными требованиями к набору и параметрам механизмов защиты, регламентирующими современные требования к обеспечению компьютерной безопасности (требованиями,

определяющими что должно быть);

- реальными механизмами защиты, реализуемыми при защите компьютерной информации. К таковым относятся прежде всего средства защиты ОС, т.к. большинство приложений используют встроенные в ОС механизмы защиты (определяющими, что есть);

- существующей статистикой угроз компьютерной безопасности - существующими успешными атаками на информационные компьютерные ресурсы (определяющими, насколько эффективно то, что есть и дающими оценку достаточности требований к тому, что должно быть).

Поэтому анализ существующих подходов к защите компьютерной информации проводят следующим образом [18]. Сначала рассматривают формализованные требования, то есть требования соответствующие нормативным документам, регламентирующие требования к защите компьютерной информации от несанкционированного доступа. Далее рассматривают механизмы защиты, реализованные в современных ОС и анализируют, в какой мере ими выполняются требования соответствующих нормативных документов.

Такой анализ необходим, чтобы определиться с причиной низкой защищенности компьютерной информации. Если встроенные в современные ОС механизмы защиты в полной мере соответствуют формализованным требованиям к ним, то, следовательно, эти требования необходимо усиливать. В противном случае необходимо усиливать механизмы защиты с целью выполнения соответствующих требований.

Следующий шаг - рассмотрение и анализ существующей статистики угроз компьютерной информации и определение причины уязвимости современных ОС. На основе этого, а также на основе нормативных документов определяются дополнительные требования к защите компьютерной информации, которые не выполняются встроенными в ОС механизмами защиты.

Затем рассматриваются непосредственно методы и механизмы, которые должны быть реализованы средствами добавочной защиты в дополнение к встроенным в ОС защитным механизмам. Особое внимание уделим методам и механизмам добавочной защиты, позволяющим функционально расширять встроенные механизмы защиты в предположении возможности потенциальных (еще не известных из опубликованной статистики)

угроз. Естественно, что будут иными архитектурные и технические решения по реализации добавочной защиты.

Классификация требований к системам защиты.

В общем случае следует говорить о необходимости учета двух (дополняющих друг друга) групп требований к системе защиты.

Первая группа требований (необходимые требования) заключается в необходимости реализации системой защиты формализованных мер безопасности (то есть мер, заданных соответствующими нормативными документами в области защиты информации).

Формализованные требования к необходимым механизмам защиты информационных систем, в части их защиты от НСД, сформулированы в руководящих документах ФСТЭК России (для нашей страны). Для других стран эти требования сформулированы в документах соответствующих организаций, например:

«Оранжевая книга», Критерии оценки надежных компьютерных систем Министерства обороны США;

Согласованные критерии оценки безопасности информационных технологий. Information Technology Security Evaluation Criteria, ITSEC, Европейские страны.

Данные документы носят общий характер. В них не в полной мере предусматривается классификация объектов, для которых должна быть реализована защита. Да это и невозможно в рамках одного документа. В частности, эти документы предъявляют единые требования для всех семейств ОС. И это несмотря на то, что ОС различных семейств имеют принципиально отличные принципы построения, а значит, для них различаются и способы НСД.

В указанных руководящих документах не дается рекомендаций по способам построения и администрирования защищенных систем, то есть не сказано, как их строить. В этих документах лишь сформулированы требования (что должно быть реализовано) к механизмам защиты информации и, отчасти, требования к их количественным характеристикам.

Данный подход к заданию формализованных требований, наверное, в целом оправдан, т.к. невозможно учесть в нормативных документах все тонкости построения и проектирования средств защиты сложных информационных систем, особенно при существующей динамике их развития.

Формализованные требования носят основополагающий характер - в том смысле, что в них формализованы требования к

основополагающим механизмам защиты информации. Поэтому их возможное со временем изменение не может быть сколько-нибудь существенным без появления новых научно обоснованных технологий защиты информации. Само же изменение неизбежно и естественно ввиду меняющейся со временем статистики угроз информационно-безопасности.

Вторая группа требований (дополнительные требования) заключается в необходимости учета существующей (текущей) статистики угроз для конкретного типа защищаемого объекта, а также потенциально возможных угроз (на данный момент отсутствующих в опубликованных угрозах, но гипотетически возможных). Необходимость этой группы требований обусловлена тем, что формализованные требования не могут учитывать все возможные угрозы объектам всех типов, требующих защиты. Также формализованные требования не могут соперничать по скорости обновления со скоростью изменения статистики угроз.

С учетом сказанного может быть сделан вывод о целесообразности рассмотрения условий необходимости и достаточности требований к защите информации. Необходимыми являются формализованные требования, определяемые соответствующими нормативными документами в области защиты информации. Достаточной является совокупность формализованных и дополнительных требований, формулируемых на основе анализа текущей статистики угроз защищаемому объекту, а также потенциально возможных угроз (на данный момент отсутствующих в опубликованных угрозах, но гипотетически возможных).

Формализованные требования к защите информации от НСД

Как ранее указывалось, общие подходы в системах защиты целесообразно рассматривать относительно соответствия их принятым формализованным требованиям. Эти требования предъявляются к механизмам защиты, которые в той или иной мере реализуются современными ОС, приложениями и добавочными средствами защиты.

Защиту информации от НСД в нашей стране на сегодняшний день регламентируют нормативные документы [16, 17] ФСТЭК России:

- *Требования к защите средств вычислительной техники (СВТ)* [16], формализуют условия защищенности отдельно взятого средства - ОС, СУБД, приложения.
- *Требования к защите автоматизированных систем (АС)* [17].

формализуют условия защищенности объекта с учетом:

- совокупности механизмов защиты, реализуемых установленными на защищаемом объекте средствами, включая ОС, СУБД (если есть), приложениями, добавочными механизмами защиты (если есть);

- дополнительных организационных мер, принимаемых для безопасного функционирования АС.

При этом, как правило, приложения используют механизмы защиты ОС. Что касается СУБД, то механизмы защиты СУБД дополняют защитные механизмы ОС, так как возникает необходимость защиты дополнительных объектов доступа - «таблиц». Действительно, для ОС защищаемыми файловыми объектами являются: логические диски (тома), каталоги, файлы. При работе с базами данных сложность обусловлена тем, что таблицы различных пользователей, к которым должен разграничиваться доступ, могут находиться в одном файле. Таким образом, получается, что в общем случае невозможно управлять доступом к базам данных только механизмами защиты ОС. Однако это относится только к СУБД. Остальные приложения обычно довольствуются защитными механизмами ОС. То есть, можно сказать, что, *как правило, все механизмы защиты автоматизированных систем (АС) по умолчанию реализуются собственно ОС.*

В общем случае формализованные требования к обеспечению защиты компьютерной информации от НСД (т.е. к средствам защиты ОС) задаются формализованными требованиями к защите средств вычислительной техники (СВТ) [16]. Однако, в связи с вышесказанным, будем для оценки эффективности защитных механизмов ОС также использовать формализованные требования из документа [17], применяемые к автоматизированным системам (АС). Это следует делать, потому что именно защитные механизмы ОС призваны обеспечивать необходимый уровень защиты автоматизированной системы (АС) в целом (требования к АС несколько расширены по сравнению с требованиями к СВТ, а требования к СВТ в большей части детализированы).

Аналогичные рассуждения могут быть проведены и относительно средства добавочной защиты. При этом, во-первых, оно может рассматриваться как отдельное СВТ, выполняющее формализованные требования документа [16]. В этом случае встроенные в ОС механизмы защиты не должны рассматриваться. А во-вторых, оно может рассматриваться как средство в составе АС

(наряду с механизмами ОС, дополняя их). В этом случае встроенные в ОС и добавочные механизмы защиты должны в совокупности выполнять формализованные требования документа [17]. Кроме того, для определенных классов защиты встроенные механизмы защиты должны быть сертифицированы.

Рассмотрим формализованные требования к защите компьютерной информации АС в соответствии с документом [17]. При этом будем рассматривать первую группу АС (в соответствии с используемой в [17] классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причем не все пользователи имеют право доступа ко всей информации АС.

Первая группа АС содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, а также различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала [17].

Требования к АС первой группы сведены в табл. 3.14. При этом используются следующие обозначения:

«—» нет требований к данному классу;

«+» есть требования к данному классу.

Как видим, рассматриваемыми требованиями выделяются следующие основные группы механизмов защиты:

- механизмы управления доступом;
- механизмы регистрации и учета;
- механизмы криптографической защиты;
- механизмы контроля целостности.

Отметим, что первая группа «Подсистема управления доступом» является основополагающей для реализации защиты от НСД, т.к. именно механизмы защиты данной группы призваны непосредственно противодействовать несанкционированному доступу к компьютерной информации.

Остальные же группы механизмов реализуются в предположении, что механизмы защиты первой группы могут быть преодолены злоумышленником. В частности они могут использоваться:

**Формализованные требования к защите
информации от НСД**

№ п/п	Подсистема и требования	Классы				
		1Д	1Г	1В	1Б	1А
1.	Подсистема управления доступом					
1.1.	Идентификация, проверка подлинности и контроль доступа субъектов:					
	- в систему	+	+	+	+	+
	- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+	+	+	+
	- к программам	-	+	+	+	+
	- к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
1.2.	Управление потоками информации	-	-	+	+	+
2.	Подсистема регистрации и учета					
2.1.	Регистрация и учет:					
	- входа (выхода) субъектов доступа в (из) систему (узел связи)	+	+	+	+	+
	- выдачи печатных (графических) выходных документов	-	+	+	+	+
	- запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
	- доступа программ субъектов доступа к защищаемым файлам, включая их создание, удаление, передачу по линиям и каналам связи	-	+	+	+	+
	- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
	- изменения полномочий субъектов доступа	-	-	+	+	+
	- создаваемых защищаемых объектов доступа	-	-	+	+	+

Продолжение табл. 3.14

№ п/п	Подсистема и требования	Классы				
		1Д	1Г	1В	1Б	1А
2.2.	Учет носителей информации	+	+	+	+	+
2.3.	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	+	+	+
2.4.	Сигнализация попыток нарушения защиты	-	+	+	+	+
3.	<i>Криптографическая подсистема</i>					
3.1.	Шифрование конфиденциальной информации	-	-	-	+	+
3.2.	Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов на разных ключах)	-	-	-	-	+
3.3.	Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+
4.	<i>Подсистема обеспечения целостности</i>					
4.1.	Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2.	Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3.	Наличие администратора (службы) защиты информации в АС	-	-	+	+	+
4.4.	Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5.	Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6.	Использование сертифицированных средств защиты	-	-	+	+	+

- для контроля действий пользователя - группа «Подсистема регистрации и учета»;

- для противодействия возможности прочтения похищенной информации (например, значений паролей и данных) - группа «Криптографическая подсистема»;

- для контроля осуществленных злоумышленником изменений защищаемых объектов (исполняемых файлов и файлов данных) при осуществлении к ним НСД и для восстановления защищаемой информации из резервных копий - группа «Подсистема обеспечения целостности».

Кроме того, эти группы механизмов могут использоваться для проведения расследования по факту НСД.

Рассмотрим более подробно требования различных групп (согласно [17]), а также соответствующие им основные подходы к защите компьютерной информации, реализуемые на сегодняшний день на практике. При этом имеет смысл остановиться лишь на двух классах:

- 1Г, задающим необходимые (минимальные) требования для обработки конфиденциальной информации;

- 1В, задающим необходимые (минимальные) требования для обработки информации, являющейся собственностью государства и отнесенной к категории секретной.

Требования к защите конфиденциальной информации.

Подсистема управления доступом должна удовлетворять следующим требованиям:

1. Идентифицировать и проверять подлинность субъектов доступа при входе в систему. Причем это должно осуществляться по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

2. Идентифицировать терминалы, ЭВМ, узлы компьютерной сети, каналы связи, внешние устройства ЭВМ по их логическим адресам (номерам).

3. По именам идентифицировать программы, тома, каталоги, файлы, записи и поля записей.

4. Осуществлять контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета должна:

1. Регистрировать вход (выход) субъектов доступа в систему (из системы), либо регистрировать загрузку и инициализацию операционной системы и ее программного останова. При этом в параметрах регистрации указываются:

• дата и время входа (выхода) субъекта доступа в систему (из

системы) или загрузки (останова) системы:

- результат попытки входа - успешная или неуспешная (при НСД);

- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- код или пароль, предъявленный при неуспешной попытке.

Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения АС.

2. Регистрировать выдачу печатных (графических) документов на «твердую» копию. При этом в параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

- идентификатор субъекта доступа, запросившего документ.

3. Регистрировать запуск (завершение) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. При этом в параметрах регистрации указывается:

- дата и время запуска;

- имя (идентификатор) программы (процесса, задания);

- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный - несанкционированный).

4. Регистрировать попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указывается:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная - несанкционированная);

- идентификатор субъекта доступа;

- спецификация защищаемого файла.

5. Регистрировать попытки доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. При этом в параметрах регистрации

указывается:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная, несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого объекта [логическое имя (номер)].

6. Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

7. Регистрировать выдачу (приемку) защищаемых носителей.

8. Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. При этом очистка должна производиться однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности должна:

1. Обеспечивать целостность программных средств системы защиты информации от НСД (СЗИ НСД), обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

- целостность программной среды обеспечивается использованием трансляторов с языка высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

2. Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должны предусматриваться контроль доступа в помещение АС посторонних лиц, а также наличие надежных препятствий для несанкционированного проникновения в помещение АС и хранилище носителей информации. Особенно в нерабочее время.

3. Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

4. Иметь в наличии средства восстановления СЗИ НСД. При этом предусматривается ведение двух копий программных средств СЗИ НСД, а также их периодическое обновление и контроль работоспособности

Требования к защите секретной информации.

Подсистема управления доступом должна:

1. Идентифицировать и проверять подлинность субъектов доступа при входе в систему. Причем это должно осуществляться по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

2. Идентифицировать терминалы, ЭВМ, узлы компьютерной сети, каналы связи, внешние устройства ЭВМ по их логическим адресам (номерам).

3. По именам идентифицировать программы, тома, каталоги, файлы, записи и поля записей.

4. Осуществлять контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

5. Управлять потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета должна:

1. Регистрировать вход (выход) субъектов доступа в систему (из системы) либо регистрировать загрузку и инициализацию операционной системы и ее программного останова. При этом в параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа - успешная или неуспешная (при НСД);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

2. Регистрировать выдачу печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества страниц. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи (успешный - весь объем, неуспешный).

3. Регистрировать запуск (завершение) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указывается:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный).

4. Регистрировать попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указывается:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: (успешная, неуспешная - несанкционированная);
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющих доступ к файлам;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.).

5. Регистрировать попытки доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указывается:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная — несанкционированная);
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- имя программы (процесса, задания, задачи),

осуществляющих доступ к файлам:

- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.).

6. Регистрировать изменения полномочий субъектов доступа, а также статуса объектов доступа. В параметрах регистрации указывается:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения.

7. Осуществлять автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.

8. Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

9. Проводить учет защищаемых носителей с регистрацией их выдачи (приема) в специальном журнале (картотеке).

10. Проводить несколько видов учета (дублирующих) защищаемых носителей информации.

11. Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Причем очистка должна осуществляться двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

12. Сигнализировать о попытках нарушения защиты.

Подсистема обеспечения целостности должна:

1. Обеспечивать целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

- целостность программной среды обеспечивается использованием трансляторов с языка высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

2. Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должно предусматриваться постоянное наличие охраны на территории здания и помещений, где находится АС. Охрана должна производиться с помощью

технических средств охраны и специального персонала, а также с использованием строгого пропускного режима и специального оборудования в помещении АС.

3. Предусматривать наличие администратора или целой службы защиты информации, ответственных за ведение, нормальное функционирование и контроль работы СЗИ НСД.

Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

4. Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью специальных программных средств не реже одного раза в год.

5. Иметь в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

6. Использовать только сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

Различия требований и основополагающих механизмов защиты от НСД.

Сравним две рассмотренные выше группы требований и их особенности для защиты информации различных категорий (конфиденциальной и секретной).

Ключевыми механизмами защиты, образующими основную группу механизмов защиты от НСД («Подсистема управления доступом») являются:

идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия;

контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Дополнительным требованием и принципиальным отличием при защите секретной информации является то, что механизмом защиты должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации.

Все три перечисленных механизма являются основополагающими. Связаны они следующим образом: все права доступа к ресурсам (разграничительная политика доступа к ресурсам)

задаются для конкретного субъекта доступа (пользователя). Поэтому субъект доступа (пользователь) должен быть идентифицирован при входе в систему, соответственно, должна быть проконтролирована его подлинность. Обычно это делается путем использования секретного слова - пароля.

Чтобы было понятно дальнейшее изложение материала, остановимся более подробно на рассмотрении механизмов, реализующих основу защиты компьютерной информации от НСД - разграничительную политику доступа к ресурсам. Таковыми механизмами являются механизмы контроля доступа. Более подробно речь об этом пойдет в четвертой части книги. Однако уже сейчас необходимо понимать, о чем идет речь.

Следуя формализованным требованиям к системе защиты информации, основу реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является *дискреционный механизм управления доступом*. При этом реализуется дискреционная модель доступа к ресурсам. Принципы организации и функционирования этой модели будут рассмотрены позднее. Сейчас лишь отметим, что при дискреционной модели права доступа задаются матрицей доступа, элементами которой являются разрешенные права доступа субъекта к объекту. Что касается контроля доступа, то он осуществляется непосредственно путем анализа прав доступа к объекту запрашивающего доступ субъекта. При этом анализируется, есть ли в матрице информация о разрешении доступа данного субъекта к данному объекту, или нет.

При защите секретной информации в основе разграничительной политики доступа (РПД) к ресурсам должен лежать помимо дискреционного (дискреционная модель управления доступом), мандатный механизм управления доступом (мандатная модель управления доступом). Его также рассмотрим позднее.

В рамках мандатного механизма каждому субъекту (пользователю, приложению и т.д.) и каждому объекту (файлу, каталогу и т.д.) ставятся в соответствие специальные классификационные метки. Посредством этих меток субъектам и объектам назначаются классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Сам контроль и управление доступом осуществляется путем сопоставления классификационных меток субъекта и объекта

доступа, отражающих их место в соответствующей иерархии. В общих чертах в этом и заключается мандатный механизм управления доступом. То есть право доступа дается на основе сравнения меток объекта и субъекта. При этом, чтобы субъект получил доступ к объекту, его уровень конфиденциальности должен быть не ниже уровня конфиденциальности объекта.

Требования к практической реализации дискретного и мандатного механизмов управления доступом, как и сами эти методы, будут рассмотрены позднее. Тем не менее, уже сейчас стоит отметить, что эти требования тесно связаны с требованиями к обеспечению целостности и очистки памяти.

Для системы защиты выполнение требования «Должна быть обеспечена целостность программных средств системы защиты информации от НСД (СЗИ НСД), обрабатываемой информации, а также замкнутость программной среды» обеспечивает возможность противодействия скрытым действиям пользователей, направленных на получение НСД к информации в обход РПД. При этом не важно, чем будет пользоваться потенциальный нарушитель - программами собственной разработки, всевозможными отладочными средствами или иным ПО. Далее будет показано, что обеспечение замкнутости программной среды - это важнейший механизм защиты в части противодействия скрытым атакам.

Требование к очистке памяти «Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов)» обуславливает невозможность доступа пользователя к остаточной информации. Его необходимость вызвана тем, что при удалении файла на внешнем накопителе системными средствами осуществляется изменение разметки накопителя, но собственно информация остается. Она так и называется «остаточная информация». При этом ввиду того, что остаточная информация уже не является объектом доступа (она соответствующим образом не размечена на диске - не является файлом), дискреционный и мандатный механизмы контроля доступа не могут осуществлять РПД к этой информации. А это значит, что доступ к ней может быть осуществлен в обход подсистемы управления доступом.

Анализ защищенности современных операционных систем.

Принципиальные различия в подходах обеспечения защиты.

Анализируя выполнение современными универсальными ОС требований, задаваемых для класса защищенности автоматизированных систем 1В (защита секретной информации), не имеет смысла в принципе. Для большинства ОС либо полностью не реализуется основной для данных приложений мандатный механизм управления доступом к ресурсам, либо не выполняется его важнейшее требование «Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации».

В связи с этим далее будем говорить лишь о возможном соответствии средств защиты современных ОС классу автоматизированных систем 1Г (защита конфиденциальной информации).

В качестве альтернативных реализаций ОС рассмотрим семейства UNIX и Windows (2000/XP).

Сначала остановимся на принципиальном, даже можно сказать, концептуальном противоречии между реализованными в ОС механизмами защиты и принятыми формализованными требованиями. Концептуальном в том смысле, что это противоречие характеризует не какой-либо один механизм защиты, а общий подход к построению системы защиты.

Противоречие состоит в принципиальном различии подходов (соответственно требований) к построению схемы администрирования механизмов защиты. Как следствие, это коренным образом сказывается на формировании общих принципов задания и реализации политики безопасности на предприятии, распределения ответственности за защиту информации на предприятии, а также на определении того, кого относить к потенциальным злоумышленникам (от кого защищать информацию). То есть сказывается на ключевых вопросах защиты информации.

Для иллюстрации из совокупности формализованных требований к системе защиты конфиденциальной информации (требований к дискреционному механизму управления доступом) рассмотрим следующие два требования [16]:

1. Право изменять правила разграничения доступа (ПРД) должно предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

2. Должны быть предусмотрены средства управления, ограничивающие распространения прав на доступ.

Данные требования жестко регламентируют схему (или модель) администрирования механизмов защиты. Это должна быть централизованная схема, единственным элементом которой выступает выделенный субъект, в частности, администратор (в общем случае следует говорить об администраторе безопасности). При этом конечный пользователь исключен в принципе из схемы администрирования механизмов защиты.

При реализации концепции построения системы защиты, регламентируемой рассматриваемыми требованиями, пользователь не наделяется элементом доверия. Таким образом, он может считаться потенциальным злоумышленником, что и имеет место на практике - этот вопрос будет рассмотрен далее. Ответственным за информационную безопасность на предприятии является доверенное с его стороны лицо - выделенный субъект, в частности, администратор безопасности.

Теперь в общих чертах рассмотрим концепцию, реализуемую в современных универсальных ОС. Здесь «владельцем» файлового объекта, то есть лицом, получающим право на задание атрибутов (или ПРД) доступа к файловому объекту, является лицо, создающее файловый объект. Т.к. файловые объекты создают конечные пользователи, то именно они и назначают ПРД к создаваемым им файловым объектам. Другими словами, в ОС реализуется распределенная схема назначения ПРД, где элементами схемы администрирования являются собственно конечные пользователи.

В данной схеме пользователь должен со стороны предприятия наделяться практически таким же доверием, как и администратор безопасности, при этом нести наряду с ним ответственность за обеспечение компьютерной безопасности. Отметим, что данная концепция реализуется и большинством современных приложений, в частности СУБД, где пользователь может распространять свои права на доступ к защищаемым ресурсам.

Кроме того, не имея в полном объеме механизмов защиты компьютерной информации от конечного пользователя, в рамках данной концепции невозможно рассматривать пользователя в качестве потенциального злоумышленника. А как мы увидим далее, именно с несанкционированными действиями пользователя на защищаемом компьютере (причем как сознательными, так и нет) связана большая часть угроз компьютерной безопасности.

Отметим, что централизованная и распределенная схемы администрирования - это две диаметрально противоположные точки зрения на защиту, требующие совершенно различных подходов к построению моделей и механизмов защиты. Но гарантированную защиту информации можно реализовать только при принятии концепции полностью централизованной схемы администрирования. Это подтверждается известными угрозами ОС.

Возможности моделей, методов и средств защиты будем далее рассматривать применительно к реализации именно концепции централизованного администрирования. Одним из элементов данной концепции является рассмотрение пользователя в качестве потенциального злоумышленника, способного осуществить НСД к защищаемой информации.

Рассмотрим основных механизмах защиты, встроенных в современные универсальные ОС. Сделаем это применительно к возможности реализации ими принятой нами для рассмотрения концепции защиты конфиденциальной информации.

Основные защитные механизмы и недостатки защитных механизмов ОС семейства UNIX

Защита ОС семейства UNIX в общем случае базируется на трех основных механизмах:

- идентификации и аутентификация пользователя при входе в систему;
- разграничении прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа;
- аудит, то есть регистрация событий.

При этом отметим, что для различных клонов ОС семейства UNIX возможности механизмов защиты могут незначительно различаться, однако будем рассматривать ОС UNIX в общем случае, без учета некоторых незначительных особенностей отдельных ОС этого семейства.

Построение файловой системы и разграничение доступа к файловым объектам имеет особенности, присущие данному семейству ОС. Рассмотрим кратко эти особенности. Все дисковые накопители (тома) объединяются в единую ВИРТУАЛЬНУЮ ФАЙЛОВУЮ СИСТЕМУ путем операции монтирования тома. При этом содержимое тома проецируется на выбранный каталог файловой системы. Элементами файловой системы являются также все устройства, подключаемые к защищаемому компьютеру (монтируемые к файловой системе). Поэтому разграничение доступа

к ним осуществляется через файловую систему.

Каждый файловый объект имеет индексный дескриптор (описатель), в котором среди прочего хранится информация о разграничении доступа к данному файловому объекту. Права доступа делятся на три категории: доступ для владельца, доступ для группы и доступ для остальных пользователей. В каждой категории определяются права на чтение, запись и исполнение (в случае каталога - просмотр).

Пользователь имеет уникальный символьный идентификатор (имя) и числовой идентификатор (UID). Символьный идентификатор предъявляется пользователем при входе в систему, числовой используется операционной системой для определения прав пользователя в системе (доступ к файлам и т.д.).

Рассмотрим в общем случае *недостатки реализации системы защиты ОС семейства UNIX* в части невыполнения требований к защите конфиденциальной информации. При этом, прежде всего рассмотрим принципиальные недостатки защиты, напрямую связанные с возможностью НСД к информации.

В ОС семейства UNIX, вследствие реализуемой ею концепции администрирования (не централизованная), *невозможно обеспечить замкнутость (или целостность) программной среды*. Это связано с невозможностью установки атрибута «исполнение» на каталог (для каталога данный атрибут ограничивает возможность «обзора» содержимого каталога). Поэтому при разграничении администратором доступа пользователей к каталогам, пользователь, как «владелец» создаваемого им файла, может занести в свой каталог исполняемый файл и, как его «владелец», установить на файл атрибут «исполнение», после чего запустить записанную им программу. Эта проблема непосредственно связана с реализуемой в ОС концепцией защиты информации.

Не в полном объеме реализуется дискреционная модель доступа, в частности не могут разграничиваться права доступа для пользователя «root» (UID = 0). Т.е. данный субъект доступа исключается из схемы управления доступом к ресурсам. Соответственно все запускаемые им процессы имеют неограниченный доступ к защищаемым ресурсам. Как мы увидим позднее, с этим недостатком системы защиты связано множество атак, в частности:

- несанкционированное получение прав root;
- запуск с правами root собственного исполняемого файла

(локально либо удаленно внедренного). При этом несанкционированная программа получает полный доступ к защищаемым ресурсам и т.д.

Кроме того, в ОС семейства UNIX *невозможно встроенными средствами гарантированно удалять остаточную информацию*. Для этого в системе абсолютно отсутствуют соответствующие механизмы.

Необходимо также отметить, что большинство ОС данного семейства *не обладают возможностью контроля целостности файловой системы*, то есть не содержат соответствующих встроенных средств. В лучшем случае дополнительными утилитами может быть реализован контроль конфигурационных файлов ОС по расписанию, в то время, как важнейшей возможностью данного механизма можно считать контроль целостности программ (приложений) перед их запуском, контроль файлов данных пользователя и др.

Что касается регистрации (аудита), то в ОС семейства Unix *не обеспечивается регистрация выдачи документов на «твердую копию», а также некоторые другие требования к регистрации событий*.

Если же трактовать требования к управлению доступом в общем случае, то при защите компьютера в составе ЛВС, необходимо управление доступом к хостам (распределенный пакетный фильтр). Однако *встроенными средствами защиты некоторых ОС семейства UNIX управление доступом к хостам не реализуется*.

Из приведенного анализа видно, что многие механизмы, необходимые с точки зрения выполнения формализованных требований, большинством ОС семейства UNIX не реализуется в принципе, либо реализуется лишь частично.

Основные защитные механизмы и недостатки защитных механизмов ОС семейства WINDOWS (2000/XP).

Теперь кратко остановимся на основных механизмах защиты, реализованных в ОС семейства Windows, и проведем анализ защищенности ОС семейства Windows (2000/XP). Здесь ряд объектов доступа (в частности, устройства, реестр ОС и т.д.) не являются объектами файловой системы. Поэтому возникает вопрос, как следует трактовать требование «Система защиты должна контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) ». То есть, не ясно, являются ли объектами доступа, к которым, следуя формальным

требованиям, необходимо разграничивать доступ пользователей, например, реестр ОС и т.д.

В отличие от семейства ОС UNIX, где все задачи разграничительной политики доступа к ресурсам решаются средствами управления доступом к объектам файловой системы, доступ в данных ОС разграничивается собственным механизмом для каждого ресурса. Другими словами, при рассмотрении механизмов защиты ОС Windows встает задача определения и задания требований к полноте разграничений (это определяется тем, что считать объектом доступа).

Также, как и для семейства ОС UNIX, здесь основными механизмами защиты являются:

- идентификация и аутентификация пользователя при входе в систему;

- разграничение прав доступа к ресурсам, в основе которого лежит реализация дискреционной модели доступа (отдельно к объектам файловой системы, к устройствам, к реестру ОС, к принтерам и др.);

- аудит, то есть регистрация событий.

Здесь явно выделяются (в лучшую сторону) возможности разграничений прав доступа к файловым объектам (для NTFS) - существенно расширены атрибуты доступа, устанавливаемые на различные иерархические объекты файловой системы (логические диски, каталоги, файлы). В частности, атрибут «исполнение» может устанавливаться и на каталог, тогда он наследуется соответствующими файлами (в отличие от ОС семейства UNIX).

При этом существенно ограничены возможности управления доступом к другим защищаемым ресурсам, в частности, к устройствам ввода. Например, здесь отсутствует атрибут «исполнение», т.е. невозможно запретить запуск несанкционированной программы с устройств ввода.

Рассмотрим принципиальные *недостатки защиты ОС семейства Windows*, напрямую связанные с возможностью НСД к информации. При этом в отличие от ОС семейства UNIX в ОС Windows невозможна в общем случае реализация централизованной схемы администрирования механизмов защиты или соответствующих формализованных требований. Вспомним, что в ОС UNIX это распространялось лишь на запуск процессов. Связано это с тем, что в ОС Windows принята иная концепция реализации разграничительной политики доступа к ресурсам (для NTFS).

В рамках этой концепции разграничения для файла приоритетнее, чем для каталога, а в общем случае - разграничения для включаемого файлового объекта приоритетнее, чем для включающего. Это приводит к тому, что пользователь, создавая файл и являясь его «владельцем», может назначить любые атрибуты доступа к такому файлу (т.е. разрешить к нему доступ любому иному пользователю). При этом обратиться к этому файлу может пользователь (которому назначил права доступа «владелец») вне зависимости от установленных администратором атрибутов доступа на каталог, в котором пользователь создает файл. Данная проблема непосредственно связана с реализуемой в ОС Windows концепцией защиты информации.

Далее, в ОС семейства Windows (2000/XP) *не в полном объеме реализуется дискреционная модель доступа*, в частности, не могут разграничиваться права доступа для пользователя «Система». В ОС присутствуют не только пользовательские, но и системные процессы, которые запускаются непосредственно системой. При этом доступ системных процессов не может быть разграничен. Соответственно, все запускаемые системные процессы имеют неограниченный доступ к защищаемым ресурсам. Как увидим ниже, с этим недостатком системы защиты связано множество атак, в частности, несанкционированный запуск собственного процесса с правами системного. Кстати, позднее мы увидим, что это возможно и вследствие некорректной реализации механизма обеспечения замкнутости программной среды.

В ОС семейства Windows (2000/XP) *невозможно в общем случае обеспечить замкнутость (или целостность) программной среды*. Это связано совершенно с иными проблемами, чем в ОС семейства UNIX, в которых невозможно установить атрибут «исполнение» на каталог. Давайте выясним, в чем сложности у ОС Windows в этом вопросе.

Рассмотрим два способа, которыми в общем случае можно реализовать данный механизм, и покажем их несостоятельность в ОС Windows. Итак, механизм замкнутости программной среды в общем случае может быть обеспечен:

1. Заданием списка разрешенных к запуску процессов с предоставлением возможности пользователям запускать процессы только из этого списка. При этом процессы задаются *полнопутевыми именами*, причем средствами разграничения доступа обеспечивается невозможность их модернизации пользователем. Данный подход

просто не реализуется встроенными в ОС механизмами.

2. Разрешением запуска пользователями программ только из заданных каталогов при невозможности модернизации этих каталогов. Одним из условий корректной реализации данного подхода является запрет пользователям запуска программ иначе, чем из соответствующих каталогов. Некорректность реализации ОС Windows данного подхода связана с невозможностью установки атрибута «исполнение» на устройства ввода (дисковод или CD-ROM). В связи с этим при разграничении доступа пользователь может запустить несанкционированную программу с дискеты, либо с диска CD-ROM (это очень распространенная атака на ОС данного семейства).

Здесь же стоит отметить, что с точки зрения обеспечения замкнутости программной среды (т.е. реализации механизма, обеспечивающего возможность пользователям запускать только санкционированные процессы (программы)) действия пользователя по запуску процесса могут быть как явными, так и скрытыми.

Явные действия предполагают запуск процессов (исполняемых файлов), которые однозначно идентифицируются своим именем. Скрытые действия позволяют осуществлять встроенные в приложения интерпретаторы команд. Примером таковых могут служить офисные приложения. При этом скрытыми действиями пользователя будет запуск макроса.

В данном случае идентификации подлежит лишь собственно приложение, например, процесс winword.exe. При этом он может помимо своих регламентированных действий выполнять те скрытые действия, которые задаются макросом (соответственно, те, которые допускаются интерпретатором), хранящимся в открываемом документе. То же относится и к любой виртуальной машине, содержащей встроенный интерпретатор команд. При этом отметим, что при использовании приложений, имеющих встроенные интерпретаторы команд (в том числе офисных приложений), не в полном объеме обеспечивается выполнение требования по идентификации программ.

Возвращаясь к обсуждению недостатков, отметим, что в ОС семейства Windows (2000/XP) *невозможно встроенными средствами гарантированно удалять остаточную информацию*. В системе просто отсутствуют соответствующие механизмы.

Кроме того, ОС семейства Windows (2000/XP) *не обладают в полном объеме возможностью контроля целостности файловой*

системы. Встроенные механизмы системы позволяют контролировать только собственные системные файлы, не обеспечивая контроль целостности файлов пользователя. Кроме того, они не решают важнейшую задачу данных механизмов - контроль целостности программ (приложений) перед их запуском, контроль файлов данных пользователя и др.

Что касается регистрации (аудита), то в ОС семейства Windows (2000/XP) *не обеспечивается регистрация выдачи документов на «твердую копию», а также некоторые другие требования к регистрации событий.*

Опять же, если трактовать требования к управлению доступом в общем случае, то при защите компьютера в составе ЛВС необходимо управление доступом к хостам (распределенный пакетный фильтр). В ОС семейства Windows (2000/XP) *механизм управления доступа к хостам в полном объеме не реализуется.*

Что касается разделяемых сетевых ресурсов, то фильтрации подвергается только входящий доступ к разделяемому ресурсу, а запрос доступа на компьютере, с которого он осуществляется, фильтрации не подлежит. Это принципиально, т.к. не могут подлежать фильтрации приложения, которыми пользователь осуществляет доступ к разделяемым ресурсам. Благодаря этому, очень распространенными являются атаки на протокол NETBIOS.

Кроме того, в полном объеме (в части фильтрации только входящего трафика) управлять доступом к разделяемым ресурсам возможно только при установленной на всей компьютерах ЛВС файловой системы NTFS. В противном случае невозможно запретить запуск несанкционированной программы с удаленного компьютера, то есть обеспечить замкнутость программной среды в этой части.

Из приведенного анализа можем видеть, что многие механизмы, необходимые с точки зрения выполнения формализованных требований, ОС семейства Windows не реализуют в принципе, либо реализуют лишь частично.

Выводы по ОС семейства UNIX Windows (2000/XP).

С учетом сказанного можно сделать важный вывод относительно того, что большинством современных универсальных ОС не выполняются в полном объеме требования к защите АС по классу 1Г. Это значит, что, учитывая требования нормативных документов [16, 17], они не могут без использования добавочных средств защиты применяться для защиты даже конфиденциальной информации. При этом следует отметить, что основные проблемы

защиты здесь вызваны не невыполнимостью ОС требований к отдельным механизмам защиты, а принципиальными причинами, обусловленными реализуемой в ОС концепцией защиты. Концепция эта основана на реализации распределенной схемы администрирования механизмов защиты, что само по себе является невыполнением формализованных требований к основным механизмам защиты.

3.3.1.3. Подходы к проектированию систем защиты компьютерной информации

Оценка надежности систем защиты информации.

Отказоустойчивость систем защиты.

Исследуя вопросы защиты компьютерной информации, необходимо уделять внимание вопросам надежности системы защиты. При этом следует понимать, что интерпретация самого понятия «надежность системы защиты», а также основных параметров и характеристик надежности системы защиты, принципиально иная, чем для свойств надежности вычислительной системы.

В общем случае надежность вычислительной системы - это свойство системы выполнять возложенные на нее функции в течение заданного промежутка времени. Применительно к системе защиты информации от НСД *надежность — это свойство системы защиты обеспечивать защиту компьютерной информации от НСД в течение заданного промежутка времени.*

В общем случае отказ системы — это случайное событие, приводящее к невозможности выполнения системой в течение некоторого времени возложенных на нее функций.

Для системы защиты понятие «отказ» может трактоваться совсем иначе, чем при рассмотрении любого иного технического средства, т.к. с отказом связан не только переход системы защиты в состояние неработоспособности (данная составляющая «отказа» присуща любому техническому средству и здесь не рассматривается), но и обнаружение в системе защиты уязвимости.

Действительно, пусть обнаружена ошибка в механизме защиты, использование которой злоумышленником прямо, либо косвенно, приводит к НСД. Это можно трактовать как отказ системы защиты, т.к. до тех пор, пока подобная ошибка не будет исправлена, система защиты не выполняет своих функций, и в данной ситуации

существует канал несанкционированного доступа к информации.

Кстати говоря, неважно, что на какой-то момент времени для системы защиты известен только один-единственный канал НСД к информации. Этого вполне достаточно, чтобы говорить об отказе системы защиты в целом, т.к. характеристикой защиты является вероятность отражения ею атак на защищаемый объект, которая в данном случае имеет нулевое значение.

Под *«отказом»* системы защиты будем понимать [18] обнаружение злоумышленником канала НСД к информации (например, ошибки в ОС, либо в приложении, которая может привести к несанкционированному доступу). Под *«отказоустойчивостью»* — способность системы защиты обеспечивать свои функции (обеспечивать защиту компьютерной информации) в условиях обнаружения канала НСД к информации.

Отметим, что, вообще говоря, вопрос обеспечения надежности функционирования любой системы является одним из важнейших при ее проектировании. Но почему-то на сегодняшний день ему уделяется незначительное внимание при построении систем защиты (в данном случае под надежностью понимаем ее отказоустойчивость к обнаружению канала НСД к информации).

Действительно, представим себе, что вся сеть предприятия реализована на единой платформе – установлен единый тип ОС, вся защита обеспечивается встроенными в ОС средствами защиты. В этом случае с момента обнаружения канала НСД к информации и до момента его ликвидации (например, посредством установки некоторого дополнительного программного обеспечения, которое должен поставить разработчик ОС), можно считать систему защиты отказавшей, а сеть предприятия незащищенной.

Аналогично тому, как это выполнено в теории надежности вычислительных систем, в данном случае можно ввести два важнейших параметра, характеризующих систему защиты: интенсивность отказов — среднее число отказов в единицу времени, λ ; время восстановления системы после отказа T_r .

Под *интенсивностью отказов* системы защиты от НСД следует понимать интенсивность обнаружения в ней каналов НСД к информации в единицу времени.

Численные значения данного параметра могут быть получены на основании статистики угроз НСД, которая для современных универсальных ОС составляет, как пример (в среднем в год) таблица 3.15 и таблица 3.16:

Таблица 3.15

**Общее количество известных успешных атак
различных ОС**

<i>Тип ОС</i>	<i>Количество атак</i>	<i>Тип ОС</i>	<i>Количество атак</i>
MS Windows	130	Linux	167
MS Windows	120	IRIX	84
BSD	64	HPUX	65
BSDI	10	AIX	42
Solaris	125	SCO	40
Sun OS	40	Novell NetWare	10
Digital Unix	25	IOS (Cisco)	7

Таблица 3.16

Общее количество известных атак на различные группы ОС

Тип ОС	Количество атак
MS Windows	230
UNIX	660
Novell Netware	10

При расчете надежности принимается, что интенсивность отказов является постоянной во времени величиной. Если предположить, что угрозы НСД взаимонезависимы и любая i -я ($i=1, \dots, I$) угроза носит катастрофический характер, предоставляя злоумышленнику несанкционированный доступ к информации, то интенсивность отказов системы защиты равна сумме интенсивностей угроз НСД к соответствующей системе защиты:

$$\lambda = \sum_{i=1}^I \lambda_i \quad (3.4)$$

Тогда вероятность исправной работы системы защиты в течение произвольного интервала времени t определяется следующим образом:

$$p(t) = e^{-\lambda t} \quad (3.5)$$

Соответственно, обратная величина интенсивности отказов системы равна среднему промежутку времени между двумя отказами и называется *временем наработки на отказ*:

$$T = 1/\lambda \quad (3.6)$$

Интенсивность отказов системы определяется рядом параметров, в том числе, сложностью исследования защитных механизмов в системе, квалификацией злоумышленника и временным интервалом эксплуатации системы защиты.

Сложность исследования механизмов защиты зависит не только от качества разработки системы защиты (уровня квалификации разработчика), но и от доступности информации о системе защиты для исследования злоумышленником. С точки зрения доступности для исследования можно выделить следующие категории систем, характеризующиеся возможностью обнаружения злоумышленником каналом ИСД к информации:

- *Очень высокая* — некоммерческие средства (в том числе ОС), характеризующиеся свободным доступом злоумышленника к их исходным кодам;

- *Высокая* — широко используемые на практике коммерческие средства (в том числе ОС), характеризующиеся отсутствием доступа злоумышленника к их исходным кодам;

- *Низкая* — ограниченно (по различным причинам) используемые на практике коммерческие средства (в том числе ОС), характеризующиеся отсутствием доступа злоумышленника к их исходным кодам.

- *Очень низкая* — используемые на практике коммерческие средства, имеющие формализованные правила ограниченного распространения, характеризующиеся отсутствием доступа злоумышленника к исходным кодам ПО. К этой категории, в первую очередь, относятся коммерческие средства защиты отечественных производителей.

Очень важно при построении системы защиты правильно учесть *квалификацию злоумышленника*. При этом в определенных случаях его квалификация может быть очень высокой, т.к. для обнаружения некорректностей в реализации механизма защиты, либо ошибок, требуется проведение некоторого системного и архитектурного анализа защищаемого объекта и т.д. В других же случаях злоумышленник вполне может обойтись небольшим набором знаний и умений. Очевидно, что квалификация злоумышленника в большой мере определяется областью применения защищаемого объекта, т.е. ценностью той информации, которая обрабатывается защищаемым объектом.

Временной интервал эксплуатации системы защиты - также весьма важный аспект, влияющий на интенсивность отказов. Ведь

понятно, что сначала злоумышленником выявляются наиболее очевидные каналы НСД к информации, которые соответствующим образом ликвидируются разработчиком. Соответственно, чем дольше эксплуатируется система, тем сложнее злоумышленнику найти канал НСД к информации. Однако это при условии, что вносимые разработчиком исправления, не приведут к новым, еще более очевидным некоррекциям и ошибкам.

Время восстановления системы защиты.

На настоящий момент очевидна целесообразность усиления средств защиты в части увеличения параметра «среднее время наработки на отказ». Однако не менее (если не более) важным является другая составляющая надежности системы защиты - так называемое «время восстановления».

Интервал времени, в течение которого после возникновения отказа системы защиты обнаруженный канал НСД к информации устраняется, будем называть временем восстановления (T_v).

В общем случае время восстановления является случайной величиной. Однако принято учитывать его среднее значение. Среднее время восстановления характеризуется компонентами:

- временем устранения соответствующего канала НСД к информации разработчиком (T_y);
- временем внедрения на защищаемый объект исправленной версии системы защиты, включая ее настройку ($T_{ин}$).

Очевидно, можем принять, что среднее время восстановления определяется временем устранения соответствующего канала НСД к информации разработчиком. Другой компонентой, ввиду ее относительной малости, можем пренебречь. Поэтому примем:

$$(T_v) = (T_y) \quad (3.7)$$

С учетом сказанного можем отметить, что в рассматриваемом случае среднее время восстановления - это одна из основных характеристик надежности функционирования системы защиты. Определяется она тем, насколько предприятие-разработчик системы защиты оперативно исправляет обнаруживаемые каналы НСД. Причем при использовании встроенных механизмов защиты этим разработчиком является сам разработчик ОС (приложения).

Отметим, что характеристика «время восстановления» объективно зависит от сложности системы. Действительно, зачастую исправление одной ошибки требует тестирования практически всех

функциональных модулей системы заново, поскольку в сложной технической системе все функциональные модули сильно взаимосвязаны.

Кстати говоря, исправление одной ошибки может привести к появлению других ошибок. Поэтому исправление ошибок в ОС и сложных приложениях требует реализации соответствующей технологии внесения исправлений. Эта технология предполагает серьезное тестирование ПО практически по всем функциям, что может составлять месяцы. Например, для ОС семейства Windows данный параметр можно охарактеризовать, как половину среднего интервала времени между выходами в свет доработок ОС - Service Pack.

Отметим, что с учетом сложности исправления ошибок, на практике разработчики сложных систем стараются не исправлять ошибки поодиночке, а приступать к тестированию системы уже по факту исправления некоторой совокупности ошибок (с учетом совокупности внесенных изменений).

При этом необходимо учитывать, что в течение всего времени восстановления можно считать систему защиты отказавшей, а защищаемый объект — незащищенным.

Следовательно, такая характеристика надежности системы защиты, как «время восстановления», может служить требованием к предприятию-разработчику системы защиты.

С позиций надежности эксплуатационные свойства системы защиты можно охарактеризовать *коэффициентом готовности*:

$$K_r = T / (T + T_n) \quad (3.8)$$

Коэффициент готовности, во-первых, характеризует долю времени, в течение которого система защиты работоспособна, а во-вторых, определяет вероятность того, что в любой произвольный момент времени система защиты работоспособна. Соответственно получаем долю времени, в течение которого объект находится в незащищенном состоянии, а также вероятность того, что в любой момент времени объект незащищен:

$$K_{нз} = 1 - K_r \quad (3.9)$$

Проведем грубую оценку характеристики «коэффициент готовности», чтобы оценить, насколько критична характеристика «время восстановления» при построении системы защиты. Примем интенсивность обнаружения ошибки, которая может привести к НСД

к информации, равной 1 в год (практика показывает, что для ряда ОС и приложений она значительно выше). В таблице 3.17 показано изменение коэффициента готовности системы (вероятности нахождения системы в защищенном виде) при различных значениях характеристики времени восстановления.

Таблица 3.17

Изменение коэффициента готовности

<i>Время восстановления</i>	<i>3 месяца</i>	<i>1 месяц</i>	<i>2 недели</i>	<i>1 неделя</i>	<i>3 дня</i>	<i>1 день</i>
Коэффициент готовности	0,80	0,92	0,96	0,98	0,992	0,997

Требования к системе защиты информации исходя из отказоустойчивости.

Требования к надежности вычислительной системы на практике определяются, как правило, значением коэффициента готовности не ниже 0,99 (в большинстве случаев -- 0,999 и выше). Соответственно, на основе представленных в табл. 1.5 исследований мы можем сделать вывод, что время восстановления системы защиты должно определяться днями, а не месяцами, как это происходит на практике при использовании встроенных в ОС (и приложения) защитных механизмов. При этом отметим, что нами исследовался наиболее благоприятный случай, когда интенсивность отказов принималась равной 1 в год. А если их будет два и более, какова будет вероятность защищенности системы?

Из сказанного могут быть сделаны следующие выводы [18]:

1. Усиление средств защиты целесообразно для повышения надежности системы защиты — уменьшения времени восстановления системы при обнаружении канала НСД к информации. В этом случае следует говорить о целесообразности замещения всех встроенных механизмов защиты на механизмы систем защиты отечественной разработки. Возможность же существенного снижения характеристики «времени восстановления» при этом обуславливается двумя причинами: во-первых, объективной — система защиты как таковая имеет на порядки меньшую сложность, чем ОС в целом (исправление ошибки в ней потребует на столько же меньших трудозатрат, чем аналогичные исправления в ОС), во-вторых, субъективной — отечественные производители могут с большей оперативностью обеспечить взаимодействие с конечным потребителем средств защиты, в частности, при распространении

исправленной версии ПО.

2. К разработчику системы защиты, при ее практическом использовании, должно выдвигаться требование к времени восстановления системы защиты — устранения каналов НСД к информации. Так как время восстановления системы защиты, с целью достижения высокого уровня ее отказоустойчивости, должно определяться днями (что на практике невозможно), то при построении системы защиты должны решаться вопросы резервирования.

3. Недопустимо использовать средства добавочной защиты, не поддерживаемые конкретным предприятием-разработчиком (в частности, свободно распространяемые и др.), а также распространяемые предприятием, не способным обеспечить необходимую оперативность восстановления системы защиты при обнаружении канала НСД к информации.

Таким образом, как видим, требования к времени восстановления системы защиты очень высоки даже при использовании на защищаемом объекте средств защиты отечественного производителя.

Методы резервирования встроенных в ОС механизмов защиты для повышения отказоустойчивости системы защиты.

Для увеличения надежности любой вычислительной системы применяется резервирование. Любое резервирование основывается на включении в состав системы защиты дополнительных средств. В нашем случае - дополнительных механизмов защиты. Причем в отличие от классических способов резервирования средств вычислительной техники, предполагающих параллельное включение резервного оборудования, однотипного с резервируемым оборудованием, в данном случае резервные механизмы (дополнительные механизмы защиты) должны включаться последовательно.

Под резервированием механизмов защиты понимают последовательное включение в систему защиты дополнительных механизмов, реализующих те же функции защиты, что и основные механизмы, но иным способом и средствами.

Требование к реализации механизмов защиты различными способами и средствами обусловлено необходимостью резервного противодействия угрозе в случае преодоления злоумышленником основного механизма защиты. То есть одна и та же угроза должна распространяться либо на резервируемый, либо на резервный

механизмы, в противном случае факт резервирования отсутствует, как таковой.

Таким образом, использование в системе защиты дополнительных механизмов можно рассматривать не только с целью расширения функций встроенных механизмов защиты, но и с целью их резервирования.

Если надежность системы защиты характеризуется вероятностью p безотказной работы за время t и определяется для встроенных средств защиты надежностью p_0 : $p = p_0$, то при использовании дополнительных механизмов защиты, обеспечивающих резервирование встроенных механизмов, и характеризуемых надежностью p_1 , имеем:

$$p = (1 - (1 - p_0)(1 - p_1)) \quad (3.10)$$

Заметим, что резервирование приводит не только к увеличению вероятности безотказной работы системы защиты, но и к снижению требований к времени восстановления.

В общем случае можно выделить три режима резервирования системы защиты дополнительными механизмами защиты:

- *Горячий резерв*, при котором основные и дополнительные механизмы защиты настроены и включены. В этом случае ограничений на время восстановления системы практически не накладывается (естественно, в разумных пределах). Этот подход обеспечивает наиболее высокий уровень защиты, т.к. при преодолении основного механизма защиты противодействие угрозе оказывает резервный механизм (в предположении, что угроза в равной мере не распространяется на основной и резервный механизмы защиты).

Для систем защиты информации, критичной к НСД, следствием сказанного будет вывод о целесообразности резервной реализации основных механизмов защиты от НСД, дополнительными механизмами защиты с их включением в режиме «горячего резерва» совместно со встроенными механизмами защиты. При этом к основным механизмам защиты от НСД прежде всего относятся механизм идентификации и аутентификации, а также механизм управления доступом к ресурсам.

- *Активный холодный резерв*, при котором основной и дополнительный механизмы защиты настроены, но включен только один из них. В этом случае время восстановления определяется

продолжительностью запуска резервной системы при отказе основной. Как правило, это время составляет несколько часов. Однако, по сравнению с горячим резервированием, здесь достигается снижение влияния системы защиты на загрузку вычислительного ресурса защищаемого объекта.

- *Пассивный холодный резерв*, при котором только одно из средств защиты (основное или дополнительное) настроено и включено. В этом случае время восстановления определяется продолжительностью настройки и запуска резервной системы при отказе основной. Обычно это составляет от нескольких часов до нескольких дней. Однако, по сравнению с активным холодным резервированием здесь достигается упрощение администрирования системы защиты, как при ее внедрении, так и в процессе функционирования.

Ранее отмечалась необходимость усиления механизмов защиты, встроенных в ОС. Однако, на основании анализа, проведенного в данном разделе, можно сделать вывод, что наряду с этим важнейшей задачей усиления системы защиты следует считать резервирование встроенных в ОС и приложения механизмов защиты. Связано это с тем, что даже при потенциально максимальной оперативности предприятия-разработчика по устранению ошибок (выявленных каналов НСД к информации), только этим невозможно обеспечить сколько-нибудь высокую отказоустойчивость системы защиты (ее способность выполнять свои функции). Таким образом, без резервирования механизмов защиты о гарантированной защите не приходится говорить в принципе.

Встроенная и добавочная защита информации.

Понятие встроенной и добавочной защиты.

По способу реализации системы защиты компьютерной информации от НСД подразделяют на встроенные и добавочные.

Под *встроенной* понимается система защиты, механизмы которой встроены в соответствующее функциональное ПО (системное и прикладное), являются его неотъемлемой частью и реализуют дополнительную для данного ПО функцию - обеспечение защиты компьютерной информации.

Под *добавочной* понимается система защиты, основное функциональное назначение которой является решение задач защиты информации. Используется добавочная система совместно с функциональным ПО и имеет своей целью усиление защитных свойств встроенных в ПО механизмов.

Изначально средства добавочной защиты появились для незащищенных ОС, не обладающих встроенными механизмами защиты. Сначала это были системы для ОС семейства DOS, затем для ОС семейства Windows 9х. Понятно, что о способах комплексирования механизмов защиты, равно как и о возможности их резервирования, здесь говорить не приходится, т.к. используются только добавочные механизмы.

В книге конкретные системы защиты как таковые не рассматриваются, а исследуются собственно подходы к их построению. Дело в том, что невозможно осуществить корректное сравнение средств добавочной защиты между собой в принципе, т.к. при этом необходимо учитывать не только, какие методы и функции защиты реализуются, но и то, каким образом они реализуются [18]. Однако, это является НОУ-ХАУ разработчика, а значит, по понятным причинам, информация об их уязвимости в открытой печати отсутствует. Поэтому сравнивать можно лишь общие подходы и технологии, реализуемые в системах защиты. При необходимости можно найти описание данных систем защиты на сайтах разработчиков.

ОС Windows 2000/XP, а также современные ОС семейства UNIX, обладают развитыми встроенными механизмами защиты. Они уже обладают реализацией ядра ОС с заложенными принципами противодействия как явным, так и скрытым угрозам. Поэтому для этих ОС уже становится актуальным выбор концептуального решения (определения подходов) при построении системы добавочной защиты, а также методов комплексирования механизмов встроенной и добавочной защиты.

Подходы к построению добавочной защиты информации.

С учетом выше изложенного материала, можно признать обоснованными основные подходы к построению добавочных средств защиты для защищенных ОС (т.е. обладающих встроенными механизмами защиты) [18]:

1. Добавление механизмов защиты, отсутствующих в ОС, и усиление добавочными средствами штатных встроенных механизмов защиты.

2. Реализация всех механизмов защиты добавочными средствами и их применение наряду со встроенными механизмами.

Очевидно, что первому подходу присущи два недостатка: во-первых, невозможность решения концептуальных вопросов защиты информации, рассмотренных ранее, во-вторых - невозможность

резервирования основных механизмов защиты. При этом, к основным механизмам защиты от НСД относятся механизмы идентификации и аутентификации пользователя при входе в систему, а также механизмы управления доступом к ресурсам.

Что касается второго подхода, то он, возможно, характеризуется некоторой избыточностью. Вместе с тем он позволяет в полном объеме решать рассматриваемые проблемы защиты информации.

В качестве замечания следует отметить, что в критичных приложениях по изложенным ранее причинам недопустимо использование свободно распространяемых (не коммерческих) средств защиты, а также свободно распространяемых защищенных систем (в частности ОС) без применения средств добавочной защиты. Говоря же о средствах добавочной защиты, прежде всего следует иметь в виду использование коммерческих отечественных продуктов, сертифицированных по принятым требованиям информационной безопасности.

Основные требования и задачи системы добавочной защиты от НСД.

Обобщая все сказанное ранее, сформулируем необходимые требования к системе добавочной защиты от НСД для защищенных ОС (ОС, обладающих встроенными механизмами защиты):

1. Механизмы добавочной защиты должны применяться наряду со встроенными в ОС и приложения механизмами защиты;
2. Механизмы добавочной защиты должны применяться с целью усиления защитных свойств встроенных механизмов (задачи добавочной защиты в части усиления защитных свойств встроенных механизмов рассмотрены выше).
3. Механизмы добавочной защиты должны применяться с целью контроля корректности функционирования встроенных механизмов защиты, обеспечивая противодействие ошибкам и закладкам в системном и прикладном ПО.
4. Механизмы добавочной защиты должны применяться с целью резервирования встроенных механизмов, прежде всего, основных механизмов противодействия НСД. Это будет приводить к повышению надежности системы защиты информации.

Итак, добавочные механизмы защиты необходимы, и определен общий круг решаемых ими задач. Вместе с тем следует отметить, что с включением в систему защиты добавочных механизмов связано и появление новых угроз - угроз именно

механизмам добавочной защиты. Эти угрозы связаны с тем, что механизмы добавочной защиты по ряду причин (в том числе и ввиду необходимости выполнять разработчиком систем добавочной защиты требования лицензионного соглашения для ОС) реализуются не на уровне ядра, а на уровне драйверов и приложений. Т.е. на них не распространяется защита системными средствами, реализуемая ядром ОС. Они являются внешними по отношению к ОС.

Опасность этого проиллюстрируем примером. Для ОС Windows 2000/XP для запуска режима загрузки системы Safe Mode достаточно осуществить авторизацию пользователя. В этом режиме пользователем возможна выборочная загрузка системы, при которой часть драйверов и приложений по усмотрению пользователя может не загружаться. И хотя это не распространяется на встроенные средства защиты (они загружаются всегда), пользователем могут быть не загружены драйверы и приложения добавочных средств защиты.

Таким образом, при включении в систему механизмов добавочной защиты дополнительно должны быть решены задачи противодействия угрозе перевода добавочной защиты в пассивное состояние. То есть должно осуществляться противодействие загрузке системы без механизмов добавочной системы. Кроме того, должно быть реализовано противодействие удалению механизмов добавочной защиты, а также переводу их в пассивное состояние при функционировании системы.

Итак, теперь мы можем сформулировать еще одну задачу, которая должна решаться при реализации в системе добавочной защиты информации от НСД:

5. Механизмы добавочной защиты должны оказывать противодействие как явным, так и скрытым угрозам их переводу в пассивное состояние в процессе функционирования системы, либо загрузке системы без механизмов добавочной защиты.

Кроме того, отметим, что ранее рассматривались требования к встроенным в ОС механизмам защиты и их возможности в предположении, что данные механизмы присутствуют в системе. Вместе с тем, существует возможность загрузки на защищаемом компьютере другой ОС, в частности, с внешнего носителя. Функции защиты загрузки системы уже не входят в задачи ОС. В частности данная задача решается BIOS, с реализацией которой также связаны некоторые угрозы. Поэтому добавочные средства защиты также могут использоваться и с целью дополнительной защиты загрузки системы, т.е. можем сформулировать еще одно требование к

механизмам добавочной защиты:

6. Механизмы добавочной защиты должны применяться с целью усиления защитных свойств от несанкционированной загрузки ОС, в частности, реализуемых отдельным программным средством BIOS.

Таким образом, таковы основные задачи механизмов добавочной защиты, однако, кроме них для добавочных механизмов защиты могут рассматриваться также и некоторые дополнительные задачи. Эти задачи связаны с корректным использованием приложений и встроенных в приложения механизмов защиты, с решением задачи централизации схемы администрирования защитных механизмов в иерархической информационной системе, с решением задач упрощения настройки защитных механизмов и др.

Вопросы оценки эффективности и проектирования системы защиты.

Ранее было приведено обоснование целесообразности применения добавочных средств защиты при построении современных информационных систем. При этом были выделены две группы требований к защищенности, которые должны учитываться при построении системы защиты — формализованные требования и требования, формулируемые на основе существующей статистики угроз. Невозможность в общем случае формализовать требования второй группы не позволяет и формализовать сравнительный анализ систем защиты, отнесенных к одному классу защищенности (в соответствии с классификацией нормативных документов).

В частности, две системы защиты, отнесенные к одному классу защищенности, могут принципиально различаться по своим возможностям. При этом необходимо отметить, что в случае предполагаемой идентичности реализации формализованных требований, для них важнейшей характеристикой становится уровень квалификации их разработчиков. Предположение идентичности обычно не соответствует действительности, т.к. в нормативных документах не указывается, каким способом должен быть реализован каждый механизм защиты. Поэтому существующие системы добавочной защиты, отнесенные к одному классу защищенности, принципиально различаются и в реализации формализованных требований.

Вопросы оценки эффективности и вопросы проектирования системы защиты тесно связаны, т.к. в их основе лежит единый

математический аппарат решения соответствующей оптимизационной задачи.

Рассмотрим возможный подход к проектированию (оценке эффективности) системы защиты. Отметим, что в данном случае мы не разделяем механизмы защиты на встроенные и добавочные, поскольку это уже вопрос реализации тех требований к набору и функциям механизмов защиты, которые будут сформулированы в результате проектирования системы защиты. При этом будем понимать, что необходимо решать задачу многокритериальной оптимизации, т.к. система защиты в общем случае характеризуется целым рядом параметров, которые должны учитываться при ее проектировании.

Общий подход к оценке эффективности системы добавочной защиты.

Критерий и параметры проектирования оптимальной системы защиты.

Будем оценивать защищенность системы (Z) количественно в зависимости от стоимости защищаемой информации, вероятности взлома, стоимости самой системы защиты, производительности системы:

$$Z = f(C_{инф}, P_{взл}, C_{сзи}, П), \quad (3.11)$$

где $C_{инф}$ - стоимость защищаемой информации;

$P_{взл}$ - вероятность взлома; $C_{сзи}$ - стоимость СЗИ;

$П$ - производительность системы.

С учетом введенного понятия защищенности системы оптимизационная задача состоит в обеспечении максимального уровня защищенности (как функции стоимости защищаемой информации и вероятности взлома) при минимальной стоимости системы защиты и минимальном влиянии ее на производительность системы:

С учетом сказанного может быть сделан важный вывод о многокритериальном характере задачи проектирования системы защиты. При этом, кроме обеспечиваемого уровня защищенности, должен учитываться еще ряд важнейших характеристик системы. Например, обязательно должно учитываться влияние системы защиты на загрузку вычислительного ресурса защищаемого объекта.

В общем случае загрузка вычислительного ресурса определяется количеством прикладных задач, решаемых объектом в единицу времени.

Исходные параметры для задачи проектирования системы защиты, а также возможности сведения задачи к однокритериальной будут следующие.

Критерии оценки защищенной системы:

1. Набор типов СЗИ (w) механизмов СЗИ (i);
2. Вероятность взлома (p);
3. Стоимость:

3.1. Стоимость информации ($C_{инф}$);

3.2. Стоимость защиты $C_{сзи}$;

4. Производительность (Π):

Для $C_{сзи}$ и Π есть ограничения: $C_{сзи} \leq C_{зад}$ и $\Pi_{сзи} \leq \Pi_{зад}$.

Далее по 2 и 3 критерию находят мультипликативный критерий риска: $R = C_{инф} \cdot p$, а по нему и первому критерию определяют математическое ожидание мультипликативного критерия риска: $R = \sum_i^w C_{инф i} \cdot p_i$

Затем определяют коэффициент защищенности по выражению: $D = 1 - R_{защ} / R_{нез}$, где: $R_{защ}$ - риск в защищенной системе; $R_{нез}$ - риск в незащищенной системе.

И потом определяют: $D(C, p) \rightarrow \max$, при ограничениях: $C_{сзи} \leq C_{зад}$ и $\Pi_{сзи} \leq \Pi_{зад}$.

Защищенность системы с точки зрения риска.

Рассмотрим защищенность системы с точки зрения риска. Заметим, что использование теории рисков для оценки уровня защищенности на сегодняшний день является наиболее часто используемым на практике подходом. Риск (R) — это потенциальные потери от угроз защищенности:

$$R(p) = C_{инф} \cdot p_{взл} \quad (3.12)$$

По существу, параметр риска здесь вводится как мультипликативная свертка двух основных параметров защищенности.

С другой стороны, можно рассматривать риск как потери в единицу времени:

$$R(\lambda) = C_{инф} \cdot \lambda_{взл}, \quad (3.13)$$

где $\lambda_{взл}$ - интенсивность потока взломов (под взломом будем понимать удачную попытку несанкционированного доступа к информации).

Эти две формулы связаны соотношением:

$$p_{взл} = \lambda_{взл} / \Lambda \quad (3.14)$$

где Λ – общая интенсивность потока несанкционированных попыток доступа злоумышленниками к информации.

Основной критерий защищенности. Общее решение задачи проектирования оптимальной системы защиты.

В качестве основного критерия защищенности будем использовать *коэффициент защищенности* (D), показывающий относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой:

$$D = (1 - R_{защ} / R_{нез}) \cdot 100\%, \quad (3.15)$$

где $R_{защ}$ – риск в защищенной системе;

$R_{нез}$ – риск в незащищенной системе.

Таким образом, в данном случае задача оптимизации выглядит следующим образом:

$$\begin{cases} D(C_{инф}, P_{взл}) \rightarrow \max; \\ C_{сзи} \rightarrow \min; \\ П_{сзи} \rightarrow \max. \end{cases} \quad (3.16)$$

Для решения этой задачи сведем ее к однокритериальной посредством введения ограничений. Тогда получаем:

$$\begin{cases} D(C_{инф}, P_{взл}) \rightarrow \max; \\ C_{сзи} \leq C_{зад}; \\ C_{сзи} \geq П_{зад}, \end{cases} \quad (3.17)$$

где $C_{зад}$ и $П_{зад}$ – заданные ограничения на стоимость системы защиты и производительность системы.

Целевая функция выбрана, исходя из того, что именно она отражает основное функциональное назначение системы защиты – обеспечение безопасности информации.

Производительность системы $П_{сзи}$ рассчитывается с применением моделей и методов теории массового обслуживания и теории расписаний (в зависимости от того, защищается ли система оперативной обработки, либо реального времени). На практике возможно задание ограничения по производительности (влияние на загрузку вычислительного ресурса защищаемой системы) не непосредственно в виде требуемой производительности системы, а как снижение производительности ($d П_{зад}$) информационной системы

от установки системы защиты. В этом случае задача оптимизации будет выглядеть следующим образом

$$\begin{cases} D(C_{инф}, P_{взл}) \rightarrow \max; \\ C_{сзи} \rightarrow \min; \\ d\Pi_{сзи} \rightarrow \max, \end{cases} \quad (3.18)$$

или после сведения ее к однокритериальной:

$$\begin{cases} D(C_{инф}, P_{взл}) \rightarrow \max; \\ C_{сзи} \leq C_{зад}; \\ d\Pi_{сзи} \leq d\Pi_{зад}, \end{cases} \quad (3.19)$$

где $C_{зад}$ и $d\Pi_{зад}$ - заданные ограничения на стоимость системы защиты и снижение производительности.

Следует отметить, что именно такой принцип сведения задачи к однокритериальной целесообразен, т.к. в любом техническом задании на разработку системы защиты указывается, в какой мере система защиты должна оказывать влияние на производительность системы. Как правило, внедрение системы защиты не должно снижать производительность системы более чем на 10%. Кроме того, обычно вводится ограничение на стоимость системы защиты.

Если рассчитанное значение коэффициента защищенности (D) не удовлетворяет требованиям к системе защиты, то в допустимых пределах можно изменять заданные ограничения и решить задачу методом последовательного выбора уступок. При этом задается приращение стоимости и снижение производительности: $C_{зад} = C_{зад} + \Delta C_{зад}$;

$$\Pi_{зад} = \Pi_{зад} + \Delta \Pi_{зад}; d\Pi_{зад} = d\Pi_{зад} + \Delta d\Pi_{зад}.$$

В таком виде задача решается в результате реализации итерационной процедуры путем отсеивания вариантов, не удовлетворяющих ограничительным условиям, и последующего выбора из оставшихся варианта с максимальным коэффициентом защищенности.

Теперь выразим коэффициент защищенности через параметры угроз. В общем случае в системе присутствует множество видов угроз. В этих условиях зададим следующие величины:

w – количество видов угроз, действующих на систему;

C_i ($i = 1, \dots, w$) – стоимость (потери) от взлома i -го вида;

λ ($i=1, \dots, w$) – интенсивность потока взлома i -го вида, соответственно;

Q_i ($i=1, \dots, w$) – вероятность появления угроз i -того вида в общем потоке попыток несанкционированного доступа к информации, причем $Q_i = \lambda / \Lambda$;

p_i ($i=1, \dots, w$) – вероятность отражения угроз i -го вида системой защиты.

Соответственно, для коэффициента потерь от взломов системы защиты имеем:

$$R(p) = \sum_1^w Ri(p) = \sum_1^w Ci \cdot p_{взл} \quad (3.20)$$

где $Ri(p)$ – коэффициент потерь от взлома i -го типа.

Для незащищенной системы $p_{взл} = Q_i$, а для защищенной системы $p_{взл} = Q_i \cdot (1 - p_i)$.

Соответственно коэффициент потерь от взлома системы защиты в единицу времени будет:

$$R(\lambda) = \sum_1^w Ri(\lambda) = \sum_1^w Ci \cdot \lambda_{взл} \quad (3.21)$$

где $Ri(\lambda)$ – коэффициент потерь от взлома i -го типа в единицу времени.

Для незащищенной системы $\lambda_{взл} = \lambda$, а для защищенной системы $\lambda_{взл} = \lambda \cdot (1 - p_i)$. Соответственно, из (3.15) имеем:

$$\begin{aligned} D &= 1 - (\sum_1^w Ci \cdot Q_i \cdot (1 - p_i)) / (\sum_1^w Ci \cdot Q) = \\ &= 1 - (\sum_1^w Ci \cdot \lambda_i \cdot (1 - p_i)) / (\sum_1^w Ci \cdot \lambda_i) \end{aligned} \quad (3.22)$$

Если в качестве исходных параметров заданы вероятности появления угроз Q , то коэффициент защищенности удобно считать через вероятности появления угроз. Если же в качестве исходных параметров заданы интенсивности потоков угроз λ_i , то, естественно, коэффициент защищенности считается через интенсивность

Способы задания исходных параметров для оценки защищенности.

При использовании любого математического метода проектирования системы защиты необходимо задавать определенные исходные параметры для оценки ее защищенности. Однако именно с

этим связаны основные проблемы формализации задачи синтеза системы защиты. Поэтому надо отдельно рассмотреть основные пути решения данной задачи.

Способы задания вероятностей и интенсивностей угроз.

Основной проблемой проведения количественной оценки уровня защищенности является задание входных параметров для системы защиты - вероятностей и интенсивностей угроз. Рассмотрим возможные способы задания вероятностей и интенсивностей угроз.

1. *Метод статистической оценки $\lambda_i(Q)$ и p_i .* Основным способом задания интенсивностей потоков угроз λ_i , (вероятностей угроз Q .) и вероятностей взломов p_i является получение этих значений на основе имеющейся статистики угроз безопасности информационных систем, в которых реализуется система защиты. Если существует статистика для аналогичной информационной системы, то задавать исходные параметры для оценки защищенности можно на ее основе. При этом желательно, чтобы сходные информационные системы эксплуатировались на предприятиях со сходной спецификой деятельности.

Статистика угроз периодически публикуется достаточно авторитетными изданиями, т.е. всегда существуют исходные данные для использования данного подхода для большинства приложений средств защиты информации. Обычно эта статистика доступна в Интернете на сайтах специализированных организаций.

Если же необходимая статистика по угрозам безопасности отсутствует, то можно воспользоваться одним из других подходов, описанных далее.

2. *Оптимистически-пессимистический подход.* В рамках данного подхода предусмотрено два разных способа.

Первый способ — *это способ равных интенсивностей $\lambda_i = \alpha$, $\alpha = const$.* При этом способе для расчета защищенности константа α может быть выбрана любой. В формуле (3.22) она будет вынесена за скобки и в конечном итоге сократится, так что защищенность в данном случае будет зависеть только от потерь:

$$\begin{aligned} D &= 1 - (\sum_1^w C_i \cdot \lambda_i \cdot (1 - p_i)) / (\sum_1^w C_i \cdot \lambda_i = \\ &= 1 - (\sum_1^w C_i \cdot \alpha \cdot (1 - p_i)) / (\sum_1^w C_i \cdot \alpha = \\ &= 1 - (\alpha \sum_1^w C_i \cdot (1 - p_i)) / (\alpha \sum_1^w C_i = \\ &= 1 - (\sum_1^w C_i \cdot (1 - p_i)) / (\sum_1^w C_i. \end{aligned} \quad (3.23)$$

Второй способ – способ пропорциональности потерям:
 $\lambda = \alpha \cdot$, $\alpha = const$.

При этом способе предполагается, что чем больше потери от взлома, тем чаще осуществляются попытки несанкционированного доступа к этой информации. То есть интенсивности потоков угроз прямо пропорциональны потерям. В этом случае защищенность будет зависеть от квадрата потерь:

$$\begin{aligned} D &= 1 - (\sum_1^w C_i \cdot \lambda_i \cdot (1 - p_i)) / (\sum_1^w C_i \cdot \lambda_i = \\ &= 1 - (\sum_1^w C_i \cdot \alpha \cdot C_i \cdot (1 - p_i)) / (\sum_1^w C_i \cdot \alpha \cdot C_i = \quad (3.24) \\ &= 1 - (\alpha \sum_1^w C_i^2 \cdot (1 - p_i)) / \alpha \sum_1^w C_i^2. \end{aligned}$$

3. *Метод экспертной оценки.* Экспертная оценка исходных параметров для расчета защищенности может осуществляться с использованием так называемой *дельфийской группы*. Дельфийская группа - это группа экспертов, созданная в целях сбора информации из определенных источников по определенной проблеме.

При этом необходимо задать лингвистический словарь возможных оценок экспертов, определить набор вопросов и условных значений квалификаций отдельных экспертов. После определения всех входных переменных производится поочередный опрос каждого эксперта. После опроса всех экспертов с учетом их квалификации определяется общая оценка группы и согласованность (достоверность) ответов для каждого вопроса.

Эксперт оценивает эффективность (вероятность) отражения угроз элементами защиты и вероятность появления угроз. Вероятности эксперт задает лингвистическими оценками: отлично, хорошо, удовлетворительно, плохо, не отражает; вероятно, близко к нулю, близко к единице, весьма вероятно и т.п. Затем эти лингвистические оценки при помощи словаря переводятся в числа p_i и Q_i в диапазоне $[0, \dots, 1]$.

Для задания

вероятности появления угрозы возможна оценка вероятности появления угрозы i -того вида в общем потоке угроз:

$$Q = \lambda i / \sum \lambda i. \quad (3.25)$$

Исходя из заданной квалификации экспертов, рассчитываются их веса (значимость) в группе по формуле:

$$k_e = Se / \sum Se, \quad (3.26)$$

где Se — квалификация эксперта, задаваемая в некотором диапазоне, например, от 0 до 10 в зависимости от опыта, образования и других качеств эксперта.

Затем оценки суммируются с учетом весов экспертов:

$$\begin{aligned} p_i &= \sum p_k \cdot k_e, \\ Q &= \sum Q_k \cdot k_e, \end{aligned} \quad (3.27)$$

где p_k и Q_k — оценки вероятностей отражения и появления угроз, сделанные одним из экспертов; k_e — «вес» эксперта в группе.

После расчета общей оценки всей группы рассчитывается согласованность ответов, которая может использоваться для оценки достоверности результатов. Согласованность рассчитывается при помощи среднеквадратического отклонения и выражается в процентах.

Максимальная согласованность достигается при одинаковых значениях оценок экспертов и в этом случае равняется 100%. Минимальная согласованность достижима при максимальном разбросе оценок экспертов

Способы задания стоимости потерь.

Важнейшей характеристикой защищаемого объекта (как следствие, и системы защиты) является стоимость потерь от взлома. Рассмотрим возможные способы задания стоимости потерь.

1. *Стоимость похищенной/искаженной/утраченной информации* ($C_{in/u/y}$).

Исходные данные:

$c_{инф}$ [руб./бит] — удельная цена информации;

v [бит/с] — скорость получения/искажения/уничтожения информации;

t [с] — время нахождения субъекта в системе;

V [бит] — объем информации.

$$C_{in/u/y} = \min(c_{инф} \cdot v \cdot t \cdot V) \quad (3.28)$$

3. Затраты от невозможности получения доступа к информации (инди).

Исходные данные:

$c_{инди}$ [руб./бит] - удельная цена недоступности информации;

$t_{вс}$ – время восстановления системы.

$$C_{инди} = c_{инди} \cdot t_{вс} \quad (3.29)$$

Способы задания соответствия между параметрами угроз, параметрами защищаемых объектов и параметрами элементов защиты.

Существуют различные классификации угроз:

- по принципам и характеру воздействия на систему;
- по используемым техническим средствам;
- по целям атаки и т.п.

Очевидно, что стоимость потерь C_i удобнее задавать для угроз, классифицированных по целям атаки. Что касается характеристики интенсивности угроз, то она определяется с помощью средств аудита и сетевого мониторинга, которые различают угрозы по принципам и характеру воздействия на систему (механизму атаки, способу проникновения). Вероятность отражения угрозы средствами защиты p_i определяется в соответствии с теми механизмами, которые реализованы в каждом средстве. Причем каждый из механизмов в общем случае может отражать несколько видов атак.

Таким образом, необходимо задавать соответствие между всеми этими параметрами (см. рис. 3.14). Для успешного приведения в соответствие различных параметров оценки защищенности необходимо корректное построение модели нарушителя. В этой модели должны быть отражены практические и теоретические возможности нарушителя, его априорные знания, время и место действия

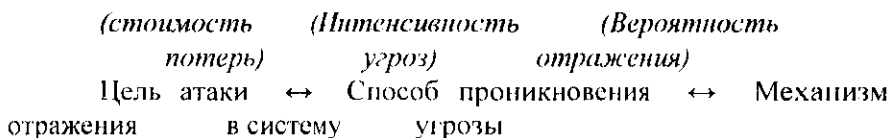


Рис. 3.14. Взаимосвязь параметров защиты

Задание соответствия между стоимостью потерь и

интенсивностью угроз.

Задание соответствия между стоимостью потерь и интенсивностью угроз можно осуществлять следующим образом:

1. *Статистический подход.* Статистический подход является основным, как обладающий большей достоверностью. Из анализа статистики можно выявить вероятности нанесения определенных видов ущерба при определенных видах взломов. Однако на практике далеко не всегда подобная статистика существует, в частности, при внедрении новых технологий защиты информации, новых версий ОС или приложений и т.д., т.к. для ее сбора требуется некоторое время. В этом случае может использоваться пессимистический подход.

2. *Пессимистический подход.* Если не имеется достаточной статистики, можно воспользоваться другим способом. Будем считать, что при проникновении в систему злоумышленник наносит наибольший вред, какой он только может причинить.

При задании соответствия между интенсивностью угроз и вероятностью их отражения нужно учитывать, что, если в системе реализовано несколько механизмов, отражающих некоторую атаку, вероятность преодоления защиты рассчитывается следующим образом.

Если p_k есть вероятность отражения i -ой угрозы каждым средством защиты, то вероятность взлома системы ($1/p_i$) будет:

$$1/p_i = \prod_k (1 - p_k). \quad (3.30)$$

А вероятность отражения угрозы системой защиты будет:

$$p_i = 1 - 1/p_i. \quad (3.31)$$

Особенности проектирования системы защиты на основе оценки защищенности системы.

Этапы проектирования системы защиты.

Задача проектирования системы защиты принципиально отличается от задач проектирования иных информационных систем. Дело в том, что проектирование осуществляется с учетом статистических данных об уже существующих угрозах. Однако, в процессе функционирования системы защиты поле угроз может принципиально измениться. В частности, это связано с тем, что многие угрозы предполагают нахождение злоумышленниками ошибок в реализации системных и прикладных средств, которые

могут быть неизвестны на момент создания системы защиты, но должны быть учтены в процессе ее функционирования.

Поэтому проектирование системы защиты - процедура итерационная, в общем случае предполагающая следующие этапы:

1. Проектирование первоначальной системы защиты (исходный вариант);

2. Анализ защищенности на основе статистических данных, полученных в процессе эксплуатации системы защиты;

3. Модификация «узких мест» системы защиты (настройка/замена/дополнение отдельных механизмов защиты информации).

После модификации «узких мест» происходит возврат к эксплуатации системы защиты и накопление статистической информации.

Этапы оценки защищенности и выбора оптимального варианта системы защиты.

Оценка защищенности с учетом приведенных выше расчетных формул и выбор оптимального варианта системы защиты (необходимого набора механизмов защиты при разработке новой системы) осуществляется следующим образом:

1. Расчет параметров C' , λ , p_i для оценки защищенности по исходным данным, полученным статистическим или, в случае недостатка статистики, одним из приведенных выше способов (оптимистически-пессимистический подход, метод экспертной оценки).

2. Расчет критериев защищенности D , $C_{сш}$, $P_{сш}$ ($dP_{сш}$) для каждого варианта системы защиты (набора механизмов защиты при разработке новой системы).

3. Выбор системы защиты (набора механизмов защиты при разработке системы) с максимальным коэффициентом защищенности D , удовлетворяющей ограничениям по стоимости $C_{сш}$ и производительности $P_{сш}$.

4. Анализ изменения коэффициента защищенности dD при задании приращений для критериев $C_{сш}$ и $dP_{сш}$ методом последовательного выбора уступок с оценкой целесообразности выбора системы, удовлетворяющей новым ограничениям.

Последовательность задач, решаемых при проектировании системы защиты. Требование непрерывности проектирования.

Последовательность задач, решаемых при проектировании системы защиты следующая:

1. Назначение ограничений: $C_{зад}$ и $P_{зад}$;
2. Получение параметров: C', λ, p_i ;
3. Расчет параметров элементов защиты: $C_{сзи}$ и $P_{сзи}$;
4. Разработка вариантов построения СЗИ;
5. Выбор лучшего варианта СЗИ;
6. Анализ влияния ограничений на уровень защищенности;
7. Выбор оптимальной СЗИ.

С учетом сказанного ранее можем сделать следующий важный вывод: *проектирование системы защиты - это непрерывный процесс, осуществляемый в течение всего жизненного цикла системы, предполагающий исходное проектирование системы по расчетным значениям параметров и последующую ее модификацию (доработку), основанную на непрерывном анализе текущего состояния обеспечиваемого системой уровня защищенности средствами мониторинга с учетом меняющегося поля угроз.*

Модификация «узких мест» системы защиты предполагает выявление новых угроз и анализ их отражения механизмами защиты, присутствующими в системе. При необходимости следует либо модифицировать существующие механизмы, либо встраивать новые.

Таким образом, с учетом сложности формализации задачи (особенно при задании исходных параметров), можно выделить характерную особенность проектирования системы защиты. В общем случае она заключается в невозможности реализовать гарантированную защиту информационной системы при условии ее проектирования *исключительно* по расчетным значениям параметров без последующего мониторинга защищенной системы. При этом в задачи мониторинга входит сбор статистики для задания параметров конкретной системы защиты, а также ее повторный расчет в рамках полученной статистики. Результатом повторного расчета будет обоснование оптимальности принятых на этапе проектирования технических решений и их соответствующая корректировка.

Метод последовательного выбора уступок.

Качественная зависимость изменения основных параметров, характеризующих систему защиты, от нее сложности — используемого набора механизмов защиты: нелинейные функции. Анализ характера зависимостей от сложности системы показал, что стоимость системы защиты возрастает неограниченно, а производительность снижается в пределе до нуля.

В то же время кривая защищенности (D) стремится к предельному значению – к единице (100%) и в некоторый момент достигает насыщения. Это приводит к тому, что при дальнейшем нарастании сложности (и, следовательно, увеличении цены, а также снижении производительности) увеличение коэффициента защищенности происходит незначительно.

Следовательно, при проектировании системы защиты, параметры защищенности которой расположены в области насыщения, целесообразно проанализировать параметры альтернативных вариантов. То есть целесообразно исследовать возможность использования менее сложных систем защиты и, задав некоторый промежуток снижения коэффициента защищенности (dD), выбрать систему, уровень защищенности которой удовлетворяет полученному ($D - dD$). Конечно, если таковые имеются. При этом может быть получен ощутимый выигрыш в цене и производительности.

В этом и состоит применение известного метода последовательных уступок при выборе оптимальной системы защиты (набора реализуемых механизмов защиты при ее проектировании). Этот метод, как уже упоминалось, подразумевает сведение многокритериальной задачи оптимизации к однокритериальной.

Метод последовательных уступок представляет собою итерационную человеко-машинную процедуру, используя которую разработчик, давая допустимые приращения одним параметрам (в частности, задавая снижение коэффициента защищенности), анализирует изменение других, принимая решение о допустимости вводимых уступок.

Методы проектирования системы защиты с избыточными механизмами защиты.

Необходимость избыточных механизмов в системе защиты.

Ранее была отмечена принципиальная особенность функционирования системы защиты. Суть ее заключается в том, что коэффициент защищенности непрерывно снижается в процессе функционирования защищенной системы. Это связано с накоплением информации злоумышленником о системе защиты, а также с накоплением статистики об ошибках реализации системных и прикладных средств.

Возникает следующая проблема. Если строить систему с требуемым уровнем защищенности (учитывающим текущую статистику угроз), то через небольшой промежуток времени

функционирования защищаемой системы систему защиты потребуется проектировать вновь, что связано с большими накладными расходами. Поэтому ранее был сделан вывод о необходимости разработки системы защиты с учетом не только существующей статистики угроз, но и с учетом потенциально возможных (неизвестных) угроз. Тем не менее приходится учитывать тот факт, что наличие запаса по параметрам защищенности приводит к значительным накладным расходам, прежде всего, по параметрам производительности.

Что касается стоимости, то лучше раз создать систему с избыточными механизмами защиты и заплатить изначально больше, чем практически сразу после ее внедрения вновь проектировать систему защиты, т.е. вновь оплачивать все расходы, связанные с этим проектированием, да еще думать об очередном ее внедрении в функционирующую систему, что, как правило, протекает весьма болезненно.

Из сказанного можем сделать важнейший вывод [18]: *с целью увеличения жизненного цикла системы защиты (без необходимости ее модификации) разработчикам следует ориентироваться не только на существующую статистику угроз, но и закладывать технические решения, позволяющие противодействовать неизвестным на момент проектирования системы защиты угрозам (потенциальным угрозам).*

Следует обратить внимание на принципиальную разницу между подходами резервирования и подходами включения избыточных механизмов. При резервировании, рассмотренном ранее в п. 3.3.1.3, механизмы защиты дублируются такими же механизмами (решают те же функциональные задачи), но реализуются иным способом. Резервный призван заменить основной механизм при выходе его из строя (при обнаружении его уязвимости к атакам).

Что касается включения избыточных механизмов, то здесь рассматривается добавление новых механизмов с иными, чем у механизмов, реализованных в системе защиты, свойствами (решающих частично, либо полностью иные функциональные задачи). Другое дело, что данные возможности на первых этапах функционирования системы защиты могут быть не востребованными. Поэтому, чтобы не загружать излишне вычислительные ресурсы системы, их рекомендуется не активизировать - благодаря избыточным механизмам реализуется запас защищенности.

Подходы к проектированию систем защиты, обладающих

избыточными механизмами. *Метод динамического анализа*

Классификация возможных подходов к проектированию рассматриваемых систем защиты следующая:

Методы построения систем защиты:

1. *Количественная оценка защищенности:*
 - 1.1. *При проектировании:*
 - 1.1.1. *Метод полного проектирования;*
 - 1.1.2. *Метод необходимого минимума;*
 - 1.1.3. *Метод динамического анализа.*
 - 1.2. *При эксплуатации:*
 - 1.2.1. *Метод динамического анализа;*
 - 1.2.2. *Метод мониторинга безопасности.*
2. *Качественная оценка защищенности:*
 - 2.1. *При проектировании:*
 - 2.1.1. *Метод полного проектирования;*
 - 2.1.2. *Метод необходимого минимума;*
 - 2.1.3. *Метод динамического анализа.*
 - 2.2. *При эксплуатации:*
 - 2.2.1. *Метод динамического анализа;*
 - 2.2.2. *Метод мониторинга безопасности.*

Альтернативные подходы составляют *метод необходимого минимума и метод полного перекрытия.*

Метод необходимого минимума состоит в поиске варианта построения системы по характеристике требуемого уровня защищенности. Метод полного перекрытия состоит в исходной реализации избыточности механизмов, что изначально позволяет построить систему защиты с большим запасом в характеристике защищенности.

Как отмечалось, данные подходы характеризуются следующими недостатками:

- метод необходимого минимума с учетом специфики функционирования рассматриваемого класса систем позволяет построить систему практически без запаса защищенности, что потребует ее достаточно скорого проектирования заново;
- метод полного перекрытия связан с существенными затратами, прежде всего в производительности системы.

Проведя анализ, можно констатировать, что *метод динамического анализа* – это наиболее обоснованный подход к проектированию для исследуемой области приложений. Суть этого метода состоит в выполнении следующих действий:

1. Исходя из возможных затрат на систему защиты, выбирается вариант, обеспечивающий максимальный уровень защищенности (при условии, что он не ниже требуемого). Причем это делается в рамках заданных ограничений на параметр производительности.

2. Затем, в рамках выбранного варианта, определяется набор механизмов защиты и их параметры, которые должны быть включены для обеспечения требуемого уровня защищенности. Остальные механизмы находятся в резерве - выключены (по существу данная задача аналогична исходной, так как определение набора изначально включенных механизмов защиты является той же задачей, что и определение варианта построения системы защиты).

3. При внедрении в систему включаются лишь необходимые механизмы, но система обладает резервом в защищенности, который может постепенно выбираться при снижении уровня защищенности.

4. В процессе функционирования системы собирается необходимая статистика о параметрах системы (реализуется метод статистической оценки) с использованием которой непрерывно оценивается уровень защищенности системы (посредством представленных ранее формул).

5. При снижении уровня защищенности ниже заданного порогового значения включаются избыточные механизмы защиты, что позволяет поддерживать требуемый уровень защищенности в течение некоторого времени функционирования системы (естественно, тем большего, чем выше исходные затраты на систему защиты).

Таким образом, особенностью метода динамического анализа является то, что исходно создается некоторый запас в механизмах защиты, что обеспечивает уровень защищенности выше необходимого на текущий момент. Вместе с тем, данные механизмы при внедрении системы защиты в эксплуатацию изначально не используются. Они находятся в резерве.

В результате, использование избыточных механизмов в системе защиты позволяет реализовать требуемый уровень защищенности без дополнительного снижения производительности. Это по существу и отличает данный подход от метода полного перекрытия. При снижении же уровня защищенности ниже требуемого порога (обнаружении новых угроз) будут подключаться избыточные механизмы.

Активация избыточных механизмов (которые при этом

становятся основными) защиты приводит к соответствующему снижению производительности системы. Однако надо отметить, что вывод из резерва новых механизмов может привести к целесообразности отключения некоторых задействованных механизмов на основании частичного дублирования выполняемых ими функций. В результате это позволит минимизировать влияние системы защиты на производительность защищаемого объекта.

Таким образом, метод динамического анализа представляет собою разумный компромисс, состоящий в следующем: чтобы обеспечить жизнеспособность системы защиты, вносятся дополнительные функции защиты (дополнительные относительно возможности обеспечения текущего уровня защищенности). Однако они не включаются при внедрении системы защиты, а помещаются в резерв. Это позволяет обеспечить максимальную производительность системы при требуемой текущей защищенности. Снижение производительности будет происходить по мере подключения резервных механизмов защиты при необходимости повышения уровня защищенности.

Важнейшим требованием к реализации описанного метода является непрерывная оценка защищенности системы, т.е. здесь должна быть реализована система мониторинга защищенности, решающая следующие задачи:

- непрерывный сбор статистики и расчет текущих значений параметров защищенности;
- оценка уровня защищенности системы и его сравнение с пороговым значением;
- выработка рекомендаций по включению зарезервированных механизмов защиты при снижении текущего уровня защищенности ниже порогового значения.

Таким образом, для выработки рекомендаций опять же осуществляется сравнение возможных вариантов защиты с использованием рассмотренных подходов. При этом варианты различаются набором включаемых механизмов, а параметры защищенности определяются уже на основании собранной статистики о конкретной системе.

3.3.2. Архитектурные принципы построения систем защиты информации

Рассмотрим основные архитектурные принципы построения

системы защиты, определим ее состав и назначение основных функциональных блоков.

Система защиты компьютерной информации от НСД может рассматриваться в двух приложениях:

- защита автономного компьютера;
- защита компьютера в составе сети

Далее рассматриваются вопросы защиты компьютера в составе ЛВС, так как задача защиты компьютера как самостоятельного объекта, предназначенного для хранения и обработки информации, должна решаться в обоих случаях.

3.3.2.1. Системный подход в проектировании систем защиты

До этого каждый из механизмов защиты рассматривался и анализировался по отдельности. Однако на практике все они реализуются в рамках одной системы защиты, а потому нельзя не учитывать их взаимное влияние. Поэтому уже на начальном этапе проектирования системы защиты необходимо придерживаться системного подхода, в рамках которого механизмы защиты рассматриваются и проектируются в совокупности.

Таким образом, при проектировании системы необходимо учитывать следующие аспекты:

- комплексирование разнородных механизмов в единой системе;
- взаимное влияние защитных механизмов;
- оптимальность системы защиты;
- ориентацию на статистику угроз.

Каждый из этих аспектов требует подробного рассмотрения.

Комплексирование разнородных механизмов в единой системе.

Никакой, даже блестяще реализованный, механизм защиты в отдельности не сможет обеспечить качественной защиты в целом. Защита информации требует комплексирования разнородных механизмов в единой системе. Причем при проектировании системы следует анализировать не отдельно взятые механизмы, а решение конкретной задачи обеспечения безопасности всей системой защиты в целом, то есть реализованной совокупностью механизмов.

Таким образом, далее будем говорить о требованиях к заданным свойствам защищенности, обеспечиваемых совокупностью реализованных защитных механизмов. Например, целесообразно

говорить не о том, что в системе защиты должен быть реализован механизм авторизации пользователя при длине пароля не менее определенного числа символов, а о том, что в системе должна быть обеспечена защита входа в систему с определенными характеристиками, а также и о совокупности механизмов защиты, обеспечивающих надежную авторизацию пользователя. Причем делать это нужно с учетом того, что существуют способы преодоления данного механизма в отдельности, например, с использованием программ-снифферов, программ подбора паролей и др.

Необходимые характеристики могут быть заданы либо количественно, либо качественно. В частности, при качественном задании характеристик целесообразно задать угрозы (из существующей статистики и возможные - потенциальные), которым необходимо противодействовать при решении задачи входа в систему.

Взаимное влияние различных механизмов защиты.

Другая сторона проблемы заключается в том, что использование одного механизма защиты может существенно изменить требования к реализации другого механизма. То есть, требования к отдельному механизму могут быть существенно снижены за счет расширения функций другого механизма.

Рассмотрим пример. В системе защиты должен быть реализован механизм гарантированной очистки остаточной информации на жестком диске. Но для просмотра остаточной информации злоумышленнику необходимо запустить соответствующую специальную программу, поскольку из обычных широко используемых приложений доступ к такой информации не получить (приложения не предоставляют подобной возможности). Однако, если в системе корректно реализован и активен важнейший механизм защиты - механизм обеспечения замкнутости программной среды, то данная скрытая угроза ликвидируется этим механизмом. При этом пользователю разрешается запускать только санкционированные для него процессы, а значит, пользователь не сможет запустить программу, предоставляющую возможность доступа к остаточной информации.

Получаем, что требования к очистке внешней памяти при корректной реализации механизма обеспечения замкнутости программной среды могут быть существенно снижены. При этом в качестве замечания отметим, что реализация данного требования весьма ресурсоемка, то есть приводит к существенному увеличению

загрузки вычислительного ресурса.

Оптимальность системы защиты.

Как отмечено ранее, реализация системы защиты влияет на другие параметры защищаемого объекта, прежде всего, на его производительность (загрузку вычислительного ресурса защищаемого компьютера). Это обуславливает необходимость выбора оптимальных решений, при этом оптимальность должна рассматриваться по совокупности параметров. Способ учета разнородных параметров при проектировании системы защиты уже был рассмотрен в п.3.3.1.3.

Ориентация на статистику угроз.

При проектировании системы защиты целесообразно ориентироваться на существующую статистику угроз. При этом ориентироваться нужно только в смысле иллюстрации возможностей того, либо иного механизма защиты. Недопустимой является разработка механизмов защиты под конкретную угрозу.

Системный подход предполагает проектирование системы защиты в предположении, что существуют потенциальные (неизвестные) угрозы, которые характеризуются скрытыми (неявными) каналами ИСД. Поэтому при проектировании системы защиты необходимо рассматривать не конкретные угрозы, а характерные признаки их возникновения и противодействовать не угрозам, а возможным каналам их возникновения.

Принципы системного подхода при проектировании системы защиты.

Все вышесказанное позволяет сформулировать принципы системного подхода при проектировании системы защиты:

1. Любой механизм защиты должен проектироваться с учетом его влияния на безопасность системы в целом и с учетом функций защиты, реализуемых другими механизмами. То есть должно выполняться классическое условие системного проектирования - учитываться влияние подсистемы на систему в целом, состоящую из совокупности подсистем.

2. Проектирование системы защиты- многокритериальная задача. Поэтому при разработке механизма защиты должен учитываться не только обеспечиваемый им уровень безопасности, но и, по крайней мере, его влияние на производительность защищаемого объекта.

3. Проектирование системы защиты должно осуществляться в предположении существования потенциальных (неизвестных)

угроз, которые характеризуются скрытыми (неявными) каналами НСД. При этом необходимо рассматривать не конкретные угрозы, а характерные признаки их возникновения и противодействовать не угрозам, а возможным каналам их возникновения.

Особенности системного подхода к проектированию системы защиты компьютерной информации в составе ЛВС.

Особенности и проблемы защиты компьютерной информации в составе ЛВС.

В части защиты компьютерной информации в составе ЛВС, кроме решения задачи защиты отдельного компьютера, возникает и задача защиты взаимодействия защищаемых объектов между собой. При этом компьютер уже должен рассматриваться не только (а при определенной технологии обработки и хранения информации - и не столько) как самостоятельный объект, требующий защиты, но и как средство удаленного доступа к другим защищаемым объектам информации.

В частности, рабочую станцию можно рассматривать, как средство удаленного, в том числе, возможно, и несанкционированного доступа к серверу, на котором хранится защищаемая информация. Причем на самой рабочей станции защищаемой информации может и не храниться.

Отметим, что защита информации в составе ЛВС по-прежнему реализуется средствами, устанавливаемыми на компьютеры (рабочие станции и серверы) в составе ЛВС. При этом, возможности механизмов защиты должны быть соответствующим образом функционально расширены.

Другой особенностью построения системы защиты в составе ЛВС является возможность реализации в ЛВС выделенного рабочего места администратора безопасности (сервера безопасности). С учетом требований к оперативности принятия решений в распределенной системе защиты это становится необходимостью.

В функции администратора входят:

- удаленное управление средствами защиты информации, установленными на компьютеры в составе ЛВС;
- контроль за действиями пользователей на защищаемом объекте;
- оперативная обработка регистрационной информации (данных аудита), формируемой механизмами защиты;
- выработка реакций на определенные виды событий и т.д.

В общем случае проблема проектирования систем защиты

информации в ЛВС связана либо с различными уровнями конфиденциальности, либо с различным функциональным назначением информации, обрабатываемой и циркулирующей в сети. Как следствие, возникают проблемы с требованиями к ее защите в рамках одной системы.

Очевидно, что говорить о разумной достаточности средств защиты невозможно без учета уровня критичности или конфиденциальности (назначения) обрабатываемой информации. При этом, как правило, реализуемые в сети информационные системы характеризуются несколькими типами потоков обрабатываемой информации. Примерами могут служить: внешний Web-сервер корпорации, доступ к которому разрешен практически с любой рабочей станции сети Internet; внешний и внутренний файловые серверы корпорации, предполагающие уже существенное разграничение прав доступа к ним; внутренний сервер баз данных, на котором может храниться конфиденциальная (например, финансовая) информация корпорации и др.

Задачи системного подхода при проектировании системы защиты ЛВС.

Системный подход при проектировании системы защиты ЛВС с различным уровнем конфиденциальности (назначения) обрабатываемой в ней информации состоит в решении следующей совокупности задач [18]:

- выделение фрагментов сети (информационных подсистем), обрабатывающих соответствующие информационные потоки различных уровней конфиденциальности (назначения);

- проектирование систем защиты каждого отдельного информационного потока в соответствии с требованиями к защищенности системы, обрабатывающей информацию данного уровня конфиденциальности (назначения). Заметим, что если несколько различных (в смысле уровня конфиденциальности) потоков обрабатываются одной подсистемой, то подсистема защищается по требованиям к параметрам защиты более конфиденциального потока информации;

- проектирование системы защиты для интерфейсов взаимодействия подсистем обработки информационных потоков различных уровней конфиденциальности (назначения).

Таким образом, основу рассматриваемого подхода составляет деление (фрагментация) системы на подсистемы с последующей защитой отдельных подсистем и соответствующих интерфейсов.

Информационные потоки будем считать различными при различии их конфиденциальности (назначения), в конечном итоге — при различии требований к их информационной безопасности. Информационные потоки будем считать одинаковыми (без анализа их функционального назначения) при совпадении требований к их информационной безопасности.

Задачу разделения различных информационных потоков можно решать либо на физическом уровне, либо на виртуальном - с использованием средств защиты, устанавливаемых на компьютер.

Практические шаги по построению системы информационной защиты ЛВС в рамках системного подхода.

Основу применения системного подхода составляет решение следующей совокупности задач проектирования системы защиты:

1. Выделяются информационные потоки, защиту которых необходимо обеспечить.

2. Для защиты каждого информационного потока устанавливается *виртуальная система защиты информационного потока* (ВСЗИП). «Виртуальная» — понимается в том смысле, что система может представлять собою некоторое программное обеспечение, устанавливаемое на существующих технических средствах обработки информации. Однако она может требовать использования выделенного технического средства защиты, либо некоторой их совокупности.

3. Для разделения информационных потоков и защиты интерфейсов взаимодействия подсистем в местах их функционального объединения устанавливаются *виртуальные системы разделения информационных потоков* (ВСРИП).

4. Разрабатываются достаточные требования к защищенности информационных потоков информационной системы с учетом конфиденциальности (назначения) информации, принадлежащей анализируемому информационному потоку (вопросы достаточности требований рассмотрены в п. 3.3.1.3.).

5. Разрабатываются требования к ВСЗИП.

6. Разрабатываются требования к дополнительным системам защиты информации, устанавливаемым на компьютеры в составе ЛВС.

7. Разрабатываются требования к ВСРИП, к которым могут быть отнесены:

- требования к архитектуре информационной системы в целом;

- требования к дополнительным средствам защиты информации, используемым для разделения информационных потоков.

Следует отметить, что описанный системный подход к проектированию систем защиты целесообразно использовать и для проектирования комплекса организационно-технических мероприятий по обеспечению информационной безопасности информационных систем. Важным при этом будет то, что организационно-технические мероприятия разрабатываются применительно к конкретному информационному потоку с учетом его конфиденциальности (назначения).

3.3.2.2. Архитектура системы защиты

Объекты угроз.

Классификация угроз по способу их осуществления.

В п. 3.3.1.2. была представлена классификация угроз, введенная исходя из проанализированной статистики. Здесь рассмотрим иную классификацию (которую также можно ввести, анализируя существующую статистику угроз), а именно классификацию угроз по способу их осуществления. Эта классификация необходима для формирования задач добавочной защиты информации:

1. Угрозы:

1.1. Явные:

1.1.1. Некорректность реализации механизма защиты.

1.1.2. Некорректность (противоречивость) возможных настроек механизмов защиты.

1.1.3. Неполнота покрытия доступа к информации защиты.

1.2. Скрытые:

1.2.1. Нерегламентированные действия пользователя.

1.2.1.1. Собственные программы пользователя.

1.2.2. Ошибки и закладки в ПО.

Явные угрозы.

В соответствии с данной классификацией угрозы компьютерной безопасности подразделяем на явные и скрытые. Под явными - понимаем такие угрозы, которые понятны и однозначно предсказуемы. Они не требуют для противодействия им каких-либо

дополнительных сведений о статистике угроз и неочевидных предположений о возможных атаках злоумышленника.

Явные угрозы связаны с некорректной реализацией и настройкой системы защиты. К таковым могут быть отнесены:

- некорректность реализации механизма защиты;
- неполнота покрытия каналов доступа к информации механизмами защиты;
- некорректность (противоречивость) возможных настроек механизмов защиты.

Рассмотрим их кратко.

Некорректность реализации механизма защиты может быть проиллюстрирована на ОС Windows 2000/XP: невозможность разграничить доступ к устройствам ввода «на исполнение», что позволяет пользователю запускать любые программы с внешних носителей.

Неполнота покрытия каналов доступа к информации механизмами защиты может быть проиллюстрирована невозможностью управления доступом к некоторым ресурсам защищаемого объекта, например, к виртуальному каналу связи и т.д. При этом ресурсы могут быть как локальными, так и сетевыми - в составе ЛВС.

Некорректность (противоречивость) возможных настроек механизмов защиты может рассматриваться в двух аспектах: собственно некорректность настроек и некорректность механизма (способа) задания настроек.

В первом случае речь идет о невозможности для механизма защиты задания корректных настроек как таковых, например, если для мандатного механизма управления доступом не реализован принцип задания настроек «все, что не разрешено, то запрещено».

Во втором случае речь идет о настройке механизмов защиты в иерархической системе, где настройки может осуществлять администратор безопасности, администратор СУБД и приложения, пользователь и т.д. Например, пользователь в ОС самостоятельно может разделять (делать доступными из сети) ресурсы, к которым ему разрешен доступ, администратор СУБД может осуществлять настройки встроенных в СУБД механизмов защиты, а пользователь самостоятельно может делегировать свою роль. В то же время ранее было показано, что задача управления безопасностью должна

решаться централизованно с доминирующей ролью администратора безопасности.

Скрытые угрозы.

Под скрытыми понимаем такие угрозы, которые не очевидны, и требуют для противодействия им дополнительных предположений о возможных атаках злоумышленника.

Скрытые угрозы связаны с нерегламентированными действиями пользователя, прежде всего, посредством запуска собственных программ, а также с использованием злоумышленником ошибок и закладок в системном и прикладном ПО.

При этом скрытая угроза может быть охарактеризована двумя свойствами:

- характеристикой объекта угрозы (например, учетная запись пользователя);
- общей характеристикой атаки злоумышленника (например, модификация учетной записи с применением собственно запущенной программы. Действий подобной программы множество, как известных, так и неизвестных).

С учетом сказанного можно сделать следующий важнейший вывод: *любой механизм защиты должен проектироваться с учетом как явных, так и скрытых (в том числе и неизвестных) угроз информационной безопасности, так как только в этом случае можно говорить о возможности реализации механизмом защитных свойств.*

Классификация объектов угроз.

Для обоснования структуры системы защиты необходимо рассмотреть классификацию объектов угроз:

1. Объекты угроз:

1.1. Информационные и иные угрозы защищаемого объекта:

1.1.1. Локальные ресурсы.

1.1.2. Сетевые (в составе ЛВС) ресурсы.

1.2. Программные средства защищаемого объекта:

1.2.1. Системное и прикладное ПО.

1.2.2. ПО систем защиты.

1.3. Настройки программного обеспечения:

1.3.1. Настройки системного и прикладного ПО.

1.3.2. Настройки ПО систем защиты.

1.4. Аппаратные средства защищаемого объекта:

1.4.1. Оборудование защищаемого объекта.

1.4.2. Оборудование системы защиты.

С учетом этой классификации к объектам защиты могут быть отнесены:

1. Информационные и иные ресурсы защищаемого объекта, включая локальные и сетевые (в составе ЛВС). К таковым могут быть отнесены собственно система (вход в систему), файловые объекты (локальные и разделяемые) и т.д.

2. Программные средства защищаемого объекта, включая программные средства ОС и приложений, а также ПО системы защиты. При этом должна быть обеспечена неизменность, а при необходимости - активность процессов, драйверов, динамических библиотек и т.д.

3. Настройки программного обеспечения, включая настройки системного и прикладного ПО (реестр ОС, файлы настроек ОС и приложений, настройки BIOS и т.д.), а также настройки системы защиты (файлы настроек, реестр ОС).

4. Аппаратные средства защищаемого объекта, включая собственно оборудование компьютера, а также оборудование системы защиты. При этом с целью усиления защищенности может использоваться дополнительное оборудование, в частности плата, обеспечивающая функциональное расширение BIOS в части ввода пароля перед загрузкой системы с внешнего носителя.

Функциональная модель системы защиты.

Основные группы механизмов защиты. Функциональная модель.

Нормативными документами в области защиты информации в части защиты от НСД [6, 7] выделяются следующие основные группы механизмов защиты:

1. Механизмы авторизации пользователей.
2. Механизмы управления доступом пользователей к ресурсам.
3. Механизмы контроля целостности.
4. Механизмы регистрации (аудита).

Функционально (с учетом действий пользователя при доступе к ресурсам, а также с учетом противодействия НСД к информации механизмами защиты) система защиты должна строиться как иерархическая система - могут быть выделены несколько основных

уровней иерархии защиты. Выделение данных уровней и их реализация является необходимым (определяется формализованными требованиями) условием построения системы защиты.

Функциональная модель системы защиты, которая может быть получена на основании анализа формализованных требований к системе защиты, будет следующая:

1. Пользователь.
2. Уровень авторизации пользователя при доступе к ресурсам системы.
3. Уровень управления доступом (разграничения прав доступа) пользователя к ресурсам.
4. Уровень контроля целостности:
 - 4.1. Ресурс 1.
 - 4.2. Ресурс М.

Функциональная модель системы добавочной защиты [18], решающей задачи (п.3.3.1.3), будет следующая:

1. Пользователь.
2. Уровень авторизации пользователя при доступе к ресурсам системы.
3. Уровень управления доступом (разграничения прав доступа) пользователя к ресурсам.
4. Уровень контроля (мониторинга) корректности выполнения функций защиты и контроля целостности:
 - 4.1. Ресурс 1.
 - 4.2. Ресурс М.

При этом «Уровень контроля (мониторинга) наличия оборудования системы защиты» → «Уровень контроля (мониторинга) активности ПО системы защиты» → и последний влияет на три пункта: п.2 (Уровень авторизации пользователя при доступе к ресурсам системы); п.3 (Уровень управления доступом (разграничения прав доступа) пользователя к ресурсам); п.4 (Уровень контроля (мониторинга) корректности выполнения функций защиты и контроля целостности).

Сравнив эти функциональные модели, можно сделать вывод, что с целью решения сформулированных выше задач добавочной защиты, в модель защиты включены:

1. Уровень контроля (мониторинга) активности ПО системы защиты;

2. Уровень контроля (мониторинга) наличия оборудования системы защиты;

3. Кроме того, принципиально изменены функции уровня контроля целостности – данный уровень защиты здесь функционально предназначен для контроля (мониторинга) корректности выполнения функций защиты и контроля целостности.

Рассмотрим назначение уровней защиты в приведенной функциональной модели. Задачи, решаемые на различных уровнях, реализуются с учетом сформулированных для них требований. При этом каждый уровень защиты будем рассматривать как функциональный блок в представленной схеме.

Уровень авторизации пользователя при доступе к ресурсам системы.

Вначале, надо определиться, кто есть пользователь. К пользователям, в рамках уровневой модели защиты, могут быть отнесены как пользователи приложений, решающие с использованием данного средства соответствующие производственные задачи, так и администратор безопасности, являющийся пользователем системы защиты.

Уровень авторизации пользователя обеспечивает проверку учетных параметров пользователя при доступе в систему и к системе защиты. Также этим уровнем защиты решается ряд вспомогательных задач, например, запуск процесса (приложения) после авторизации ответственного лица и др. Более подробно авторизация рассмотрена в п.3.3.3.

Уровень управления доступом (разграничения прав доступа) пользователя к ресурсам.

Уровень управления доступом (разграничения прав доступа) реализует собственно разграничительную схему доступа пользователей к ресурсам защищаемого объекта, а также политику администрирования системы защиты в рамках выполнения политики информационной безопасности. Под системой защиты здесь понимаем соответствующие механизмы, встроенные в ОС, СУБД, приложения, а также добавочные механизмы защиты.

Для решения задачи управления доступом к ресурсам на этом уровне выделяются локальные и сетевые ресурсы. К локальным ресурсам, требующим разграничения доступа пользователей, относятся:

- файловые объекты (логические диски, каталоги, файлы);
- устройства со сменными носителями (в частности, дисковод и CD-ROM);

- отчуждаемые физические носители информации (в частности дискеты и CD-ROM диски);

- коммуникационные порты;

- локальные принтеры;

- процессы (исполняемые файлы), в том числе процессы ОС, системы защиты и приложений - в части их модификации и запуска;

- настройки ОС (для ОС Windows - реестр ОС);

- файлы настроек системы защиты;

- файлы настроек приложений;

- при использовании СУБД - таблицы данных и таблицы настроек;

- настройки «рабочего стола» ОС и т.д.

К сетевым ресурсам (в составе ЛВС), требующим разграничения доступа пользователей, относятся:

- разделяемые сетевые ресурсы (по протоколу NetBios для сети Microsoft), к которым относятся разделяемые файловые объекты, устройства со сменными носителями (виртуальные каналы связи сети Microsoft);

- сетевые ресурсы, например, по протоколу T R/IP (хосты, протоколы), виртуальные каналы связи сети T R/IP;

- сетевые принтеры;

- сетевые службы и приложения (в том числе приложения информационных систем, например, СУБД), в части их модификации и запуска;

- файлы настроек сетевых служб и приложений и т.д.

Разграничительная политика рассматривается как в виде разграничения доступа к ресурсам, так и в виде функций, реализующих разрешенный доступ (например, чтение, запись, исполнение и др). Решение задач разграничения доступа пользователей к ресурсам предполагает и реализацию процедур возврата коллективно используемого ресурса в исходное состояние для его предоставления другому пользователю (например, очистка оперативной и внешней памяти).

На этом уровне также решается задача распределения функций администрирования безопасностью системы между пользователями, системным (сетевым) администратором,

администраторами СУБД и приложений, администратором безопасности. При этом решается задача централизации схемы администрирования безопасности, в рамках которой изменение настроек безопасности на различных уровнях иерархии системы должно осуществляться только при непосредственном контроле со стороны администратора безопасности.

Вопросы корректности и полноты, а также возможности противодействия группе скрытых угроз, связанных с нерегламентированными действиями пользователя, для данного уровня защиты будут рассмотрены в п.3.3.4.

Уровень контроля (мониторинга) корректности выполнения функций защиты и контроля целостности.

Сама по себе задача контроля целостности предполагает возможность несанкционированного доступа к информации (в противном случае достаточно первых двух уровней защиты). Таким образом, данный механизм априори служит противодействию скрытым угрозам в предположении, что злоумышленником преодолены первые два уровня защиты, которые реализуют разграничительную политику доступа к ресурсам защищаемого объекта.

В рамках формализованных требований недостаток механизма контроля целостности состоит в том, что данный механизм, во-первых, реализует очень ограниченный набор функций, а во-вторых, не позволяет обеспечивать эффективную реакцию на скрытую атаку в реальном времени. По сути он только фиксирует ее факт и последствия.

С учетом сказанного функциональные задачи этого уровня защиты имеет смысл принципиально расширить. При этом к уже существующим задачам контроля целесообразно добавить контроль (мониторинг) корректности выполнения разграничительной политики доступа, реализуемой на предыдущем уровне. В том числе на этом уровне следует в реальном времени фиксировать факты использования злоумышленником ошибок и закладок в системном и прикладном ПО, а также оказывать противодействие данной группе скрытых угроз. К этому уровню также следует отнести контроль целостности программ и данных, то есть контроль объектов файловой системы.

В отличие от двух предыдущих уровней, где соответствующие механизмы (программные модули системы защиты) запускаются асинхронно по факту запроса в системе на доступ к

ресурсу, данный уровень реализует синхронную процедуру контроля. При этом он контролирует соответствующие события периодически, что связано с его более сильным влиянием на загрузку вычислительного ресурса защищаемого объекта по сравнению с большинством механизмов защиты двух предыдущих уровней.

Исключение составляют лишь реализуемые на предыдущем уровне механизмы распределения функций администрирования безопасностью системы между пользователями, системным (сетевым) администратором, администраторами СУБД и приложений, а также администратором безопасности. Эти механизмы также реализуются с использованием синхронной процедуры контроля.

Подробно эти технологии и особенности их реализации рассматриваются далее (п. 3.3.4.6. и 3.3.5.1.).

Уровень контроля (мониторинга) активности системы защиты.

Очевидно, что большинство задач защиты информации решаются программно, т.е. защищенность компьютерной информации обеспечивается до тех пор, пока активно ПО системы защиты. При этом включение в систему механизмов добавочной защиты, которые могут быть реализованы на различных уровнях (как на системном, так и на прикладном), связано с появлением дополнительной группы угроз - угроз загрузки системы без механизмов добавочной защиты и угроз перевода механизмов защиты в пассивное состояние (отключение) в процессе функционирования защищаемого объекта.

В задачи данного уровня входит контроль активности системы защиты, с предотвращением возможности функционирования системы в незащищенном состоянии. Последнее может быть связано как с возможностью загрузки ОС без системы защиты (либо с усеченными функциями), так и с возможностью перевода системы защиты, либо ее компонент, в пассивное состояние в процессе функционирования защищаемого объекта.

Очевидно, что активность одной программы не имеет смысла контролировать другой программой, запущенной на том же компьютере. Поэтому в рамках данного уровня должны быть реализованы следующие две возможности анализа активности системы защиты:

- локальная - с использованием аппаратной компоненты (платы);
- сетевая - удаленно, администратором с сервера безопасности.

При реализации данного уровня защиты должно оказываться противодействие как явным, так и скрытым угрозам. Соответствующая технология защиты рассматривается в п.3.3.7.

Уровень контроля (мониторинга) наличия оборудования системы защиты.

Данный уровень защиты целесообразно реализовывать в том случае, если система защиты содержит аппаратную составляющую. При этом защита от угрозы удаления аппаратной компоненты, помимо организационных мероприятий, может обеспечиваться техническими средствами.

Изначально данный уровень обеспечивает техническую защиту от угрозы удаления аппаратной компоненты системы защиты. Однако, его реализация позволяет комплексировать в единой технической системе защиты информации различные функции защиты: защиты компьютерной информации, контроля доступа в помещения, противопожарной безопасности и т.д. Причем все это будет доступно с единого рабочего места администратора.

Сводные рекомендации по отдельным уровням функциональной модели.

С учетом сказанного в данном разделе можем сделать следующие выводы [18]:

1. При построении системы добавочной защиты информации целесообразно принципиально пересмотреть функции уровня контроля целостности. Будем позиционировать данный уровень защиты, как уровень контроля (мониторинга) корректности выполнения функций защиты и контроля целостности.

2. В уровневую функциональную модель защиты имеет смысл включить уровень контроля (мониторинга) активности системы защиты, а при использовании аппаратной компоненты защиты функциональная модель может быть дополнена уровнем контроля (мониторинга) наличия оборудования системы защиты.

3. Уровни же авторизации пользователя и управления доступом должны обеспечивать решение задач корректности и полноты разграничений доступа пользователя к ресурсам. Кроме того, должна быть реализована также возможность противодействия группе скрытых угроз, связанных с нерегламентированными действиями пользователя.

Регистрация (аудит) событий.

Регистрация (аудит) событий осуществляется каждым реализованным в системе механизмом защиты. С учетом включения в

функциональную модель системы защиты уровня контроля (мониторинга) корректности выполнения функций защиты и контроля целостности имеет смысл принципиально изменить концепцию сбора и обработки регистрационной информации.

Особенностью реализованной модели защиты с точки зрения построения подсистемы регистрации (аудита) является введение в системе двух уровней аудита.

• *Аудит первого уровня.* Этот аудит осуществляется уровнем авторизации пользователя при доступе к ресурсам системы, а также уровнем управления доступом (разграничения прав доступа) пользователя к ресурсам. На этих уровнях ведется полный аудит действий пользователя системы. При этом фиксируются все действия, связанные как с правомерными, так и неправомерными попытками доступа пользователя к ресурсам защищаемого объекта. Регистрируемыми фактами НСД здесь являются неправомерные (противоречащие реализуемой политике информационной безопасности) действия пользователя (как ошибочные, так и сознательные), которые предотвращены механизмами защиты рассматриваемых уровней.

• *Аудит второго уровня.* Осуществляется уровнем контроля (мониторинга) корректности выполнения функций защиты и контроля целостности. Аудит второго уровня уже фиксирует не все действия пользователя, включая НСД, а только критичные факты НСД, связанные с преодолением злоумышленником механизмов защиты первых двух уровней рассматриваемой модели. По существу, на данном уровне осуществляется мониторинг корректности функционирования разграничительных механизмов защиты. При этом здесь уже речь идет не об ошибках пользователя, а об осознанных действиях нарушителя.

Таким образом, реализация уровневой модели защиты позволяет ввести уровневую модель аудита. При этом принципиально различается функциональное назначение уровней аудита. На первом уровне регистрируются все действия пользователей, в том числе и попытки НСД. Причем регистрации подлежат как сознательные нарушения, так и нарушения, связанные с ошибками пользователей. На втором уровне регистрируются только факты НСД, обусловленные сознательными нарушениями пользователей, связанные с преодолением защиты первых двух уровней модели защиты (либо с некорректным функционированием данных уровней защиты).

Другими словами, рассматриваемый подход позволяет разделить регистрируемые события на некритичные (аудит первого уровня) и критичные (аудит второго уровня). При этом различаются как требования к оперативности обработки регистрационной информации уровней аудита, так и вероятность регистрируемых событий на данных уровнях, а также объемы регистрируемой информации.

Так, на первом уровне аудита ведется непрерывная регистрация событий, т.е. накапливаются большие объемы некритичной к оперативности обработки регистрационной информации. Подобную информацию администратор может получать на сервер по своему запросу в моменты минимальной нагрузки на опорную сеть, а затем обрабатывать ее в рамках проведения расследований по факту НСД.

Напротив, на втором уровне аудита регистрируется критичная к оперативности обработки информация по фактам НСД. Данные этого уровня аудита должны поступать администратору безопасности немедленно и обрабатываться в реальном времени. При этом данные обычно поступают на специальный сервер ошибок - специальную программу сервера безопасности, а их обработка производится либо автоматически, либо с привлечением администратора безопасности.

Что касается мониторинга функционирования системы защиты, то здесь также реализуются два уровня мониторинга: мониторинг корректности выполнения системой защиты своих функций и мониторинг активности системы защиты (возможности выполнения ею своих функций).

Итак, мы можем сделать вывод, что включение в функциональную модель защиты уровня контроля (мониторинга) корректности выполнения функций защиты и контроля целостности позволяет реализовать в системе двухуровневую схему обработки данных регистрации событий (данных аудита). Это позволяет выделить лишь малую часть регистрационной информации, к которой выставляются требования по обработке в реальном времени. Таким образом, реализация двухуровневой модели аудита значительно повышает оперативность обработки регистрационной информации администратором безопасности и снижает нагрузку на трафик опорной сети при реализации сетевой системы защиты.

3.3.2.3. Особенности архитектуры сетевой системы защиты

Архитектура сетевой системы защиты.

Общим элементом архитектуры любой современной информационной системы, в том числе, сетевой системы защиты, является использование в той или иной мере распределенной модели межсетевое взаимодействия клиент-сервер. Причем в большинстве случаев это взаимодействие основывается на протокольных стеках ТСР/РР.

В общем случае в ЛВС могут быть реализованы следующие варианты архитектур системы защиты:

- распределенная архитектура;
- централизованная архитектура;
- централизованно-распределенная архитектура.

Возникает необходимость обоснованного выбора архитектуры системы защиты, а в случае выбора централизованно-распределенной архитектуры - задача функционального распределения задач защиты между архитектурными компонентами.

Распределенная архитектура системы защиты.

Распределенная архитектура представляет собой исходный вариант системы без обеспечения функций сетевого контроля и управления с выделенного рабочего места администратора безопасности (которое для данной архитектуры отсутствует). Все механизмы защиты и функции их администрирования реализуются непосредственно на защищаемом объекте. При этом какой-либо элемент централизации системы отсутствует как таковой.

К неоспоримым достоинствам подобной архитектуры следует отнести:

- максимальный обеспечиваемый уровень надежности системы защиты, так как отсутствует какой-либо структурообразующий элемент, отказ которого приводит к отказу всей системы в целом;
- отсутствие какого-либо влияния системы защиты на пропускную способность связанного ресурса защищаемой сети.

К принципиальным недостаткам архитектуры относятся:

- невозможность обеспечения оперативного управления рассредоточенной системой защиты в целом. То есть невозможно управление защитой одного объекта при зарегистрированных событиях на других защищаемых объектах. Можно управлять лишь отдельным элементом защиты с локальной консоли;

- невозможность оперативной обработки регистрационной информации, а также невозможность оперативного контроля действий пользователей на защищаемых сетевых объектах. Как следствие, невозможно оперативное расследование по фактам НСД.

Централизованная архитектура системы защиты.

В основу централизованного типа архитектуры положен принцип удаленной реализации защиты объектов с центральной консоли администратора безопасности. Все функции по обеспечению информационной безопасности защищаемых объектов делегированы одной компоненте системы защиты - серверу безопасности. Таким образом, в основе централизованных систем лежит построение виртуальной сетевой системы защиты, наложенной на опорную сеть передачи данных (ЛВС).

Естественно, что данной архитектуре присущи достоинства и недостатки, диаметрально противоположные распределенной архитектуре.

К неоспоримым недостаткам подобной архитектуры следует отнести:

- минимальный обеспечиваемый уровень надежности системы защиты. В системе присутствует один структурообразующий элемент - сервер безопасности, отказ которого приводит к отказу всей системы в целом;
- максимальное влияние системы защиты на пропускную способность связанного ресурса защищаемой сети.

К принципиальным достоинствам архитектуры относятся:

- обеспечение максимально оперативного управления рассредоточенной системой защиты в целом (управление защитой одного объекта при зарегистрированных событиях на других защищаемых объектах). Возможность управлять всеми элементами защиты с локальной консоли сервера безопасности;
- максимальные возможности по оперативной обработке регистрационной информации и контролю над пользователями. Как следствие, можно выделить максимальную оперативность при расследовании фактов НСД.

Централизованно-распределенная архитектура системы защиты.

Достоинства и недостатки.

Реализация данной архитектуры призвана объединить в себе все достоинства архитектурных решений, рассмотренных выше (соответственно, устранить их недостатки).

Остановившись на рассмотрении достоинств и недостатков

распределенной и централизованной архитектур системы защиты, естественно (интуитивно понятно) будет сделать предположение об оптимальности следующего распределения функциональных задач между компонентами централизованно - распределенной сетевой системы защиты:

- полностью распределенно должны решаться задачи защиты рабочих станций и серверов ЛВС. Реализовываться это должно устанавливаемой на них клиентской частью системы защиты;

- централизованно должны решаться:

- * администрирования клиентских частей системы защиты;
- * обработка регистрационной информации, собираемой клиентскими частями системы защиты;
- * контроль за действиями пользователей на защищаемых объектах.

Все это должно производиться с серверной части системы защиты - сервера безопасности.

Следует обратить внимание на то, что при централизованно-распределенной системе защиты, ее администрирование осуществляется полностью централизованно. То есть выполняется то принципиальное условие, которое было обосновано ранее. Описываемое далее распределение и масштабирование административных функций означает лишь распределение ресурсов. призванное снизить вред от возможного выхода из строя сервера безопасности. При этом сам принцип централизованного администрирования сохраняется, так как вершиной системы защиты является не сервер безопасности, а администратор безопасности. То есть именно администратор безопасности является централизующим звеном.

Итак, для поддержания функционирования системы в случае отказа сервера безопасности функции администрирования клиентских частей должны дублироваться распределенно. Кроме того сетевым агентам (клиентским частям системы защиты) должна отводиться часть общей задачи контроля и управления. При этом настройка клиентских частей производится самим администратором безопасности (в рамках централизованной схемы администрирования), а база данных администратора безопасности оказывается распределенной.

Режимы защиты, обеспечиваемые в рамках данной архитектуры, являются более интеллектуальными, поскольку сетевой агент располагает информацией, необходимой для экстренного

принятия решений без непосредственного сигнала от менеджера. При этом потоки информации, передаваемые по сети, существенно сокращаются.

Структура сетевой системы защиты в рамках централизованно-распределенной архитектуры.

Структура сетевой системы защиты определяется следующим набором компонент:

- *Клиентская часть системы защиты* — обеспечивает реализацию механизмов защиты на объекте. Используется для проведения контрольных проверок и регистрации действий пользователей на локальных рабочих станциях и информационных серверах ЛВС. Обеспечивает формирование системных журналов в соответствующем формате и отображение их на локальной консоли при запуске соответствующего интерфейсного модуля.

- *Модуль управления локальной базы данных (ЛБД) узла ЛВС* обеспечивает формирование ЛБД администратора безопасности на основе сбора и предварительной обработки локальных системных журналов (собственных и базовых журналов используемой платформы и прикладного ПО), сигналов синхронизации от центральной базы данных (ЦБД), а также сигналов администратора по настройке и обеспечению соответствующей политики безопасности в ЛВС.

- *Сетевой агент* - программный модуль, обеспечивает маскирующее кодирование (шифрование) и передачу сигналов управления, сигналов синхронизации между локальными и удаленными модулями системы защиты, а также обеспечивающий целостность соединений агент — элемент - менеджер.

- *Сетевой менеджер* - обеспечивает в дополнение к агенту мультиплексирование/демультиплексирование сигналов, передаваемых между ЦБД и ЛБД. Таким образом, им предоставляется связь точка-многоточка на прикладном уровне модели протоколов ISO/OSI. Кроме того, сетевой менеджер реализует сеансовую авторизацию клиентских частей системы защиты при их соединении с серверной частью.

- *Сетевая подсистема* - обеспечивает эмуляцию консоли удаленной станции с передачей сигналов управления и обратной связи по сетевому интерфейсу агент — элемент - менеджер.

- *Модуль ЦБД* - обеспечивает хранение и синхронизацию данных в ЛБД и ЦБД, а также инициализацию учетных данных

пользователей ресурсов ЛВС.

• *Интерфейсный модуль* - обеспечивает просмотр и редактирование ЦБД в соответствии с принятой политикой обеспечения безопасности. Также он осуществляет инициализацию функций расширенного контроля удаленного узла (сканирование удаленной консоли) и вывод результатов на консоль администратора безопасности.

На рис. 3.15 представлена диаграмма потоков управления и компонентный состав системы контроля на основе рассматриваемой архитектуры.

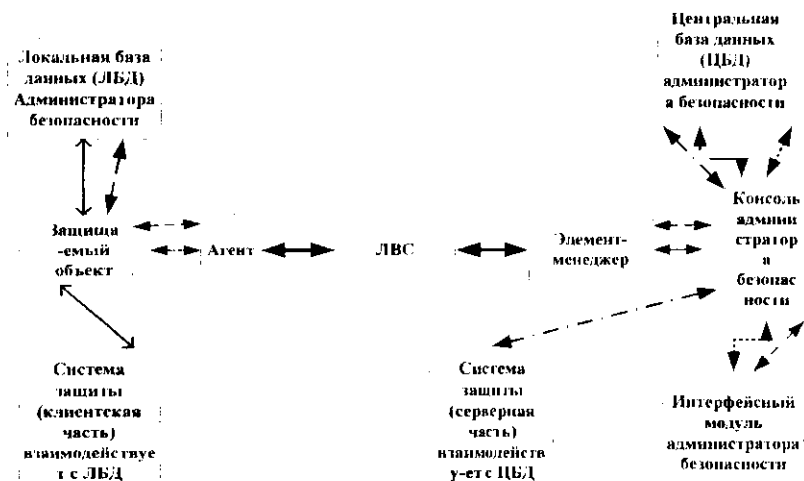


Рис. 3.15. Диаграмма потоков управления и компетентный состав системы контроля на основе централизованной архитектуры

Сплошными тонкими стрелками на диаграмме выделен информационный поток, обеспечивающий запросы удаленного выполнения программных процедур, запускаемых из интерфейсного модуля администратора в специализированном формате, представляя собой по существу некоторое подобие сетевых программ удаленного доступа.

Пунктирными стрелками обозначен поток данных, обеспечивающий автоматическую передачу журналов регистрации, фрагментов системных структур ядра ОС, а также любых настроек

программного обеспечения сетевого агента узла ЛВС.

Сплошными толстыми стрелками обозначен поток данных, инкапсулирующий в себе команды, данные и параметры конфигурации сетевого агента, а также несущий в себе последовательность меток временной синхронизации. Защищенность этого потока обеспечивается в режиме канального шифрования из конца в конец (то есть при непосредственной передаче информации от агента к менеджеру через ЛВС).

Пунктирными стрелками с точками на диаграмме выделяются данные, передаваемые через стыковочный пилот сетевой подсистемы защиты при выполнении контроля в режиме эмуляции удаленного узла. В данном случае имеется в виду, что внешний вид системы и интерфейс администратора сохраняются, однако система выбирает информацию для контроля не из структуры ядра и журнальных файлов, а из центральной базы данных (ЦБД) администратора безопасности.

Стрелками, состоящими из точек, выделяется взаимодействие интерфейсного модуля администратора и ЦБД, в рамках которого реализуются основные функции удаленного управления (смена паролей, установка таймеров протокола, настройка параметров бюджета пользователей и узлов ЛВС, и т.д.).

Тонкими стрелками (в виде стрелы) выделяются локальные взаимодействия обеспечивающие функции защиты на основе технических средств системы защиты, реализуемых клиентской частью.

Централизованно-распределенная архитектура характеризуется незначительным усложнением клиентской части системы защиты по сравнению с распределенной архитектурой, при существенном упрощении серверной компоненты системы защиты по сравнению с централизованной архитектурой.

Многоуровневая централизованно-распределенная система.

В рамках реализации централизованно-распределенной архитектуры очевидна возможность распределения функций удаленного управления системой защиты, в частности, посредством реализации многоуровневой схемы администрирования. В централизованно-распределенной одноуровневой архитектуре, рассмотренной выше, использовался единственный узел концентрации управления безопасностью в ЛВС.

Можно разработать и большую степень децентрализации, при которой происходит дальнейшее наращивание уровней контроля и

управления безопасностью защищаемых объектов. Реализуется этот вариант с использованием промежуточных систем, которые будут концентрировать управляющую нагрузку различных ЛВС и далее транслировать ее уже непосредственно на рабочее место администратора безопасности (сервер безопасности более высокого уровня). Таким образом, можно обеспечить масштабирование задач управления безопасностью распределенных корпоративных сетей большой сложности.

Анализ эффективности централизованно-распределенной системы защиты.

Параметры и характеристики эффективности. Информационная сигнатура.

С точки зрения анализа эффективности централизованно-распределенной архитектуры системы защиты будем оценивать влияние, оказываемое на опорную сеть передачи данных (на пропускную способность) наложенной сетью системы защиты. Цель такого анализа - выработка рекомендаций по централизации задач, решаемых системой защиты в рамках сетевой реализации системы.

При этом выделим три основных функции системы защиты, характеризующих ее функционирование в штатном режиме (не рассматривается начальный этап функционирования системы, связанный с заданием настроек ее параметров) [18]:

1. Контроль изменений состояния защищаемых объектов, выработка реакции на изменение состояния;
2. Контроль пользователя, работающего на защищаемом объекте;
3. Регистрация (аудит) событий на защищаемом объекте.

Введем следующие обозначения:

- параметр $\lambda_{\text{вход1}}$ определяется, как интенсивность изменения состояний защищаемого узла ЛВС, которые должны быть зафиксированы системой защиты (именно на них должно быть выработано управляющее воздействие);
- параметр $\lambda_{\text{вход2}}$ определяется, как интенсивность проведения контроля действий пользователя на защищаемом объекте;
- параметр $\lambda_{\text{вход3}}$ определяется, как интенсивность получения запросов администратором безопасности на серверную часть регистрационной информации (данных аудита) с защищаемого объекта;
- параметр P — мера централизации системы защиты, определяется как вероятность того, что событие изменения состояния

защищаемого объекта - узла ЛВС, будет обрабатываться системой защиты распределенно (клиентской частью - без участия сервера безопасности). Соответственно, с вероятностью $(1-P)$ событие будет обрабатываться централизованно - серверной частью системы защиты (сервером безопасности).

Будем считать, что все входные потоки пуассоновские (простейшие), что позволяет осуществлять суммирование их интенсивностей, при определении интенсивности входного потока в канале связи.

Далее будем использовать понятие информационной сигнатуры, генерируемой в канале связи системой защиты в единицу времени. Под информационной сигнатурой будем понимать общий объем информации, измеряемый в килобайтах в секунду и передаваемый системой защиты по каналу связи.

Определим объемы информационных взаимодействий клиентской и серверной компонент системы защиты:

V_u - объем информации, идентифицирующей изменение состояния защищаемого объекта (дата, время, идентифицирующие параметры события, текущий пользователь и т.д.);

V_y - объем информации, идентифицирующей управляющее воздействие системы защиты на факт изменения состояния защищаемого объекта;

$V_{зк}$ - объем информации, передаваемый в запросе на проведение контроля действий пользователя;

$V_{за}$ - объем информации, передаваемый в запросе на получение регистрационной информации (аудита) с защищаемого объекта;

V_k - объем информации контроля действий пользователя на защищаемом объекте (например, экранная копия);

V_a - объем регистрационной информации (аудита).

Так как в ЛВС может одновременно находиться несколько десятков и сотен защищаемых объектов, взаимодействующих с одним сервером безопасности, то через N обозначим число защищаемых узлов в ЛВС.

С учетом введенных обозначений информационная сигнатура S , генерируемая в канале связи системой защиты в единицу времени, может быть определена следующим образом:

$$S = N \cdot [P \cdot \lambda_{\text{вход1}} \cdot (V_u + V_y) + \lambda_{\text{вход2}} \cdot (V_{зк} + V_k) +$$

$$+ \lambda_{\text{вход3}} \cdot V_a]. \quad (3.32)$$

Так как объем запрашиваемой с сервера регистрационной информации зависит от параметра P (на сервер следует запрашивать только регистрационную информацию, обрабатываемую в системе распределенно; информация, обрабатываемая централизованно, поступает на сервер в реальном масштабе времени с вероятностью $(1-P)$), то объем информации регистрации определяется следующим образом:

$$V_a = ((1-P) \cdot V_u + \lambda_{\text{вход1}} / \lambda_{\text{вход3}}). \quad (3.33)$$

Если пропускную способность связанного ресурса обозначить через S , то доля пропускной способности связанного ресурса, занимаемая системой защиты K составит:

$$K = S/C. \quad (3.34)$$

При этом под пропускной способностью связанного ресурса будем понимать не физическую скорость передачи данных в канале связи, а скорость передачи собственно информации, без учета передачи заголовков, подтверждений, затрат времени на арбитраж требований связанного ресурса в ЛВС и т.д. Следует отметить, что обработка заявок на обслуживание системой защиты по сравнению с обработкой заявок от прикладных задач, должна осуществляться в приоритетном режиме.

Проанализируем полученное выражение (3.32). Если в него подставить выражение (3.33), задающее параметр V_a , то получим следующее приближение характеристики S :

$$S = N \cdot [\lambda_{\text{вход1}} \cdot (V_u + V_y) + \lambda_{\text{вход2}} \cdot (V_{\text{жк}} + V_k)]. \quad (3.35)$$

Откуда можно сделать важный вывод, что осуществление регистрации (аудита) событий в реальном времени на сервере безопасности, по существу, приводит к выполнению условия $P=1$. Это означает получение характеристик, практически полностью совпадающих с характеристиками централизованной архитектуры системы защиты.

Таким образом, при построении системы защиты должно решаться следующее противоречие. С одной стороны, регистрировать

события на сервере безопасности целесообразно в реальном масштабе времени (в противном случае, администратор безопасности не будет обладать необходимой текущей информацией о защищаемом объекте). С другой стороны, реализация данного условия приводит к нивелированию преимуществ централизованно-распределенной архитектуры с точки зрения эффективности использования связного ресурса в защищаемой сети (не с точки зрения оперативности реакций на регистрируемые события).

Ранее было отмечено, что исходя из соображений оперативности реакции на возможные факты НСД, а также исходя из обеспечения высокой надежности системы защиты, все механизмы защиты должны быть реализованы распределенно (должно выполняется условие: $P = 0$). То есть они должны исполняться клиентской частью системы защиты, устанавливаемой на защищаемые объекты. Характеристика S в этом случае задается следующим выражением:

$$S = S1 + S2 = N \cdot [\lambda_{\text{вход1}} \cdot V_u + \lambda_{\text{вход2}} \cdot (V_{\text{зк}} + V_{\text{к}})]. \quad (3.36)$$

Здесь:

- характеристика $S1 = N \cdot [\lambda_{\text{вход1}} \cdot V_u]$ определяет влияние на пропускную способность опорной сети подсистемы регистрации событий (аудита);

- характеристика $S2 = N \cdot [\lambda_{\text{вход2}} \cdot (V_{\text{зк}} + V_{\text{к}})]$ определяет влияние подсистемы контроля действий пользователя на защищаемом объекте.

Количественная оценка характеристик эффективности централизованно-распределенных систем защиты.

Приведем грубую количественную оценку рассматриваемых характеристик. Рассмотрим влияние подсистемы аудита (характеристика $S1$) на пропускную способность связного ресурса. При этом зададим следующие значения параметров.

Пусть в сети находится 250 защищаемых объектов: $N = 250$ (это ЛВС средних масштабов). Параметр V_u определяется объемом регистрационной информации, характеризующим изменение состояние защищаемого объекта (тип события, текущий пользователь, время, дата и т.д.); примем: $V_u = 100$ байт. Параметр $\lambda_{\text{вход1}}$ обоснованно задать наиболее сложно, т.к. события, характеризующие состояние станции, имеющие различный физический смысл, могут генерироваться с частотой, различающейся

на порядка.

Примем $\lambda_{\text{вход1}} = 10 \text{ с}^{-1}$ (например, за 1 секунду запускается 10 различных процессов, осуществляется 10 обращений к файловым объектам и т.д.), понимая, что реальное значение данного параметра при осуществлении атаки может быть значительно больше.

При заданных значениях параметров получаем, что $S1 = 0,25$ Мбайт/с. Оценим значение искомой характеристики C . Физическая скорость в канале для ЛВС Ethernet составляет 10 Мбит/с (соответственно, Fast Ethernet — 100 Мбит/с). Скорость передачи данных грубо можно принять на порядок меньше физической скорости в канале связи (затраты времени на передачу служебных частей заголовков, подтверждений передачи, разрешения коллизий и т.д.), откуда для сети Ethernet получаем порядка: $C = 0,1$ Мбайт/с, а для Fast Ethernet получаем порядка: $C = 1$ Мбайт/с.

Таким образом, для введенных предположений получаем, что для сети Ethernet трафик системы защиты в рамках реализации подсистемы аудита превышает исходную пропускную способность сети Ethernet и снижает пропускную способность сети Fast Ethernet на 25% ($K = S1/C = 0,25$).

Поиск оптимального решения.

Возможные подходы.

Из полученных результатов можем сделать вывод о невозможности в системе защиты реализовать передачу регистрационной информации в полном объеме на сервер безопасности в реальном времени. Было показано, что это обусловлено слишком большими потерями производительности связного ресурса, то есть доли полосы пропускания канала связи ЛВС, занимаемой системой защиты информации.

С целью поиска оптимального решения проанализируем две составляющие — $S1$ и $S2$. Из выражения $S1 = N \cdot [\lambda_{\text{вход1}} \cdot V_u]$ можем сделать вывод, что уменьшение характеристики $S1$ возможно только за счет уменьшения значения параметра $\lambda_{\text{вход1}}$ (т.к. уменьшить параметр V_u практически невозможно). Но волонтаристски параметр $\lambda_{\text{вход1}}$ уменьшить невозможно, так как он определяется пользователем, работой ОС и приложений. Однако можно значительно снизить долю регистрационной информации, которую следует выдавать на сервер в реальном времени. При этом всю остальную информацию можно получать на сервер по запросу администратора безопасности в моменты наименьшей загрузки канала связи (например, после завершения рабочего дня, во время

обеденного перерыва и т.д.).

Резонно предположить, что в реальном времени на сервер безопасности следует выдавать только информацию, связанную с НСД, то есть информацию о преднамеренных действиях пользователя, противоречащих разграничительной политики доступа к ресурсам. Это позволит снизить значение параметра $\lambda_{\text{вход1}}$ на несколько порядков, обеспечивая долю потерь производительности связного ресурса в пределах единиц (долей) процентов.

Однако здесь появляется угроза генерирования злоумышленником событий НСД (ошибок) с целью перегрузки канала связи ЛВС и временного вывода из строя ЛВС как опорной сети связи предприятия. Поскольку заявки системы защиты в канале связи обрабатываются с более высоким приоритетом, чем заявки на занятие связного ресурса, поступающие от приложений, то у злоумышленника такая возможность имеется.

Для противодействия этому необходимо выделять и обрабатывать в реальном времени (передавать на сервер безопасности) только те зарегистрированные события НСД, которые каким-либо образом преодолевают механизмы защиты, реализуемые клиентской частью системы защиты, и потому требуют немедленного вмешательства в процесс обработки информации администратора безопасности.

Характеристика $S2 = N \cdot [\lambda_{\text{вход2}} \cdot (V_{\text{зк}} + V_{\text{к}})]$ отражает влияние на пропускную способность опорной сети подсистемы контроля действий пользователя на защищаемом объекте. Проанализируем данную зависимость. Во-первых, очевидно, что $V_{\text{зк}} \ll V_{\text{к}}$, т.е. далее параметр $V_{\text{к}}$ в выражении для $S2$ можем опустить. Во-вторых, контроль действий пользователя осуществляется подсистемой оперативной обработки, реакцию которой задает человеческий фактор. Реальный интервал времени, с которым администратор безопасности может просматривать контролируемую информацию (например, изображение на мониторе защищаемого объекта) — это от 5 до 15 сек., причем вне зависимости от числа подключенных к ЛВС защищаемых объектов. Поэтому здесь примем: $N \cdot \lambda_{\text{вход2}} = 0,1 \text{ с}^{-1}$.

Объем контролируемой информации может быть достаточно велик, однако для передачи по каналу связи контролируемая информация может сжиматься. Поэтому примем $V_{\text{к}} = 10 \text{ Кбайт}$.

С учетом сказанного получаем: $S2 = 1 \text{ Кбайт/с}$, соответственно, для сети Ethernet получаем: $K = S2/C = 0,01$, для сети Fast Ethernet получаем: $K = 0,001$, т.е. контроль действий пользователя на

защищаемом объекте снижает пропускную способность сети, соответственно, на 1% и на 0,1%.

Таким образом, несмотря на большие объемы контролируемой информации, ввиду низкого уровня оперативности подсистемы контроля, обусловливаемой человеческим фактором, реализация данной подсистемы в системе защиты не оказывает сколько-нибудь заметного влияния на производительность связного ресурса ЛВС. Причем это верно вне зависимости от числа подключаемых к сети контролируемых объектов защиты.

Сводные рекомендации по построению централизованно-распределенных сетевых систем защиты, исходя из анализа эффективности.

Система защиты должна содержать три основных компоненты:

- собственно компоненту защиты, реализующая разграничительную политику доступа пользователей к ресурсам;
- компоненту регистрации (аудита) изменений событий на защищаемом объекте;
- компоненту контроля действий пользователя на защищаемом объекте.

На основании проведенного анализа эффективности централизованно-распределенной архитектуры системы защиты могут быть даны следующие рекомендации по ее построению.

1. *Компонента защиты* должна быть реализована практически полностью распределенно. При этом все ее механизмы защиты должны быть реализованы клиентской частью системы, устанавливаемой на защищаемом объекте. Централизация для этой компоненты состоит только лишь в возможности удаленного администрирования механизмов защиты с сервера безопасности, причем с дублированием данной функции с консоли защищаемого объекта (т.е. распределенно).

2. *Компонента регистрации (аудита)* должна быть реализована по централизованно-распределенной схеме с двумя уровнями обработки регистрационной информации. Распределенность компоненты состоит в том, что все события аудита должны регистрироваться клиентской частью. При этом на сервер должны поступать только те данные, которые зарегистрированы клиентской частью системы защиты.

Уровни обработки определяют механизмы построения централизованной компоненты аудита и задают способы передачи

регистрационной информации на сервер безопасности. Первый уровень (обработка в реальном времени) предполагает немедленную отправку регистрационной информации клиентской частью на сервер безопасности, второй уровень - уровень оперативной обработки — предполагает выдачу регистрационной информации по удаленному запросу администратором безопасности с сервера в моменты минимальной загрузки канала связи.

С целью минимизации влияния системы защиты на производительность связного ресурса на первом уровне должны обрабатываться минимальные объемы регистрационной информации - факты ИСД (в пределе - факты преодоления злоумышленником распределенно реализуемых в системе механизмов защиты информации).

3. *Компонента контроля* пользователей на защищаемом объекте представляет собою реализацию централизованной схемы сбора и обработки информации. При этом контролируемая информация генерируется и выдается на сервер безопасности по команде с сервера. Несмотря на большие объемы передаваемой информации, реализация данной компоненты не оказывает сколько-нибудь заметного влияния на производительность связного ресурса (занимает доли процента полосы пропускания канала связи). Причем это независимо от числа контролируемых системой защиты объектов (рабочих станций и серверов ЛВС).

Функциональные подсистемы и модули центрально-распределенной системы защиты.

Функциональная структура сетевой системы защиты.

С учетом особенностей рассматриваемого в книге класса систем (систем защиты, основные функции которых реализуются на системном уровне), система должна быть хорошо структурирована. Функциональная структура системы защиты задает распределение реализуемых функций по отдельным *функциональным подсистемам*. Функциональная подсистема состоит из нескольких модулей, реализующих набор механизмов, необходимых для покрытия требований данной подсистемы.

Функциональный модуль определяется как структурный элемент, реализующий набор механизмов или используемый для вспомогательных целей (организации взаимодействия между другими модулями в рамках решения всего комплекса задач).

Используя определенные выше компоненты системы защиты и сформулированные в предыдущем подзаголовке рекомендации,

можно получить структуру сетевой системы защиты, основанную на реализации централизованно-распределенной архитектуры.

В общем случае могут быть выделены следующие типы функциональных подсистем:

1. Подсистема защиты рабочих станций и информационных серверов (клиентская часть системы защиты). К этой же подсистеме отнесем функции регистрации событий.

2. Подсистема удаленного контроля рабочих станций и информационных серверов.

3. Подсистема удаленного управления механизмами защиты рабочих станций и серверов.

Подсистема защиты рабочих станций и информационных серверов (клиентская часть системы защиты).

Подсистема защиты рабочих станций и информационных серверов (клиентская часть системы защиты) является структурообразующим элементом, призванным решать собственно задачи защиты информации и содержащем в себе следующие основные функциональные модули:

1. Модули, реализующие механизмы защиты (каждый механизм защиты реализуется отдельным функциональным модулем):

- модуль аутентификации;
- модуль управления доступом;
- модуль контроля целостности;
- модуль противодействия ошибкам и закладкам в системном и функциональном программном обеспечении;

• модуль очистки памяти и изоляции программных модулей и др. (в зависимости от реализуемых в системе механизмов защиты).

2. Модуль регистрации (аудита).

3. Модуль управления режимами, который решает задачи инициализации механизмов при доступе к защищаемым ресурсам.

Подсистема удаленного контроля рабочих станций и информационных серверов.

Подсистема удаленного контроля рабочих станций и информационных серверов реализует, в дополнение к перечисленным функциям защиты, контроль служебной деятельности сотрудников и информации, располагаемой на защищаемом объекте.

Данная подсистема состоит из следующего набора функциональных модулей:

1. *Модуль сканирования клавиатуры и монитора.*

Модуль сканирования клавиатурного буфера удаленной консоли осуществляет копирование информации, набираемой на клавиатуре видеотерминала, с целью последующего архивирования и передачи на рабочее место администратора безопасности. При этом передача может осуществляться либо в синхронном режиме - по расписанию, либо в асинхронном режиме - по внешним запросам администратора безопасности. Предварительное накопление информации по результатам контроля состояния осуществляется либо в специальной, защищенной от просмотра области внешнего диска, либо в виде, не пригодном для непосредственного просмотра и удаления пользователями. Режим функционирования модуля определяется согласно установке соответствующих параметров локальной базы данных системы защиты по сигналам от модуля управления режимами. Команды управления режимами инкапсулируются в кадрах протокола управления сетевыми соединениями системы защиты и непосредственно передаются модулю управления режимами.

Модуль сканирования видеобуфера удаленной консоли реализует аналогичные контролирующие функции по отношению к видеотерминалу удаленной консоли. В дополнение к перечисленному, данным модулем осуществляется автоматическое архивирование полученной информации непосредственно перед передачей на рабочее место администратора безопасности. Период выполнения контролирующих функций данного вида определяется необходимостью выборочного контроля пользователей.

2. *Модуль сканирования состояния системы* реализует функции удаленного контроля состояния системы:

- контроля файловой системы защищаемого объекта. Реализуется возможность удаленного просмотра объектов файловой системы, создания, записи, удаления файла (каталога) на защищаемом объекте, запрета доступа пользователей к удаленно создаваемому файлу;

- контроля среды исполнения. Реализуется возможность удаленного контроля запущенных на защищаемом объекте процессов, удаленного запуска процесса, в том числе в невидимой для пользователя консоли;

- контроля настроек ОС. Реализуется возможность удаленного просмотра объектов реестра ОС, создания, записи, удаления ключа реестра на защищаемом объекте, запрета доступа пользователей к ветви или ключу реестра ОС;

- контроля параметров сетевого доступа, в частности, занятых TCP портов и т.д. и др. (в зависимости от реализуемых в системе механизмов контроля).

3. *Модуль управления режимами* решает задачи инициализации механизмов при запуске функций контроля.

Подсистема удаленного управления механизмами защиты рабочих станций и серверов (серверная часть системы защиты - сервер безопасности).

Подсистема удаленного управления механизмами защиты рабочих станций и серверов (серверная часть системы защиты - сервер безопасности) обеспечивает централизацию управления техническими средствами клиентской части системы защиты и контроля (по соответствующим журналам) со стороны серверной части в удаленном режиме. Функциональные возможности подсистемы обеспечиваются следующим набором модулей:

1. *Модуль обработки сетевых соединений* предоставляет интерфейс служб представительского уровня МОС/ВОС для подсистемы системы защиты и интерфейс сеансового уровня для подсистемы контроля рабочих станций и информационных серверов. Межсетевое взаимодействие целесообразно реализовать на основе служб транспортного протокола TCP и сетевого протокола IP. В качестве транспортного интерфейса для организации передачи команд и ответов реализуется закрытый протокол, позволяющий шифровать трафик. Для организации сетевых соединений и мониторинга подключения рабочих станций используется интерфейс сокетов высокого уровня. При установлении виртуального канала и передаче данных должна использоваться сеансовая аутентификация агентов и контроль целостности соединений по последовательным номерам команд-ответов и таймерам ожидания/блокировки соединения. Передача кадров протокола реализуется с использованием внешних подключаемых алгоритмов маскирования и шифрования информации.

Модуль непосредственно взаимодействует с модулем доступа к базе данных администратора безопасности при выполнении репликации (согласования) элементов учетных записей централизованной базы данных и локальных сегментов баз данных удаленных узлов. Модуль инициализируется при запуске сервера безопасности и остается активен до момента остановки серверной части.

2. *Модуль базы данных администратора безопасности*

используется для хранения, предварительной обработки (сортировки, фильтрации) и выборки информации следующих типов:

- регистрационные записи журнальных файлов;
- параметры конфигурации и настройки системы защиты;
- сообщения об ошибках работы ОС и системы защиты

(журналы ошибок).

3. *Модуль графического интерфейса администратора безопасности* используется для доступа к базе данных выделенного сервера администратора безопасности и осуществления прямого контроля удаленных узлов в режиме реального времени, включая выдачу команд чтения буферов клавиатуры и видеотерминала, проверки подключения пользователя к сети, команд обновления конфигурации и опроса статуса удаленного узла. Интерфейс целесообразно строить в удобной для использования форме, базирующейся на стандартных для Windows-приложений графических примитивах. При этом должны предусматриваться различные способы группирования объектов контроля в различные уровни иерархии, включая:

- группирование пользователей в функциональные группы по особенностям служебной деятельности;
- группирование пользователей в функциональные группы в соответствии с особенностями физического их расположения на территории предприятия;
- группирование узлов в сетевые сегменты в соответствии с особенностями физического их расположения и способов подключения к ресурсам сети;
- группирование узлов в информационные (автоматизированные) системы в соответствии с их принадлежностью к системам обработки данных;
- комбинированное группирование с учетом перечисленных возможностей.

По соображениям удобства мониторинг объектов контроля осуществляется с применением одного из указанных представлений.

4. *Модуль управления режимами* решает задачи инициализации режимов мониторинга и управления.

Функционирование системы защиты должно осуществляться в двух режимах в зависимости от наличия активного соединения клиентской части с сервером безопасности.

- При работе в автономном режиме (серверная часть отсутствует) функционирование системы защиты начинается с

загрузки операционной системы на защищаемом сервере или рабочей станции. При этом в качестве сервиса ОС автоматически загружается система защиты с заданными настройками параметров механизмов защиты.

- При работе в сетевом варианте (с сервером безопасности) после загрузки клиентской части осуществляется автоматический поиск сервера безопасности (по его заданному IP-адресу или имени), подключение к серверу по протоколу ТСРДР на заданный порт и проведение сеансовой аутентификации компонент системы защиты.

3.3.3. Авторизация, методы идентификации и авторизации пользователя

3.3.3.1. Авторизация

Понятие идентификации и аутентификации. Процедура авторизации.

Идентификация призвана каждому пользователю (группе пользователей) сопоставить соответствующую ему разграничительную политику доступа на защищаемом объекте. Для этого пользователь должен себя идентифицировать - указать свое «имя» (идентификатор). Таким образом, проверяется, относится ли регистрирующийся пользователь к пользователям, идентифицируемым системой. В соответствии с введенным идентификатором пользователю будут сопоставлены соответствующие права доступа.

Аутентификация предназначена для контроля процедуры идентификации. Для этого пользователь должен ввести секретное слово - пароль. Правильность вводимого пароля подтверждает однозначное соответствие между регистрирующимся пользователем и идентифицированным пользователем.

В общем случае идентифицируются и аутентифицируются не только пользователи, но и другие субъекты доступа к ресурсам [18].

Совокупность выполнения процедур идентификации и аутентификации принято называть *процедурой авторизации*. При этом заметим, что иногда не требуется идентифицировать пользователя, а достаточно только выполнения процедуры аутентификации. Например, это происходит когда требуется подтвердить текущего (уже зарегистрированного) пользователя при выполнении каких-либо действий, требующих дополнительной защиты. В свою очередь, не всегда требуется осуществлять контроль

идентификации, то есть в некоторых случаях аутентификация может не производиться.

Процедура авторизации имеет ключевое значение при защите компьютерной информации, т.к. вся разграничительная политика доступа к ресурсам реализуется относительно идентификаторов пользователей. То есть, войдя в систему с чужим идентификатором, злоумышленник получает права доступа к ресурсу того пользователя, идентификатор которого был им предъявлен при входе в систему.

Требования к идентификации и аутентификации.

Формализованные требования.

Формализованные требования к данным механизмам защиты состоят в следующем:

- Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов (для классов защищенности 1Г и 1В по классификации АС) [16];

- Система защиты должна требовать от пользователей идентифицировать себя при запросах на доступ;

- Система защиты должна подвергать проверке подлинность идентификации - осуществлять аутентификацию. Для этого она должна располагать необходимыми данными для идентификации и аутентификации;

- Система защиты должна препятствовать доступу к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась (для 5 класса защищенности по классификации СВТ) [17]. Для 3 класса защищенности по классификации СВТ вводится дополнительное требование: система защиты должна обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя [17].

Очевидно, что кроме ограничения «...паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов...» данные требования никак не формализуют подходы к реализации механизмов парольной защиты. Кроме того, данные требования не определяют, каким образом должны быть реализованы механизмы парольной защиты, а также не накладывают дополнительных ограничений, связанных с повышением стойкости пароля к подбору. В частности, они не регламентируют

использование внешних носителей парольной информации - дискет, смарт-карт и т.д.

Дополнительные требования.

Как отмечалось ранее, существует целая группа угроз, связанная с некорректностью реализации процедуры авторизации в современных ОС, а также с наличием ошибок в реализации соответствующих механизмов защиты. Это обуславливает целесообразность рассмотрения механизмов авторизации с целью их добавочной защиты. Кроме того, механизмы идентификации и аутентификации являются важнейшими для противодействия НСД к информации, а значит, следует рассматривать возможные варианты их резервирования (как «горячего», так и «холодного»).

Кроме того, в рамках декларируемого системного подхода к проектированию системы защиты (рассмотренного нами в п.3.3.2.1), при разработке механизмов авторизации следует рассматривать как явные, так и скрытые угрозы преодоления защиты.

И еще: в рамках системного подхода следует рассматривать не отдельно механизм авторизации как таковой, а необходимую и достаточную совокупность механизмов защиты, призванных в комплексе решать рассматриваемую задачу защиты. Далее будет показано, что как бы хорошо не был исполнен механизм авторизации, в отдельности он не позволяет обеспечить надежную защиту от несанкционированного входа пользователя в систему.

Авторизация в контексте количества и вида зарегистрированных пользователей.

Кого следует воспринимать в качестве потенциального злоумышленника.

В системе зарегистрирован один пользователь.

В общем случае в системе может быть зарегистрирован один либо несколько пользователей. Случай, когда в системе зарегистрирован только один пользователь, характеризуется тем, что данный пользователь является и прикладным пользователем, и администратором безопасности. Здесь источником потенциальной угрозы является только сторонний сотрудник предприятия, а вся задача защиты сводится к контролю доступа в компьютер (либо в систему), т.е. к парольной защите.

Данный случай является вырожденным и далее не рассматривается, т.к. в соответствии с формализованными требованиями к защите информации от НСД (см. п.3.3.1.2) даже при защите конфиденциальной информации предполагается обязательное

наличие администратора безопасности.

В системе зарегистрированы администратор безопасности и один прикладной пользователь.

Общий случай функционирования системы с одним прикладным пользователем - это наличие в системе администратора безопасности и только одного прикладного пользователя. В задачи администратора безопасности здесь входит ограничение прав прикладного пользователя по доступу к системным (администратора безопасности) и иным ресурсам компьютера. В частности, может ограничиваться набор задач, разрешенных для решения на компьютере, набор устройств, которые могут быть подключены к компьютеру (например, внешний модем, принтер и т.д.), способ сохранения обрабатываемых данных (например, на дискетах только в шифрованном виде) и т.д.

В данном случае потенциальным злоумышленником в части несанкционированного использования ресурсов защищаемого объекта может являться как сторонний сотрудник предприятия, так и собственно прикладной пользователь. Заметим, что прикладной пользователь здесь может выступать в роли сознательного нарушителя, либо стать «инструментом» в роли стороннего нарушителя (например, запустив по чьей-либо просьбе какую-нибудь программу).

В системе зарегистрированы администратор безопасности и несколько прикладных пользователей.

Кроме администратора безопасности, в системе может быть заведено несколько прикладных пользователей. При этом ресурсами защищаемого компьютера могут пользоваться несколько сотрудников, решая различные задачи. Ввиду этого информационные и иные ресурсы защищаемого объекта должны между ними разграничиваться.

В данном случае к потенциальным нарушителям добавляется санкционированный прикладной пользователь, целью которого может служить НСД к информации, хранимой на защищаемом объекте другим пользователем.

При использовании компьютера (прежде всего, рабочей станции) в составе ЛВС, помимо локальных ресурсов защищаемого объекта, защите подлежат сетевые ресурсы. В этом случае между пользователями могут разграничиваться права по доступу к серверам, сетевым службам, разделенным сетевым ресурсам (общим папкам и устройствам, например, к сетевым принтерам) и т.д. Здесь

злоумышленник (санкционированный пользователь) может осуществлять попытку получить НСД к сетевому ресурсу, к которому ему доступ не разрешен, с целью осуществления на него атаки с рабочей станции.

Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей.

Наиболее простой в реализации защитой является защита от стороннего сотрудника. В этом случае все мероприятия по защите возлагаются на использование механизма парольного входа. Простота же состоит в том, что, как будет показано далее, в этом случае следует оказывать противодействие только явным угрозам преодоления парольной защиты, от которых защититься не представляет большого труда.

Основной же угрозой служат преднамеренные или неумышленные действия санкционированного пользователя, который обладает возможностью осуществления скрытой атаки на защищаемый ресурс (например, запустив какую-либо программу собственной разработки).

Очевидно, что механизмы идентификации и аутентификации должны предусматривать противодействие всем потенциальным злоумышленникам, т.е. как сторонним по отношению к защищаемому объекту, так и санкционированным пользователям, зарегистрированным на компьютере. При этом речь идет о прикладных пользователях, т.к. осуществить какую-либо защиту от НСД к информации от администратора безопасности невозможно, даже включая применение механизмов криптографической защиты (он сумеет снять информацию до момента ее поступления в драйвер шифрования).

С учетом сказанного можно сделать следующие выводы:

1. На защищаемом объекте, как правило, зарегистрированы, по крайней мере, два пользователя - прикладной пользователь и администратор безопасности. Поэтому в качестве потенциального злоумышленника при реализации механизмов парольной защиты в общем случае следует рассматривать не только стороннее по отношению к защищаемому объекту лицо, но и санкционированного пользователя, который преднамеренно либо неумышленно может осуществить атаку на механизм парольной защиты.

2. Рассматривая атаки на парольную защиту следует учитывать, что по сравнению со сторонним лицом, которое может характеризоваться явными угрозами парольной защите, защита от

атак санкционированного пользователя качественно сложнее, т.к. им могут быть реализованы скрытые угрозы.

Классификация задач, решаемых механизмами идентификации и аутентификации.

Классификация задач по назначению защищаемого объекта.

Основу классификации задач, решаемых механизмами парольной защиты, составляет назначение защищаемого объекта (компьютера). Именно в соответствии с назначением объекта определяется перечень защищаемых ресурсов и источников угроз (потенциальных злоумышленников).

Рассматриваемые процедуры парольной защиты могут устанавливаться на любые действия системы и пользователя (например, на запуск каждого процесса). Однако необходимо понимать, что это, как правило, не оправдано, поскольку приводит к существенной дополнительной загрузке вычислительного ресурса, т.к. данная процедура выполняется не автоматически.

Возможные классификации механизмов авторизации, реализованных в современных системах защиты.

Классификации механизмов идентификации и аутентификации, получены на основе анализа применения механизмов парольной защиты в ОС (прежде всего семейства Windows), приложениях и современных добавочных средствах защиты ОС.

Классификация по функциональному назначению (классификация решаемых задач) процедур идентификации и аутентификации, применяемых на практике в системах защиты (в том числе и в добавочных средствах защиты):

1. *Функциональное назначение процедур идентификации аутентификации:*

1.1. *Контроль загрузки:*

- 1.1.1. Доступ к загрузке системы.
- 1.1.2. Доступ к заданию способа загрузки.
- 1.1.3. Доступ к заданию режима загрузки.

1.2. *Контроль функционирования:*

- 1.2.1. Доступ к системе.
- 1.2.2. Доступ к запуску процесса (приложения).
- 1.2.3. Доступ к локальным ресурсам системы.
- 1.2.4. Доступ к сетевым ресурсам.

1.3. *Блокирование:*

- 1.3.1. Загрузки системы.

- 1.3.2. Доступа в систему.
- 1.3.3. Учетной записи пользователя.
- 1.3.4. Загрузка приложения.

Классификация по принадлежности идентификаторов и паролей:

1. *Принадлежность идентификатора и пароля:*

1.1. *Пользователь:*

- 1.1.1. Прикладной.
- 1.1.2. Администратор.

1.2. Ответственное лицо.

Классификация по способу задания идентификатора и пароля:

1. Способ задания идентификатора и пароля:

- 1.1. Администратором.
- 1.2. Пользователем.
- 1.3. Ответственным лицом.

Классификация по способу ввода идентификатора и пароля:

1. Способ ввода идентификатора и пароля:

- 1.1. Ввод с клавиатуры.
- 1.2. Ввод с внешнего носителя:
 - 1.2.1. Стандартные устройства ввода.
 - 1.2.2. Специализированные устройства ввода.

Классификация по способу хранения идентификатора и пароля:

- 1. Локально на защищаемом объекте.
- 2. Удаленно на сервере.

3.3.3.2. *Парольная защита*

Функциональное назначение механизмов парольной защиты.

По функциональному назначению парольный вход, как правило, используется для контроля загрузки системы, контроля функционирования и с целью блокировки. С целью контроля загрузки может устанавливаться процедура идентификации и аутентификации пользователя перед началом загрузки системы, например, встроенными средствами BIOS. В этом случае выполнить загрузку системы сможет только санкционированный пользователь.

Доступ к заданию режима загрузки контролируется штатными средствами BIOS, где после аутентификации пользователь может установить, откуда загружается система - с жесткого диска или с внешнего носителя, а также указать очередность выбора средств

загрузки. В качестве контроля доступа к заданию режима загрузки может устанавливаться парольный вход на возможность загрузки в безопасном режиме. Например, для загрузки в режиме Safe Mode для ОС Windows 2000/XP пользователю необходимо пройти авторизацию. Загрузиться в аналогичном безопасном режиме в ОС семейства UNIX после авторизации может только пользователь с правами «root».

Для решения задачи контроля функционирования вычислительной системы выделяются:

- *Контроль пользователя при доступе в систему.* Реализуется в том числе штатными средствами ОС.

- *Контроль при запуске процесса.* Благодаря этому при запуске некоторых приложений может быть установлена парольная защита. Прежде всего, здесь интерес представляет установка пароля ответственного лица, например, начальника подразделения (будет рассмотрено ниже).

- *Контроль при доступе к локальным ресурсам.* Например, при доступе к локальному принтеру и т.д. также может использоваться аутентификация ответственного лица.

- *Контроль при доступе к сетевым ресурсам.* Реализуется в том числе штатными средствами ОС. Например, доступ к ресурсам можно разделить паролем. Так осуществляется сетевой доступ к общим ресурсам по протоколу NETBIOS для ОС семейства Windows.

В качестве реакции на несанкционированные действия пользователя системой защиты может устанавливаться блокировка некоторых функций: загрузки системы, доступа в систему, учетных записей пользователя (идентификаторов), запуска определенных приложений. Для снятия блокировки необходима авторизация администратора безопасности или ответственного лица.

Кроме того, пользователь может сам выставить блокировку на доступ к системе и к приложениям и т.д., чтобы доступ в систему и к этим приложениям в его отсутствие был заблокирован. Для разблокировки приложения необходимо авторизоваться текущему пользователю. При этом администратор безопасности может блокировать учетные записи пользователей для входа в систему в нерабочее время.

С учетом введенной классификации может быть сделан вывод о функциональном назначении применения механизмов парольной защиты:

- С целью контроля загрузки может устанавливаться возможность контроля пользователя перед началом загрузки системы. Кроме того, контроль пользователя может осуществляться при задании способа и при доступе к заданию режима загрузки.

- С целью контроля доступа выделяется контроль пользователя при доступе в систему. Также могут иметь место контроль при запуске процесса (прежде всего, здесь интерес представляет установка пароля ответственного лица) и контроль при доступе к локальным и сетевым ресурсам.

- С целью снятия блокировки (реакции) используется контроль администратора безопасности или ответственного лица. Кроме того, пользователь может выставить блокировку на некоторые приложения и т.д. Для их снятия осуществляется контроль пользователя.

Особенности парольной защиты, исходя из принадлежности пароля.

С точки зрения принадлежности пароля в классификации выделены «пользователь», к которому относится прикладной пользователь системы и администратор, а также «ответственное лицо», в качестве которого может, например, выступать начальник подразделения. Авторизация ответственного лица может устанавливаться для реализации физического контроля доступа пользователя к ресурсам, прежде всего, к запуску процесса. При этом особенностью здесь является то, что авторизация ответственного лица осуществляется не при доступе в систему, а в процессе функционирования текущего пользователя.

Рассмотрим пример. Пусть требуется обеспечить физически контролируемый доступ к внешней сети, например, к сети Internet. На запуск соответствующего приложения устанавливается механизм авторизации ответственного лица (его учетные данные хранятся в системе защиты). Тогда при запуске соответствующего приложения появится окно авторизации ответственного лица, и приложение может быть запущено только после его успешной авторизации. При этом приложение запускается только на один сеанс.

Таким образом, приложение физически запускается ответственным лицом с локальной консоли защищаемого объекта. В результате ответственное лицо будет знать, кто и когда запросил доступ в сеть Internet, так как сам принимает решение - разрешать доступ или нет. Если доступ разрешается, ответственное лицо может полностью контролировать данный доступ, т.к. запуск приложения возможен только в его присутствии.

В соответствии с классификацией принадлежности учетной записи введена и классификация способов задания учетных данных (идентификаторов и паролей). Соответственно, назначение учетных данных могут осуществлять как владелец учетной записи, так и администратор (принудительно).

Реализация механизмов парольной защиты.

Ввод идентификатора и пароля может осуществляться, как с применением штатных средств компьютера - клавиатуры, устройств ввода (например, дисковод - с дискеты), так и с использованием специализированных устройств аутентификации - всевозможных аппаратных ключей, биометрических устройств ввода параметров и т.д.

Естественно, что для сравнения вводимой и эталонной информации, эталонные учетные данные пользователей должны где-то храниться. Возможно хранение эталонных учетных данных непосредственно на защищаемом объекте. Тогда при вводе учетных данных из памяти считываются эталонные значения и сравниваются с вводимыми данными.

Кроме того, эталонные данные могут располагаться на сервере. Тогда эталонные значения на защищаемом объекте не хранятся, а вводимые данные передаются на сервер, где и сравниваются с эталоном. При этом именно с сервера разрешается или запрещается доступ субъекту, который ввел учетные данные.

Очевидно, что хранить эталонный пароль, как на защищаемом объекте, так и на сервере в открытом виде недопустимо. Поэтому для хранения пароля используется необратимое преобразование (хеш-функция), позволяющая создавать некий образ пароля - прямое преобразование. Этот образ однозначно соответствует паролю, но не позволяет осуществить обратное преобразование - из образа восстановить пароль. Образы паролей уже могут храниться на защищаемом объекте, т.к. их знание не позволяет злоумышленнику восстановить исходный пароль. Для реализации необратимого преобразования наиболее часто на сегодняшний день используется алгоритм хеширования MD5.

Угрозы преодоления парольной защиты.

Обобщенная классификация основных угроз парольной защите следующая:

1. Угрозы преодоления парольной защиты:

1.1. Явные:

1.1.1. Физические:

- 1.1.1.1. Хищение носителя;
- 1.1.1.2. Визуальный съем пароля при входе.
- 1.1.2. Технические:
 - 1.1.2.1. Подбор пароля:
 - 1.1.2.1.1. Автоматизированный;
 - 1.1.2.1.2. Автоматический.
 - 1.1.2.2. Съем пароля на защищаемом объекте.
- 1.2. Скрытые:
 - 1.2.1. Технический съем пароля при вводе:
 - 1.2.1.1. Снифер клавиатуры;
 - 1.2.1.2. Снифер канала.
 - 1.2.2. Отключение механизма защиты идентификации и аутентификации.
 - 1.2.3. Модификация учетных данных на защищаемом объекте:
 - 1.2.3.1. Замена учетных данных;
 - 1.2.3.2. Сброс пароля.

Данная классификация сделана как в соответствии со статистикой известных угроз, так и в соответствии с потенциально возможными угрозами. Кроме того, при построении данной классификации учитывался анализ принципов работы механизмов идентификации и аутентификации.

Рассмотрим представленные угрозы. Наиболее очевидными явными угрозами являются физические хищение носителя (например, дискеты с паролем, электронного ключа с парольной информацией и т.д.), а также визуальный съем пароля при вводе (с клавиатуры, либо с монитора). Кроме того, при использовании длинных сложных паролей пользователи подчас записывают свой пароль, что также является объектом физического хищения.

К техническим явным угрозам можно отнести подбор пароля - либо автоматизированный (вручную пользователем), либо автоматический, предполагающий запуск пользователем специальной программы подбора паролей. Кроме того, для сравнения вводимого и эталонного значений пароля, эталонное значение пароля должно храниться на защищаемом объекте (либо на сервере в сети). Это эталонное значение без соблюдения соответствующих мер по хранению паролей (хеширование, разграничение доступа к области памяти или реестра, где хранятся пароли), может быть похищено злоумышленником.

Естественно, что наиболее опасными являются скрытые

угрозы, например:

- технический съём пароля при вводе;
- модификация механизма парольной защиты;
- модификация учетных данных на защищаемом объекте.

Первая группа скрытых угроз наиболее очевидна. Пароль должен быть каким-либо образом введен в систему с клавиатуры, со встроенного или дополнительного устройства ввода, из сети (по каналу связи). При этом злоумышленником может быть установлена соответствующая программа, позволяющая перехватывать поступающую на защищаемый объект информацию. Развитые подобные программы позволяют автоматически фильтровать перехватываемую информацию по определенным признакам - в том числе, с целью обнаружения паролей. Примером таких программ могут служить sniffеры клавиатуры и канала связи. Например, sniffер клавиатуры позволяет запоминать все последовательности нажатий кнопок на клавиатуре (здесь пароль вводится в явном виде), а затем фильтровать события по типам приложений.

Злоумышленник, установив подобную программу, и задав режим ее запуска при входе в систему какого-либо пользователя, получит его пароль в открытом виде. Затем, например, троянская программа может выдать этот пароль по сети на другую рабочую станцию. Таким образом, если в системе зарегистрировано несколько пользователей, то один пользователь может узнать пароль другого пользователя, а затем осуществить доступ в систему с правами последнего и т.д.

Второй тип скрытых угроз предполагает возможность отключить механизм парольной защиты злоумышленником, например, загрузить систему с внешнего носителя (дисковода или CD-ROM). Если механизм парольной защиты представляет собой некий процесс (в добавочной системе защиты), то выполнение данного процесса можно остановить средствами системного монитора, либо монитора приложений, например, встроенными средствами в оболочку Fag. Подобная возможность существует для ОС Windows Me.

Третья группа скрытых угроз заключается в модификации учетных данных на защищаемом объекте. Это осуществляется либо путем их замены, либо путем сброса в исходное состояние настроек механизма защиты. Примером может служить известная программная атака на BIOS - сброс настроек BIOS в исходное состояние посредством изменения контрольных сумм BIOS.

Из этого можно сделать важный вывод, подтверждающий выводы, сделанные ранее: *каким бы надежным ни был механизм парольной защиты, он сам по себе в отдельности, без применения иных механизмов защиты, не может обеспечить сколько-нибудь высокого уровня безопасности защищаемого объекта.*

Другой вывод состоит в том, что *невозможно сравнивать между собой альтернативные подходы к реализации механизма защиты (в частности, механизма парольной защиты), так как можно оценивать лишь уровень защищенности, обеспечиваемый всей системой защиты в целом, то есть обеспечиваемый совокупностью механизмов защиты (с учетом их реализации), комплексированных в системе.*

Способы усиления парольной защиты.

Основные механизмы ввода пароля. Усиление парольной защиты за счет усовершенствования механизма ввода пароля.

Рассмотрим основные известные на сегодняшний день способы ввода пароля:

1. Консольный (ввод с клавиатуры);
2. С внешнего носителя;
3. С использованием биометрических характеристик пользователя.
4. Комбинированный (объединяет консольный и с внешнего носителя).

Наиболее очевидный способ ввода пароля, который реализован практически во всех ОС, состоит в вводе пароля с клавиатуры. Недостатком данного способа является возможность визуального съема пароля злоумышленником. При этом в меньшей степени опасность представляет набор пароля пользователем на клавиатуре - этому можно противодействовать организационными мерами. В большей степени угроза состоит в том, что при задании сложного пароля пользователь стремится его куда-нибудь записать, чтобы не забыть.

В качестве противодействия угрозе визуального съема пароля могут использоваться внешние носители информации. При этом могут использоваться как стандартные средства ввода информации (например, флэш), так и средства, предполагающие подключение специальных средств ввода парольной информации — всевозможные электронные ключи, «таблетки» и т.д. На этих носителях записывается пароль, который считывается системой при аутентификации пользователя. Здесь может задаваться достаточно

большая длина пароля без угрозы его визуального съема. Применение для ввода пароля стандартного или специального носителя с точки зрения обеспечиваемого уровня безопасности практически равноценно. Вопрос выбора носителя определяется его ценой, долговечностью, удобством хранения.

Дополнительные носители парольной информации для усиления парольной защиты ОС используются практически всеми современными средствами добавочной защиты.

Недостатком применения внешних носителей информации для ввода пароля является потенциальная угроза его хищения злоумышленником.

Для противодействия хищению злоумышленником носителя информации с паролем могут рассматриваться следующие альтернативные способы защиты:

- Использование биометрических характеристик пользователя - подход, позволяющий отказаться от внешнего носителя с паролем как такового. При этом идентификатором пользователя становятся его биометрические параметры. Причем ввиду их однозначного соответствия пользователю эти параметры служат одновременно и паролем.

- Комбинирование способа ввода пароля с клавиатуры и способа ввода пароля с внешнего носителя. Например, механизм ввода пароля с клавиатуры может рассматриваться как дополнение к механизму ввода пароля с внешнего носителя.

Комбинированный способ осуществляется двумя механизмами, один из которых является основным, а другой - дополнительным. На наш взгляд, при защите компьютеров имеет смысл использовать следующий комбинированный способ ввода пароля:

- основной - с внешнего носителя (целесообразно реализовать добавочными средствами защиты);

- дополнительный - с клавиатуры (для этого могут использоваться встроенные в ОС механизмы авторизации пользователя).

Таким образом, можно выделить следующие приоритеты в использовании механизмов ввода пароля (расположены в порядке убывания):

1. Биометрический способ идентификации пользователя;
2. Комбинированный способ (консольный ввод плюс использование внешнего носителя);

3. Ввод пароля с внешнего носителя;

4. Консольный ввод (ввод пароля с клавиатуры).

Соответственно механизмы парольной защиты можно усиливать уже на этапе ввода пароля. Для этого необходимо в системе предусмотреть наиболее приоритетный способ ввода пароля.

Основное достоинство биометрических систем контроля доступа.

Новая парольная защита, реализуется на основе контроля биометрических характеристик пользователя.

Гипотетически возможна угроза, связанная с тем, что один пользователь передает свои парольные данные другому пользователю, а тот воспользуется ими для несанкционированного входа в систему последним (в определенном смысле это можно трактовать, как изменение ПРД к ресурсам пользователем не администратором безопасности, что противоречит формальным требованиям к системе защиты).

В общем же случае механизмы биометрической идентификации пользователя (естественно, при их корректной реализации) предотвращают возможность какой-либо передачи парольной информации между пользователями. А это достаточно важно при реализации централизованной (без участия пользователя) схемы администрирования механизмов защиты. В этом и заключается несомненное достоинство данных подходов парольной защиты по сравнению с применением внешних аппаратных носителей парольных данных (всевозможных ключей, смарт-карт и т.д.). Другими словами, *корректно в общем случае концепция централизованного администрирования системы защиты может быть реализована с применением биометрических систем контроля доступа.*

Достоинством же применения внешних аппаратных носителей парольных данных является большая универсальность в смысле возможности хранения учетных данных. То есть на них может храниться не только информация, идентифицирующая пользователя, но и ключи шифрования, а также иные данные.

Основные способы усиления парольной защиты, используемые в современных ОС и приложениях.

Классификация основных способов усиления пароля, используемых в современных ОС и в приложениях:

1. *Способы усиления пароля:*

1.1. Посредством задания дополнительных требований к параметрам пароля:

1.1.1. Увеличение длины пароля (число символов в пароле);

1.1.2. Увеличение алфавита набором символов одного типа для задания пароля;

1.1.3. Увеличение алфавита набором типов символов для задания пароля.

1.2. Посредством исключения ограничений на процедуру аутентификации:

1.2.1. Ограничение на число неверных введенных значений пароля;

1.2.2. Ограничение на число типов символов в пароле;

1.2.3. Ограничение на повторяемость пароля (история паролей);

1.2.4. Ограничение на возможность задания простых паролей;

1.2.5. Ограничение на периодичность смены пароля пользователем.

Все они призваны воспрепятствовать подбору пароля злоумышленником.

Анализ способов усиления парольной защиты.

Каковы же цели применения рассматриваемых способов усиления пароля.

Руководящие документы ФСТЭК России не дают конкретных рекомендаций по выбору пароля или расчету его стойкости, за исключением длины, которая составляет от 6 (класс 3Б, 3А, 2Б, 2А) до 8 (класс 1Б, 1А) буквенно-цифровых символов и необходимости периодической смены пароля.

Существуют методы количественной оценки стойкости парольных систем [18] (формула Андерсона):

$$4,32 \times 10^4 \times (k) \frac{M}{P} \leq A^1, \quad (3.37)$$

где k - количество попыток подбора пароля в минуту;

M - время действия пароля в месяцах;

P - вероятность подбора пароля;

A^1 - мощность пространства паролей (A - мощность алфавита

паролей, l - длина пароля).

Таким образом, наибольшее влияние на вероятность раскрытия пароля оказывает величина l . Другие составляющие данной формулы чрезвычайно редко оказывают влияние на величину P , превышающее один порядок. Увеличение же длины пароля только на один символ значительно увеличивает требуемое злоумышленнику время для его раскрытия.

Параметры P , V , T и A^l связаны между собой следующим соотношением [18]:

$$P = \frac{V \times T}{A^l}, \quad (3.38)$$

где P - вероятность подбора пароля в течение его срока действия (подбор осуществляется непрерывно в течение всего срока действия пароля);

V - скорость подбора паролей (скорость обработки одной попытки регистрации проверяющей стороной либо скорость вычисления хэш-значения одного пробного пароля);

T - срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть сменен);

A^l - мощность пространства паролей (A - мощность алфавита паролей, l - длина пароля).

В случае, когда неизвестна точная длина искомого пароля, максимальное время подбора пароля ($T_{\max}$) будет вычисляться в соответствии со следующей формулой [18]:

$$T_{\max} = \frac{\sum_{i=1}^l A^i}{V} \quad (3.39)$$

Доскональное знание способов хранения учетных записей пользователей в базе данных системы защиты позволяет оптимизировать программы восстановления (вскрытия) паролей. Подробные знания организации парольной системы операционных систем Windows 2000/XP позволяют авторам указанных программ заявлять скорость осуществления перебора от 3,9 миллиона паролей/сек. до 5,4 миллиона паролей/сек. на ПЭВМ с процессором Athlon XP 1700+ или говорить о возможности нахождения всех алфавитно-цифровых паролей за трое суток на ПЭВМ с процессором Pentium II/450 [18].

исследователю Филиппу Экслину удается взламывать алфавитно-цифровые пароли Windows в среднем за 13,6 секунды. Для взлома использовался компьютер на базе процессора Athlon XP 2500+ с 1,5 Гб оперативной памяти. Таблица, в которой хранились варианты паролей, занимала 1,4 Гб и полностью загружалась в оперативную память компьютера, что позволило существенно поднять скорость взлома. При размере таблицы в 20 Гб и наличии в пароле букв, цифр и 16 спецсимволов пароль взламывается, в среднем, за 30 секунд.

Итак, какой же пароль сможет оказать достойное сопротивление попыткам его подбора? Длинный, состоящий из букв разного регистра, цифр и спецсимволов. При этом он должен быть случайным, т.е. выбор символов осуществляется произвольно (без какой бы то ни было системы) и более нигде не использоваться, при этом единственным местом фиксации пароля должна быть голова единственного человека. Однако необходимо учитывать и вопросы практического использования пароля. Очень длинный пароль сложно запомнить, особенно, если учесть тот факт, что пользователю приходится иметь не один пароль. Осуществить быстрый ввод длинного пароля также не представляется возможным. Произвольно выбранные символы запомнятся, если их произнесение вслух имеет запоминаемую звуковую форму (благозвучие) или они имеют характерное расположение на клавиатуре, в противном случае без шпаргалки не обойтись.

Помочь пользователю составить пароль по определенным критериям могут программы генерации паролей. Одна из таких программ *Advanced Password Generator* позволяет создавать пароли с помощью генератора случайных чисел либо по задаваемому пользователем ключевому слову, а также содержит алгоритм создания слов, наиболее близких к естественному языку (русскому или английскому). При использовании указанного режима получаются «запоминаемые», но не имеющие смысла слова. Под термином «запоминаемый» следует понимать благозвучность получаемой комбинации. В этом режиме использование цифр, спецсимволов или смешанного регистра букв автоматически отключается.

Вот несколько созданных программой «запоминаемых» паролей: ELASWOWA, DEDRYTON, BENEROMO, SARMANED. Программа позволяет создавать пароль длиной от 4 до 32 символов.

«Запоминаемый» пароль из 32 символов выглядит, например, так: NONEERESSPYOVENAPARDERETOURVENFF.

Пароль DV24*KK4 также можно отнести к «запоминаемым», несмотря на наличие цифр и спецсимвола.

Уникальность сгенерированного подобного рода программами пароля напрямую зависит от степени «случайности» используемого для этих целей генератора. Современные комплексы защиты информации ограничивают возможную длину используемого пароля 12 - 16 символами. Чаще всего это латинские буквы, цифры и специальные символы. Большинство СЗИ обладает следующими возможностями по увеличению эффективности парольной системы:

1. *Установление минимальной длины пароля;*
2. *Установление максимального срока действия пароля;*
3. *Установление требования не повторяемости паролей (препятствует замене пароля по истечении его срока действия на один из используемых ранее);*
4. *Ограничение числа попыток ввода пароля (блокирует пользователя после превышения определенного количества попыток ввода, осуществляемых подряд; но не действует на учетную запись администратора).*

Для того чтобы усложнить задачу злоумышленника по получению базы данных системы защиты многие СЗИ хранят ее в энергонезависимой памяти своей аппаратной части. Некоторые комплексы защиты информации от НСД содержат встроенные механизмы генерации паролей и доведения их до пользователей. Очевидным минусом и основным фактором, толкающим пользователя записать пароль, является невозможность запоминания «абракадабры» из, к примеру, 8 буквенно-цифровых символов никак не связанных между собой. В случае если пользователю самостоятельно необходимо сформировать пароль, в качестве критериев выбора пароля можно выделить следующие:

1. *Использование букв разных регистров;*
2. *Использование цифр и спецсимволов совместно с буквами.*

При составлении пароля не рекомендуется использовать:

1. *Свое регистрационное имя, в каком бы то ни было виде (как есть, обращенное, заглавными буквами, удвоенное, и т.д.);*
2. *Свое имя, фамилию или отчество в каком бы то ни было виде;*
3. *Имена близких родственников; информацию о себе, которую легко можно получить. Она включает номера телефонов, номера*

лицевых счетов, номер вашего автомобиля, название улицы, на которой вы живете, и т.д.:

4. Пароль из одних цифр или из одних букв;

5. Слово, которое можно найти в словарях.

Нужно запомнить (постараться не записывать) свой пароль. Если запомнить качественный пароль оказалось непосильной задачей для вас, не записывайте пароль целиком, разделите его на две части и запишите в разных местах. Только не оснащайте эти записи комментариями типа: «Это первая часть моего пароля для выхода в Интернет, вторая часть на следующей странице». Если вы составляли пароль по фразе, то, например, запись вида: Everybody*love(the)freedom, напомним, что ваш пароль: e*v(e) (брали каждую третью букву с добавлением спецсимволов). Более скрытный способ предполагает дополнение записанного по определенному пользователем принципу. В этом случае найденная запись: DeReVo не позволит автоматически раскрыть действительный пароль: *DterReceV*o.

И все-таки, пароль, используемый для работы с информацией ограниченного доступа, необходимо запомнить и нигде не записывать. Необходимо потренироваться вводить пароль, чтобы эта процедура занимала как можно меньше времени. Несмотря на то, что желательно уметь вводить пароль не глядя на клавиатуру, на первых порах подключайте зрительную память. Главное правило: никто, кроме вас, не должен знать ваш пароль. Вот несколько вариантов подбора элементов, составляющих пароль:

1. Выберите строку или две строки из песни или поэмы и используйте первую букву каждого слова, добавьте цифры (спецсимволы);

2. Выберите известное изречение (поговорку, слоган и т.п.) и используйте каждую четвертую букву, добавьте цифры (спецсимволы);

3. Замените в слове одну согласную и одну или две гласных, добавьте цифры (спецсимволы);

4. Выберите два коротких слова и соедините их вместе со знаком пунктуации между ними, добавьте цифры (спецсимволы).

Но существует «парадокс человеческого фактора». Состоит он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее.

Действительно, необходимость ввода пароля каждый раз при входе в систему, не говоря уже о необходимости запоминать сложную знаковую последовательность, удобством не является. Единственной мерой противодействия указанному обстоятельству является формирование у пользователей грамотного подхода к вопросам обеспечения безопасности информации.

Но эти методы (учет параметров, характеризующих процедуру ввода пароля пользователем - скорость набора символов и др.) едва ли применимы в распространенных приложениях ввиду их тривиальности. Поэтому рассмотрим другие [18].

Пусть A - исходный алфавит для задания пароля (некоторое число символов, включая их типы, для назначения пароля), а L — длина пароля. В этих предположениях число возможных паролевых комбинаций составит:

$$R = f(A, L). \quad (3.40)$$

Обозначим вероятность подбора злоумышленником пароля с одной попытки P_1 (в предположении, что все паролевые комбинации равновероятны: $P_1 = 1/R$). Если для подбора пароля злоумышленником совершается n попыток в единицу времени t , то за интервал времени T (число единиц времени), вероятность подбора пароля злоумышленником будет описываться следующей зависимостью:

$$P = F(A, L, P_1, n(t), T). \quad (3.41)$$

Теперь, в соответствии с полученной зависимостью, рассмотрим, какие способы усиления пароля (указаны в п.3.3.3.2) на какой параметр призваны влиять.

Применение способов усиления пароля, посредством задания дополнительных требований к параметрам пароля в соответствии с зависимостью $R = f(A, L)$ призваны увеличить число возможных паролевых комбинаций.

Ограничения на «число типов символов в пароле», «возможность задания простых паролей», и на «повторяемость паролей» задаются с целью уменьшения параметра P_1 , то есть с целью, по возможности, обеспечить равновероятность для злоумышленника всех исходных паролевых комбинаций.

Ограничение на «число неверно введенных значений пароля» реализует возможность совершить пользователю только заданное число N попыток подбора пароля. В случае превышения этого

количества может либо блокироваться учетная запись данного пользователя, либо блокироваться защищаемый объект в целом.

Данное ограничение является одним из важнейших, т.к. оно призвано противодействовать возможности автоматического подбора паролей. В этом случае число попыток подбора злоумышленником жестко фиксировано параметром N и исходная зависимость для вероятности подбора пароля злоумышленником принимает следующий вид:

$$P = F(A, L, P1, N). \quad (3.42)$$

Данное ограничение можно рассматривать как альтернативу применению способов усиления пароля, основанных на дополнительных требованиях к параметрам пароля в соответствии с зависимостью $R = f(A, L)$. То есть, уменьшая параметр N , тем самым можно снижать требования к параметру L . А это, как отмечено ранее, крайне важно при использовании механизма парольной защиты, предполагающего ввод пароля с клавиатуры. Очевидно, что без использования данного ограничения с учетом больших темпов роста производительности компьютеров, приводящего к заметному увеличению параметра $n(t)$, без применения данного ограничения соответственно возрастают требования к параметрам A, L .

Ранее было отмечено, что в основе проектирования системы защиты должен лежать системный подход. В рамках этого подхода при проектировании механизмов парольной защиты необходимо учитывать наличие других механизмов в системе защиты.

Так, если в системе защиты обеспечена замкнутость программной среды, которая не позволит пользователю запустить программу подбора паролей, т.е. реализовать автоматический способ подбора, то не столь актуальным становится и реализация ограничения на число неверно введенных значений пароля. Действительно, в этом случае параметр $n(t)$ уже имеет значение: 1-на попытка за 5... 15 с. (определяется скоростью ручного ввода пароля пользователем), что не позволит сколько-нибудь эффективно противодействовать парольной защите.

С учетом сказанного можно сделать важный вывод: существуют альтернативные подходы к усилению пароля с целью преодоления возможности его подбора. Наиболее эффективным из них можно признать «Ограничение на число неверно введенных значений пароля», использование которого позволяет существенно снизить требования к длине пароля. Однако, аналогичный результат

достигается, если в системе защиты обеспечивается замкнутость программной среды, противодействующая выполнению автоматического (программного) подбора пароля.

Кроме того, в случае, если не используется ограничение на число неверно введенных значений пароля, вероятность подбора пароля зависит не только от параметра $n(t)$, но и от параметра T . При этом данное ограничение устанавливается на параметр T , позволяя снизить суммарное число попыток подбора для одного установленного значения пароля (за счет ограничения отведенного на это времени).

Возможность ограничения «на число неверно введенных значений пароля» является важнейшей в части усиления парольной защиты и, наряду с другими рассмотренными выше возможностями, присутствует в механизмах парольной защиты практически всех современных ОС большинства приложений. При этом в различных семействах ОС возможности установки ограничений на пароль различаются незначительно.

Дополнительно в системах парольной защиты может использоваться ограничение на периодичность смены пароля пользователем, которое призвано ограничить возможность использования одного и того же значения пароля в течение сколь угодно продолжительного времени (например, более месяца).

3.3.3.3. Методы добавочных механизмов усиления парольной защиты

Требования к добавочным механизмам в рамках усиления парольной защиты.

Как отмечалось ранее, важнейшими способами усиления парольной защиты является комплексное использование механизмов, так как сам по себе механизм парольной защиты не может обеспечить гарантированной защиты от несанкционированного входа в систему.

Рассмотрим группу задач, которые должны решаться средствами добавочной защиты в общем случае, без учета реализации встроенных в ОС механизмов защиты.

Добавочной защитой в рамках противодействия скрытым угрозам преодоления механизма парольной защиты должны решаться следующие задачи [18]:

- должна обеспечиваться замкнутость программной среды, не позволяющая запускать пользователю в системе программы с целью осуществления нерегламентированных действий, например, запуск

программ-снифферов (канала связи, каналов ввода с внешних устройств и с клавиатуры) и иных потенциально опасных программ, в частности, позволяющих модифицировать механизм парольной защиты;

- должно обеспечиваться разграничение прав доступа к реестру ОС (для ОС семейства Windows), к каталогам и файлам, хранящим учетные данные механизмов парольной защиты для ОС UNIX;

- должен обеспечиваться контроль целостности (с возможностью автоматического восстановления из эталонной копии) ключей и ветвей реестра, а также файлов, хранящих учетные данные механизмов парольной защиты, применяемый в предположении, что разграничение прав доступа к реестру ОС, каталогам и файлам злоумышленником преодолены;

- должна обеспечиваться защита от возможности отключения механизма защиты, в частности, возможности загрузки системы с внешних устройств, останова процесса или драйвера, реализующего парольную защиту добавочными средствами;

- должно обеспечиваться хеширование паролей, применяемое в предположении, что разграничение прав доступа к реестру ОС, каталогам и файлам злоумышленником преодолены, в том числе с использованием ошибок и закладок в ПО.

Необходимые механизмы добавочной защиты, направленные на усиление парольной защиты.

С учетом сказанного можно выделить ряд механизмов, которые должны быть реализованы с целью усиления парольной защиты от скрытых угроз на защищаемом объекте. В общем случае эти механизмы таковы [18]:

- Механизм обеспечения замкнутости программной среды.

- Механизм разграничения прав доступа к настройкам ОС и приложений (к реестру ОС для ОС семейства Windows, к каталогам и файлам настроек для ОС семейства Unix).

- Механизм контроля целостности с возможностью автоматического восстановления из резервной копии настроек ОС и приложений (ключей реестра ОС для ОС семейства Windows, файлов для ОС семейства Unix).

- Механизм защиты от возможности отключения парольной защиты, в частности, возможности загрузки системы с внешних устройств, останова процесса или драйвера, реализующего парольную защиту добавочными средствами.

- Механизм хеширования парольной информации и др.

Применяющиеся подходы: двухуровневая авторизация.

Сформулируем требования и рассмотрим, какие используются подходы для усиления механизмов парольной защиты добавочными средствами.

Двухуровневая авторизация на уровне ОС.

Ранее отмечалось, что целесообразно усилить парольную защиту за счет включения в механизм идентификации и аутентификации возможности ввода пароля с внешнего носителя.

Реализация данной возможности имеет смысл, прежде всего, для однопользовательских ОС, к которым относятся ОС семейства Windows (под однопользовательской будем понимать систему, в которой в каждый момент времени может присутствовать только один прикладной пользователь). Здесь пользователь авторизуется при консольном входе в систему. Для многопользовательских ОС, к которым относятся ОС семейства UNIX, характерна удаленная работа на компьютере многих пользователей, поэтому рассматриваемая задача дополнительной авторизации здесь не столь актуальна.

В простейшем случае рассматриваемая возможность усиления парольной защиты достигается подключением внешних носителей пароля к встроенным (прежде всего для ОС Windows) механизмам идентификации и аутентификации. При этом средства разработчика, поставляемые изготовителем аппаратных носителей парольной информации, как правило, содержат соответствующие примеры решения данной задачи.

Однако, как отмечалось ранее, имеет смысл реализовать режим двухуровневой авторизации - так называемый комбинированный режим. При этом авторизация производится сначала с внешнего устройства, а затем с клавиатуры. Это позволяет оказывать противодействие несанкционированному входу в систему при хищении носителя с парольной информацией.

Для современных ОС может быть реализован комбинированный способ авторизации, использующий развитый механизм авторизации пользователя при входе в систему с консоли (например, ОС Windows 2000). Это, собственно, и составляет одну из основных задач добавочной защиты ОС (на практике это реализовано в КСЗИ «Панцирь»).

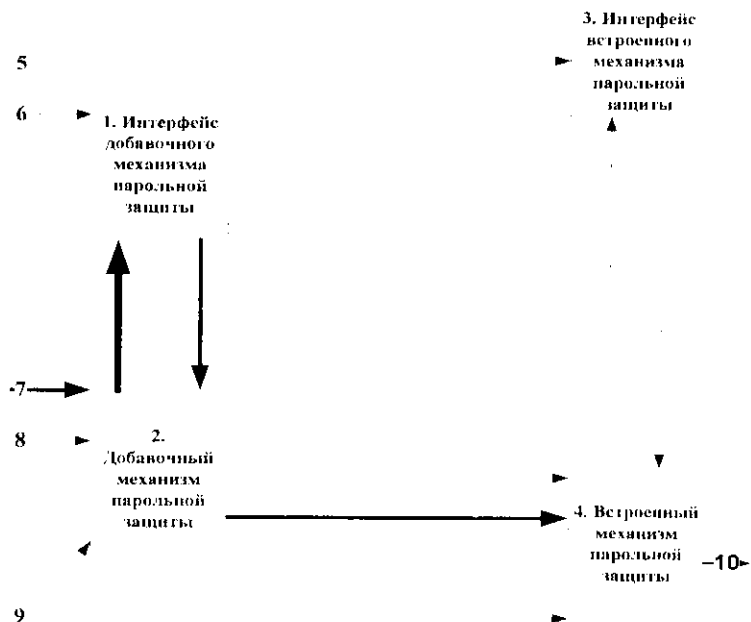


Рис. 3.16. Схема двухуровневой авторизации

Работает схема следующим образом. Сначала из входа 8 задается пароль для аутентификации механизмом добавочной защиты (значение этого пароля записывается на внешний носитель, например, на флэш). Затем из входа 9 задается пароль для аутентификации встроенным механизмом защиты. Этот пароль заносится и в блок 4, и в блок 2. При запросе доступа в систему (из входа 7) блок 2 запускает интерфейс для ввода пользователя пароля со входа 6 (с внешнего носителя).

При успешной аутентификации блоком 2 выдается в блок 4 запрос пользователя на доступ в систему и системный пароль. Причем системный пароль подставляется блоком 2 по запросу аутентификации пользователя блоком 4 без запуска интерфейса 3. Если пароль совпадает, то на выход 10 выдается сигнал об успешном прохождении пользователем процедуры аутентификации. В противном случае, блоком 4 запускается блок 3, и пользователю предлагается пройти аутентификацию из входа 5 в стандартном окне

системной аутентификации - в блоке 3. При успешной аутентификации вырабатывается сигнал на выходе 10.

Таким образом, представленная схема позволяет реализовать два режима аутентификации - одноуровневый и двухуровневый. При одноуровневом режиме из входа 9 в блоки 2 и 4 заносятся одинаковые значения системного пароля для пользователя, а пользователь аутентифицируется только в интерфейсе добавочного механизма парольной защиты. При этом системную аутентификацию за пользователя реализует уже собственно механизм добавочной парольной защиты. Делает он это без выдачи соответствующего окна системной аутентификации на экран монитора.

При двухуровневом режиме (из входа 9 в блоки 2 и 4 заносятся различные значения системного пароля для пользователя), пользователь сначала аутентифицируется в интерфейсе добавочного механизма парольной защиты с использованием внешнего носителя с паролем. Затем, при успешной аутентификации, ему предлагается пройти второй уровень - уровень системной аутентификации в окне ОС. Для этого ему нужно ввести пароль с клавиатуры.

Таким образом, помимо ввода пароля с внешнего носителя, пользователю дополнительно предлагается ввести пароль с клавиатуры. Это предотвращает неконтролируемый вход пользователя в систему при хищении внешнего носителя с паролем. При этом заметим, что требования к дополнительному паролю уже могут быть не столь жесткими, как к основному.

Требованием к реализации данного механизма является отсутствие какой-либо общности как собственно в реализации основного (встроенного в ОС) и добавочного механизмов защиты, так и в способах хранения и преобразования учетных данных пользователей. При выполнении данного требования добавочный механизм может использоваться не только в качестве усиления парольной защиты, но и для резервирования механизма идентификации и аутентификации.

Актуальность и даже необходимость резервирования данного механизма, как одного из основных механизмов защиты от НСД, очевидна. Напомним, что учетные данные пользователя, подтверждаемые паролем при входе пользователя в систему, являются основой задания разграничительной политики доступа к ресурсам.

Двухуровневая авторизация на уровне BIOS.

Альтернативный известный вариант реализации

двухуровневой парольной защиты состоит в реализации добавочного механизма не на уровне входа в ОС, а перед загрузкой системы (средствами расширения BIOS). При этом перед загрузкой системы добавочное средство защиты предлагает пользователю авторизоваться с использованием внешнего носителя пароля. Затем уже при входе в систему могут использоваться штатные средства авторизации ОС. Таким образом, в отличие от рассмотренного выше подхода, здесь заменяется (дополняется) не механизм парольной защиты входа в систему, а механизм парольной защиты BIOS (контроля загрузки системы). Данный подход используется в специальных дополнительных программно-аппаратных средствах защиты, так называемых «электронных замках». (При этом, несмотря на использование аппаратной компоненты, собственно защита осуществляется программно).

К достоинствам данного подхода, по сравнению с рассмотренным выше, можно отнести противодействие скрытым угрозам непосредственно в процессе загрузки системы. В частности, загрузочное меню ОС здесь уже может быть вызвано только санкционированным пользователем.

К очевидным недостаткам данного подхода можно отнести необходимость использования дополнительной аппаратной компоненты системы защиты - платы, реализующей функцию расширения BIOS.

3.3.3.4. Сетевая авторизация

Описанные ранее способы двухуровневой авторизации могут быть реализованы как в локальном, так и в сетевом исполнении. Оба данных подхода могут осуществлять локальную авторизацию добавочным средством при использовании сетевой авторизации пользователя на контроллере домена встроенным в ОС механизмом. Кроме того, для двухуровневой авторизации на уровне ОС оба уровня защиты могут быть выполнены в виде сетевой авторизации. При этом дополнительная авторизация осуществляется на сервере безопасности (т.е. пароли добавочного средства защиты хранятся не на защищаемом компьютере, а на сервере безопасности) [18].

В этом случае механизм добавочной защиты содержит клиентскую часть, устанавливаемую на защищаемый компьютер, и серверную часть, устанавливаемую на сервер безопасности. Серверная часть содержит учетную запись пользователя, а также

пароли для аутентификации пользователя добавочным механизмом защиты и на контроллере домена при выполнении процедуры авторизации, серверная часть функционирует аналогично контроллеру домена. При этом наряду с функциями контроллера домена она реализует собственно процедуру авторизации, выдавая на клиентскую часть (на компьютер, где осуществлена загрузка ОС) окно ввода идентификатора и пароля пользователем. Клиентская же часть осуществляет сокрытие окна авторизации контроллера домена и подстановку пароля ОС, который поступает с серверной части при прохождении авторизации пользователем в добавочном механизме защиты.

Отметим, что применение сетевой авторизации в данном случае, не давая каких-либо преимуществ по защите пароля (предполагая, что на защищаемом компьютере установлено добавочное средство защиты, локально обеспечивающее надежную защиту учетных и парольных данных пользователя), существенно сказывается на надежности функционирования защищаемой сети. Действительно, выход из строя сервера безопасности приводит к отказу всей сети. При этом ни на одном компьютере сети не сможет быть осуществлен вход пользователя в систему. Таким образом, надежность сети в целом (а в общем случае и всех информационных систем, реализованных на базе данной сети) в данном случае определяется надежностью одного компьютера. А это недопустимо в большинстве приложений информационных систем. И, прежде всего, это касается тех из них, которые предполагают распределенную обработку данных.

С учетом сказанного могут быть сформулированы следующие рекомендации по реализации механизмов двухуровневой авторизации: *дополнительный механизм защиты должен быть реализован локально.* При этом системой защиты должно обеспечиваться надежное хранение парольной информации на защищаемом компьютере. Встроенный в ОС механизм может быть настроен как в режиме локальной, так и в режиме сетевой авторизации, в зависимости от задач, решаемых в сети.

3.3.4. Управление доступом к ресурсам

3.3.4.1. Основные требования и задачи управления доступом

Общие положения.

Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам - объектам [18]. В качестве субъектов в простейшем случае понимается пользователь. Однако в дальнейшем это понятие надо будет расширить.

На практике наличие механизмов управления доступом необходимо, даже если в системе может находиться только один прикладной пользователь. Это вызвано тем, что, как правило, в системе должен быть также заведен пользователь с правами администратора, который настраивает параметры системы защиты и права доступа к ресурсам защищаемого объекта. При этом у администратора принципиально иные права, чем у прикладного пользователя. Обо всем этом было изложено ранее.

Абстрактные модели доступа.

Механизм управления доступом реализует на практике некоторую абстрактную (или формальную) модель [18], определяющую правила задания разграничительной политики доступа к защищаемым ресурсам и правила обработки запросов доступа к защищаемым ресурсам.

Модель Биба.

Одной из первых моделей была опубликованная в 1977 году модель Биба (Biba). Согласно этой модели все субъекты и объекты предварительно разделяются по нескольким уровням доступа. Затем на их взаимодействия накладываются следующие ограничения:

- субъект не может вызывать на исполнение субъекты с более низким уровнем доступа;
- субъект не может модифицировать объекты с более высоким уровнем доступа.

Эта модель очень напоминает ограничения, введенные в защищенном режиме микропроцессоров Intel 80386+относительно уровней привилегий.

Модель Гогена-Мезигера.

Модель Гогена-Мезигера (Goguen-Meseguer), представленная

ими в 1982 году, основана на теории автоматов. Согласно этой модели система может при каждом действии переходить из одного разрешенного состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы - домены.

Переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано, какие операции может выполнять субъект, например, из домена С над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская модель.

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, основана на взаимодействии субъектов и потоков информации. Так же как и в предыдущей модели, здесь используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Модель Кларка-Вильсона.

Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989 году. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. В данной модели впервые исследована защищенность третьей стороны - стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор.

Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены субъекта в момент между его идентификацией и собственно командой. Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

Дискреционная (матричная) модель.

Рассмотрим так называемую матричную модель защиты (ее еще называют дискреционной моделью), получившую на сегодняшний день наибольшее распространение на практике. В

терминах матричной модели, состояние системы защиты описывается следующей тройкой:

(S, O, M), где:

S - множество субъектов, являющихся активными структурными элементами модели;

O - множество объектов доступа, являющихся пассивными защищаемыми элементами модели. Каждый объект однозначно идентифицируется с помощью имени объекта;

M - матрица доступа.

Значение элемента матрицы M [S, O] определяет права доступа субъекта S к объекту O.

Права доступа регламентируют способы обращения субъекта S к различным типам объектов доступа. В частности, права доступа субъектов к файловым объектам обычно определяют как чтение (R), запись (W) и выполнение (E).

Основу реализации управления доступом составляет анализ строки матрицы доступа при обращении субъекта к объекту. При этом проверяется строка матрицы, соответствующая объекту, и анализируется - есть ли в ней разрешенные права доступа для субъекта или нет. На основе этого принимается решение о предоставлении доступа.

При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, матричным моделям присущи серьезные недостатки. Основной из них - это излишне детализированный уровень описания отношений субъектов и объектов. Из-за этого усложняется процедура администрирования системы защиты. Причем это происходит как при задании настроек, так и при поддержании их в актуальном состоянии при включении в схему разграничения доступа новых субъектов и объектов. Как следствие, усложнение администрирования может приводить к возникновению ошибок.

Многоуровневые (мандатные) модели.

С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Деннинга. Многоуровневые модели предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или мандатов, назначаемых субъектам и объектам доступа.

Так, для субъекта доступа метки, например, могут определяться в соответствии с уровнем допуска лица к информации, а для объекта доступа (собственно данные) - признаками конфиденциальности информации. Признаки конфиденциальности фиксируются в метке объекта.

В связи с использованием терминов «мандат», «метка», «полномочия» - многоуровневую защиту часто называют соответственно либо мандатной защитой, либо защитой с метками конфиденциальности, либо полномочной защитой

Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности. Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например: конфиденциально, секретно, для служебного пользования, несекретно и т.п.

Основу реализации управления доступом составляют:

1. Формальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрошен доступ;

2. Принятие решений о предоставлении доступа на основе некоторых правил, основу которых составляет противодействие снижению уровня конфиденциальности защищаемой информации.

Таким образом, многоуровневая модель предупреждает возможность преднамеренного или случайного снижения уровня конфиденциальности защищаемой информации за счет ее утечки (умышленного переноса). То есть эта модель препятствует переходу информации из объектов с высоким уровнем конфиденциальности и узким набором категорий доступа в объекты с меньшим уровнем конфиденциальности и более широким набором категорий доступа.

Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа. Причем, так как отдельно взятые категории одного уровня равнозначны, то, чтобы их разграничить наряду с многоуровневой (мандатной) моделью, требуется применение матричной модели.

С помощью многоуровневых моделей возможно существенное упрощение задачи администрирования (настройки). Причем это касается как исходной настройки разграничительной политики доступа (не требуется столь высокого уровня детализации

задания отношения субъект-объект), так и последующего включения в схему администрирования новых объектов и субъектов доступа.

Выбор модели.

Следуя формализованным требованиям к системе защиты информации, основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является *дискреционный механизм управления доступом*, а секретных сведений - *мандатный механизм управления доступом* [16, 17].

Как было показано ранее, в теории защиты информации известны и иные модели управления доступом [18]. Причем ранее были рассмотрены лишь основные из них. Однако, ввиду их более теоретического, нежели практического интереса, останавливаться на них нецелесообразно. Рассмотрим решения, реализованные на практике встроенными и добавочными средствами защиты.

И рассмотрим две основных модели, нашедших отражение в соответствующих нормативных документах в области защиты информации [16, 18] и реализуемых на практике современными ОС и добавочными средствами защиты. Это дискреционная и мандатная модели управления доступом.

Дальнейшее описание дискреционного и мандатного механизмов управления доступом представим в виде рассмотрения формализованных требований к соответствующим механизмам защиты.

Дискреционная модель управления доступом.

Следуя формализованным требованиям к системе защиты информации, основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является дискреционный механизм управления доступом. При этом к нему предъявляются следующие требования [16]:

- Система защиты должна контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

- Для каждой пары (субъект объект) в средстве вычислительной техники (СВТ) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

- Система защиты должна содержать механизм, претворяющий

в жизнь дискреционные правила разграничения доступа.

- Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

- Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил или прав разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов; право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

- Должны быть предусмотрены средства управления, ограничивающие распространения прав на доступ.

Мандатная модель управления доступом.

Основу реализации разграничительной политики доступа к ресурсам при защите секретной информации является требование к реализации, помимо дискреционного, мандатного механизма управления доступом. Требования к мандатному механизму состоят в следующем [16]:

- Каждому субъекту и объекту доступа должны сопоставляться классификационные метки, отражающие их место в соответствующей иерархии (метки конфиденциальности). Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

- Система защиты при вводе новых данных в систему должна запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта ему должны назначаться классификационные метки. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри системы защиты).

- Система защиты должна реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта. При этом иерархические

категории в классификационном уровне субъекта должны включать в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации. При этом все иерархические категории в классификационном уровне субъекта должны включаться в иерархические категории в классификационном уровне объекта.

- Реализация мандатных ПРД должна предусматривать возможность сопровождения, изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

- В СВГ должен быть реализован диспетчер доступа, т.е. средство, во-первых, осуществляющее перехват всех обращений субъектов к объектам, а во-вторых, разграничивающее доступ в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Дополнительные требования к защите секретной информации в контексте использования дискреционной и мандатной моделей управления доступом.

Требования непосредственно к дискреционному и мандатному механизмам.

При защите секретной информации используется и дискреционная и мандатная модели управления доступом. Требования к реализации мандатной модели в рамках защиты секретной информации были приведены в предыдущем пункте. Что касается требований к дискреционному механизму, то при защите секретной информации следует придерживаться тех же требований, что и для защиты конфиденциальной информации (дискреционная модель управления доступом). Однако, в дополнение к последним добавляется еще пара требований:

- Система защиты должна содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, недопустимого с точки зрения заданного ПРД). Под

«явными» [16] подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д. Под «скрытыми» - иные действия, в том числе с использованием злоумышленником собственных программ работы с устройствами.

- Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

Кроме того, отдельно сформулированы требования к управлению доступом к устройствам. Эти требования рассмотрены ниже.

Защита ввода и вывода на отчуждаемый физический носитель информации:

- Система защиты должна различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (выводе на «помеченное» устройство) система защиты должна обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

- Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем системы защиты.

Сопоставление пользователя с устройством:

- Система защиты должна обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так для идентифицированных (при совпадении маркировки).

- Система защиты должна включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется с выделенным ему конкретным устройством.

Определение и классификация задач, решаемых механизмами управления доступом к ресурсам.

Понятия «владелец» и «собственник» информации.

Принципиальным моментом при исследовании проблем управления доступом к ресурсам является трактовка понятия «владельца» информации (в терминологии, применяемой при реализации механизмов управления доступом в ОС) или соответственно «собственника» информации (как увидим далее, это не одно и то же). Сформулируем эти понятия, исходя из приведенных

выше формализованных требований к механизмам защиты [16, 17], а также из принципов реализации встроенной защиты в современных универсальных ОС. При этом будем учитывать, что «владелец» файлового объекта во встроенных в ОС механизмах защиты может устанавливать и изменять атрибуты доступа, т.е. назначать и распространять ПРД.

На сегодняшний день в качестве «владельца» информации рассматривается либо пользователь, либо некое ответственное лицо. В качестве последнего, как правило, выступает сотрудник подразделения безопасности, в частности, администратор безопасности. Следует отметить, что в существующих ОС пользователь сам может устанавливать атрибуты на создаваемые им файловые объекты и не во всех случаях данные действия пользователя могут осуществляться в рамках задаваемых администратором разграничений прав доступа к ресурсам.

Таким образом, в рамках существующих ОС «владелец» объекта файловой системы – это лицо, которое может устанавливать права доступа (атрибуты) к данному файловому объекту. В общем случае, это может быть либо администратор, либо пользователь, создающий файловый объект.

Однако, права «владельца», в конечном счете, определяются тем, кто является собственником информации, т.к. именно собственник информации может принимать решение о ее передаче другим лицам. Естественно, что когда речь идет о домашнем компьютере, то собственником и «владельцем» является непосредственный хозяин компьютера, обрабатывающий на нем собственную информацию.

Другое дело – применение вычислительных средств (соответственно средств защиты) на предприятии. Использование защищаемого компьютера на предприятии, как правило, связано с защитой служебной информации, конфиденциальных данных и т.д. Но эта информация уже не является собственностью пользователя, следовательно, не пользователь должен являться ее конечным «владельцем». При этом также необходимо учитывать, что, по статистике, большинство хищений информации на предприятии (умышленно или нет) осуществляется непосредственно сотрудниками, в частности, пользователями защищаемых компьютеров. Естественно, то же (но в большей мере) относится к защите секретной информации, собственником которой является государство.

Таким образом, следует говорить о подходах к защите информации, «владельцем» которой априори не является пользователь. В частности, владельцем служебной информации является предприятие. Что касается конфиденциальной информации, то здесь все зависит от ее типа. В связи с этим большинство приложений систем защиты связано именно с защитой данных, собственником которых пользователь не является.

Следует отметить, что на практике существует некоторое противоречие в определении дискреционного управления доступом и требований, формулируемых к его реализации. Так, определение дискреционного управления доступом предполагает: «Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту». Другими словами, «владельцем» файлового объекта здесь непосредственно пользователь. Именно данная концепция принимается в качестве основы создания разграничительной политики доступа, к ресурсам в современных ОС, прежде всего, в ОС семейства Windows (само собой подразумевается, что говоря о разграничении к файловым объектам для ОС Windows, мы подразумеваем файловую систему NTFS).

Вместе с тем, возвращаясь к формализованным требованиям к дискреционному управлению (т.е. требований к системе защиты, предназначенной для обработки конфиденциальной информации) среди этих требований можем видеть:

- контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов);
- механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил или прав разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов;
- право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и т.д.);
- должны быть предусмотрены средства управления, ограничивающие распространения прав на доступ.

Другими словами, рассмотренными требованиями к дискреционному управлению доступом регламентируется, что все права по назначению и изменению ПРД предоставляются не субъектам (пользователям), а выделенному субъекту -

администратору безопасности. При этом должны быть предусмотрены средства, ограничивающие распространение прав на доступ, т.е. препятствующие передаче прав одним субъектом другому. Из данных требований вытекает, что в качестве «владельца» ресурса должен рассматриваться администратор безопасности, т.к. «владелец» имеет возможность назначить, изменить и распространить права на доступ.

Видим, что здесь вступают в противоречие концептуальные подходы к определению «владельца» информации, а как следствие и подходы к построению разграничительной политики доступа к ресурсам. В одном случае, если «владельцем» информации считать пользователя, то естественным будет предоставить ему возможность передачи прав доступа к своим ресурсам («владельцем» которых он является) другим пользователям. В другом случае, если «владельцем» информации пользователь не является (что чаще всего), то все права по назначению и распространению (переназначению) прав доступа должны принадлежать выделенным субъектам - ответственным лицам «владельца» информации, например, администраторам безопасности. В общем случае правомерен именно второй подход. Поэтому, говоря далее о дискреционном управлении доступом, будем предполагать, что назначение и изменение ПРД в системе предоставляется выделенным субъектам - администраторам безопасности. При этом модели дискреционного доступа будем рассматривать именно в данных предположениях. Соответственно, они будут отличаться от моделей, предусматривающих, что «владельцем» файлового объекта является пользователь.

С учетом сказанного можем сделать вывод о том, что в основу разграничительной политики доступа должен быть положен следующий тезис: *Пользователь не является собственником обрабатываемой им информации, как следствие, не может рассматриваться ее «владельцем», т.е. не должен иметь прав назначать и изменять ПРД к объектам файловой системы. «Владельцем» объектов файловой системы должен рассматриваться администратор безопасности, являющийся ответственным лицом собственника, в частности, предприятия.*

Корректность и полнота реализации разграничительной политики доступа.

Дальнейшее изложение материала будем проводить с учетом того, что пользователь не является «владельцем» информации, им

обрабатываемой. Для механизмов управления доступом к ресурсам данный подход связан с понятиями корректности и полноты реализации разграничительной политики доступа к ресурсам.

Под *корректностью реализации разграничительной политики* доступа к ресурсу будем понимать свойство механизма управления доступом полностью разделять ресурс между пользователями системы. При этом разграничение доступа должно быть реализовано таким образом, чтобы различные пользователи имели доступ к непересекающимся элементам разделяемого ресурса, т.е. чтобы обеспечивалась невозможность несанкционированного обмена ими информацией между собой по средством данного ресурса.

Под *полнотой реализации разграничительной политики* доступа к ресурсам будем понимать свойство системы защиты обеспечивать корректную реализацию разграничительной политики доступа ко всем ресурсам системы, посредством которых возможен несанкционированный обмен информацией пользователей между собой.

Данные определения вытекают из рассмотренных выше формализованных требований к дискреционному управлению доступом к ресурсам.

Системой защиты, используемой в автоматизированных системах обработки информации, владельцем которой не является пользователь (информация не является собственностью пользователя), должно выполняться требование к полноте реализации разграничительной политики доступа к ресурсам. Причем это требование должно выполняться по отношению к каждому защищаемому ресурсу, что в совокупности обеспечивает невозможность несанкционированного обмена информацией субъектов доступа в системе между собой.

Очевидно, что требование к полноте разграничений доступа к ресурсам может выполняться только в том случае, когда доверенным лицом владельца информации (предприятия, либо государства) выступает не пользователь, а некий субъект, внешний по отношению к информации, обрабатываемой на защищаемом компьютере. Этот субъект наделяется специальными полномочиями и обладает необходимым элементом доверия со стороны владельца информации (в частности, предприятия). Таким субъектом и является администратор безопасности.

3.3.4.2. Механизм обеспечения замкнутости программной среды

Механизм обеспечения замкнутости программной среды и его роль в системе защиты.

Под обеспечением замкнутости программной среды понимается локализация прикладных программ для пользователей. Осуществляется это механизмом управления доступом к исполняемым файлам [18].

При этом, механизм обеспечения замкнутости программной среды реализуется корректно только в том случае, если выполняются требования к полноте управления доступом к исполняемым файлам.

Проиллюстрируем сказанное примером. Например, для ОС Windows 2000/XP могут устанавливаться разграничения на исполнение файлов (запуск программ) с жесткого диска. Однако данные ОС не позволяют управлять запуском программ с внешних устройств ввода. Поэтому корректно обеспечить замкнутость программной среды, с целью локализации прикладных программ для пользователя, возможно лишь при отключении внешних устройств ввода.

Таким образом, разграничение доступа на запуск исполняемого файла и обеспечение замкнутости программной среды не одно и то же. Замкнутость программной среды реализуется посредством механизма управления доступом на запуск к исполняемым файлом, но можно говорить о его реализации в системе лишь при выполнении требований к полноте подобных разграничений.

Несмотря на то, что в современных универсальных ОС присутствует механизм управления доступом к запуску процессов, механизм обеспечения замкнутости программной среды в них не реализован. Это объясняется невыполнением требований к полноте разграничений - для ОС Windows исполняемый файл может быть запущен с внешнего устройства ввода, например, посредством флэшки. В ОС семейства UNIX невозможно установить атрибут «исполнение» на каталог (под этим атрибутом для каталога подразумевается «обзор»), т.е. невозможно запретить запуск из каталога. При этом (этот вопрос ранее рассматривался) пользователь сам может присвоить атрибут создаваемому им файлу, т.е. пользователь может записать в свой каталог исполняемый файл, установить на него для себя право исполнения, затем запустить данный файл.

Обеспечение замкнутости программной среды - это важнейший механизм противодействия организации пользователем скрытых каналов доступа к ресурсам защищаемого объекта. Целью применения механизма является предоставление пользователям возможности запускать только санкционированные программы из заданных для них списков. При этом предотвращается возможность запуска пользователем собственной программы, которая может содержать скрытый канал доступа к ресурсам. Без реализации данного механизма в системе защиты вообще не приходится говорить о какой-либо защищенности объекта [18].

В общем случае механизм обеспечения замкнутости программной среды предназначен для локализации программного обеспечения на компьютере (системного, функционального и прикладного ПО) и обеспечение невозможности запуска пользователем несанкционированного процесса (программы). Благодаря этому обеспечивается то, что пользователь может работать на компьютере только жестко в рамках своих функциональных обязанностей и инструкций, т.е. в границах списка санкционированных действий. К этой же задаче относится защита от проникновения (прежде всего из сети) и запуска на компьютере деструктивных программ (троянов, программ sniffer клавиатуры и канала, программ взлома или подбора паролей, программ перепрограммирования BIOS, инструментальных средств и т.д.).

Если вернуться к рассмотрению существующей статистики угроз (приведенной в п. 3.3.1.2), то можно сделать вывод, что подавляющая их часть требует от пользователя запуска программного средства, реализующего данные угрозы. Таким образом, путем предотвращения возможности запуска пользователем собственных программ, злоумышленник лишается собственно инструментария взлома. При этом неважно, о какой угрозе, о какой цели и способе атаки идет речь. Поэтому данный механизм позиционируется как основной механизм защиты, позволяющий противодействовать скрытым угрозам НСД к информации.

Ранее отмечалось, что защита информации - это комплексная задача, решение которой достигается реализацией совокупности механизмов защиты и что невозможно рассматривать механизм защиты в отдельности, т.к. найдутся угрозы данному механизму, которые должны предотвращаться другими механизмами. Рассмотрим иную сторону этой проблемы, когда использование в системе защиты одного механизма может принципиально изменить

требование к другим механизмам.

С учетом применения механизма обеспечения замкнутости программной среды могут существенно снижаться требования к реализации других механизмов защиты. Рассмотрим пример.

Ввиду того, что при удалении информации с диска осуществляется лишь переразметка диска, а собственно информация на нем остается, появляется скрытый канал в виде возможности несанкционированного доступа к остаточной информации на диске. Данный канал может быть устранен, если реализовать механизм гарантированного удаления информации, который будет заключаться:

1. В перехвате обращения приложения к ядру ОС «на удаление» объекта.

2. В записи в объект маскирующей информации (осуществляется N - кратная запись «О» и «I»).

3. В передаче ядру ОС запрос «на удаление» объекта.

При этом остаточной информации на диске не остается. Реализация данного механизма защиты связана с существенными потерями производительности защищаемого объекта. Остаточная информация также может оставаться в оперативной памяти после завершения процесса (если ОС или приложение не осуществляет ее очистку).

Однако, стандартным приложением прочитать остаточную информацию не представляется возможным, для этого нужны специальные программы, запуск которых на компьютере предотвращается механизмом обеспечения замкнутости программной среды. Таким образом, прочитать остаточную информацию без запуска несанкционированного процесса на защищенном компьютере становится невозможно. Остается только одна возможность ее прочтения - это удалить с компьютера жесткий диск и считать информацию с него на другом компьютере. Но если такое возможно, то оберегать уже следует не остаточную, а актуальную информацию на диске, для чего, в рассматриваемых предположениях, должны применяться криптографические методы защиты информации на диске. Сказанное в полной мере относится и к защите оперативной памяти. Вместе с тем, учитывая, что критичной ситуацией здесь является запуск несанкционированного процесса пользователем, механизм очистки памяти, конечно же, следует запускать в качестве реакции на обнаружение запущенного несанкционированного процесса. Это решает диспетчер доступа.

Существуют и иные примеры, когда использование в системе

механизма обеспечения замкнутости программной среды либо делает необязательными целый ряд других механизмов защиты, либо существенно изменяются требования к решаемым ими задачам.

Таким образом, можно сделать следующий вывод: *механизм обеспечения замкнутости программной среды - важнейший механизм, который обязательно должен присутствовать в системе защиты, т.к. этот механизм можно позиционировать, как основной механизм противодействия скрытым угрозам (возможности реализации неизвестной угрозы, присутствующей в несанкционированной пользовательской программе).*

Ввиду того, что данный механизм не имеет корректной реализации в современных ОС, его следует реализовать добавочными средствами защиты информации. В противном случае, невозможно говорить о возможности противодействия скрытым угрозам в принципе.

Механизм обеспечения замкнутости программной среды может быть реализован двумя способами:

1. В виде задания списков исполняемых файлов.
2. В виде задания каталогов исполняемых файлов.

Реализация механизма обеспечения замкнутости программной среды.

Посредством задания списков исполняемых файлов.

Данный механизм состоит в задании для каждого пользователя списка процессов (исполняемых файлов), которые ему разрешено запускать. Корректность функционирования механизма связана с предотвращением явных и скрытых каналов модификации списка санкционированных исполняемых файлов, а также запуска исполняемых файлов, не вошедших в список.

При данном подходе объект в матрице доступа к исполняемым файлам представляет собой список исполняемых файлов.

Требования к корректности функционирования механизма обеспечения замкнутости программной среды таковы [18]:

- исполняемый файл должен быть задан с указанием его полного пути, что предотвращает возможность запуска несанкционированного процесса с таким же именем из другого места. При этом пользователю должен быть запрещен запуск программ с внешних устройств ввода (локальных и общих - разделяемых в сети), а также из общих папок (разделяемых в сети файловых объектов), т.к. иначе невозможно противодействовать запуску несанкционированной

программы пользователя с полнопутьным именем легальной программы;

- пользователю должен быть задан список санкционированных для его запуска исполняемых файлов, к которым ему должен быть разрешен доступ «на исполнение». Ко всем другим файловым объектам пользователю должен быть запрещен доступ «на исполнение»;

- пользователю должен быть запрещен доступ «на запись» и «модификацию» к исполняемым файлам. В противном случае он сможет подменить санкционированный файл другого пользователя. Особенно это критично по отношению к системным процессам, поскольку нельзя допускать, чтобы пользователь мог подменить его собственным несанкционированным процессом. Из сказанного следует, что механизм обеспечения замкнутости программной среды не может быть корректно реализован без запрета доступа «на запись» и «на модификацию» к системному диску и без возможности управлять доступом на исполнение программ с устройств ввода, с разделяемых в сети ресурсов (устройств и файловых объектов).

Рассмотренный подход интуитивно понятен, но имеет существенные недостатки. Главным из них является необходимость перечислять в списках все процессы, разрешенные к запуску пользователем, в том числе и процессы, порождаемые уже разрешенными процессами. Из-за этого списки разрешенных процессов становятся очень громоздкими, существенно снижается производительность системы за счет больших затрат времени на анализ таких списков при каждом обращении к объекту файловой системы.

Сильно усложняется администрирование подобной системы защиты, так как администратору приходится составлять такие списки для каждого пользователя, а при добавлении новых программ изменять списки у каждого пользователя. Соответственно, при удалении некоторой программы приходится удалять из множества списков не только саму программу, но и все процессы, порождаемые удаляемой программой. Кроме того, возникает проблема, связанная с необходимостью введения в список разрешенных некоторому пользователю процессов отладочных и иных программ, которые необходимо запускать эксплуатационным службам при работе этого пользователя в системе. С другой стороны, необходимо исключить возможность прямого запуска этих отладочных программ несанкционированным пользователем.

Посредством каталогов исполняемых файлов.

Обеспечить замкнутость программной среды можно непосредственно заданием списков разрешенных к запуску процессов, а областью дискового пространства (каталогом), откуда пользователю можно запускать процессы. То есть пользователю можно разрешать/запрещать не что запускать, а откуда запускать. Другими словами, для каждого пользователя может быть выделен каталог, только из которого ему будет дозволено запускать программы. На этот каталог должно быть установлено право «исполнение» для пользователя. Причем в данный каталог ему должен быть запрещен доступ «на запись» и «на модификацию», с целью предотвращения возможности внесения в данный каталог других, не разрешенных к запуску программ, а также с целью предотвращения возможности модификации расположенных в каталоге программ.

При этом из всех остальных каталогов (а также с устройств ввода), кроме системного, пользователю должен быть запрещен запуск программ. Кроме того, пользователю должен быть запрещен доступ «на запись» и «на модификацию» в системный каталог. Это необходимо с целью предотвращения возможности модификации системного каталога - занесения в него несанкционированных процессов).

Список разрешенных к запуску программ (не процессов) определяется набором программ, установленных администратором безопасности в каталог, откуда пользователю разрешен их запуск [18].

Можем сформулировать следующие требования к корректности функционирования рассматриваемого механизма:

- для пользователя должен быть задан каталог, откуда ему разрешено запускать программы. На доступ к этому каталогу пользователю должно быть установлено право «исполнение», а доступ «на запись» и «на модификацию» должен быть запрещен;
- в этот выделенный каталог администратором должны быть установлены программы, разрешенные пользователю для запуска;
- ко всем остальным каталогам, а также к устройствам (дисководу, CD-ROM и т.д.), разделяемым сетевым ресурсам пользователю должен быть запрещен доступ «исполнение»;
- к системному диску, а также к каталогам с исполняемыми файлами остальных пользователей, пользователю должен быть запрещен доступ «на запись» и «на модификацию».

Достоинством рассмотренного здесь механизма является серьезное упрощение его администрирования, т.к. исключается необходимость перечисления всех процессов, которые запускает программа, при разрешении ее запуска пользователем (при установке и удалении программы из списка разрешенных к запуску). Кроме того, в предыдущей реализации механизма обеспечения замкнутости программной среды необходимость подобного перечисления могла привести к тупикам. Например, программе для работы может потребоваться некоторый процесс, а разрешать запускать этот процесс пользователю нельзя.

Расширение возможностей механизма обеспечения замкнутости программной среды.

Расширение возможностей механизма защиты обеспечения замкнутости программной среды состоит в том, чтобы и в качестве субъекта доступа, и в качестве объекта доступа рассматривать «процесс». В этом случае можно разграничивать права доступа для процессов на запуск процессов, т.е. можно обеспечивать замкнутость программной среды не на уровне списков санкционированных процессов (разрешения запуска пользователем отдельных программ), а уже на уровне последовательностей запуска процессов (технологий обработки данных). Другими словами, можно задавать последовательности обработки - каким процессом какой процесс может быть запущен.

3.3.4.3. Оценка влияния системы защиты на загрузку вычислительного ресурса информационной системы

В общем случае, следует различать два вида субъекта доступа к ресурсам – «пользователь» и «процесс». Поэтому в общем случае диспетчером доступа по отношению к объектам должны реализовываться следующие возможности [18]:

- разграничение прав доступа к объектам процессов вне разграничений пользователей;
- разграничение прав доступа к объектам пользователей вне разграничений процессов;
- комбинированное разграничение прав доступа – разграничение прав доступа к объектам процессов в рамках разграничений пользователей (совместное разграничение доступа процессов и пользователей).

Субъект доступа «процесс» является вторичным по

отношению к субъекту доступа «пользователь». В отличие от субъекта «пользователь» он может либо присутствовать, либо отсутствовать в схеме разграничения прав доступа.

Проведем оценку, в какой мере влияет на загрузку вычислительного ресурса защищаемого объекта включение в схему управления доступом дополнительного субъекта доступа «процесс». Для этого следует построить следующие математические модели:

- математическую модель рабочей станции без системы защиты;
- математическую модель рабочей станции с реализацией управления доступом к файловым объектам для субъекта доступа «пользователь»;
- математическую модель рабочей станции с реализацией управления доступом к файловым объектам для субъектов доступа «пользователь» и «процесс».

Будем строить математическую модель функционального объекта, где элементы модели в общем случае отображают не структурные элементы физического объекта (что, естественно, является менее корректным решением задачи, с точки зрения подходов к математическому моделированию), а функциональные взаимодействия, что более наглядно иллюстрирует получаемый результат (и, что нетрудно подтвердить, приводит к незначительной погрешности в результатах).

Модель рабочей станции без системы защиты.

Общие положения.

Для построения модели необходимо решить, на какой круг задач будет рассчитана вычислительная система. Будем рассматривать типовые задачи, с которыми чаще всего приходится сталкиваться в современных вычислительных системах общего назначения. Задачи гипотетической вычислительной системы, модель которой требуется построить, ограничим следующим списком:

1. Обработка текстов. Редактирование и верстка.
2. Математическая обработка данных.
3. Разработка программ. Редактирование и сборка.

В качестве типовых приложений, реализующих вышеперечисленные задачи, рассмотрены следующие программы:

- текстовый редактор — MS Word 2007;
- текстовый компилятор — MikTeX 2.2;
- электронные таблицы — MS Excel 2007;
- разработка программ — MS Visual C++ 9.0.

Основные параметры (число операций счета, количества обращений к внешним устройствам и т.п.) этих программ определяются экспериментально, т.е. определяются параметры приложений, полученных в результате серии экспериментов и последующих расчетов с использованием моделей. Параметры приложений приведены в таблице 3.18.

Таблица 3.18

Параметры приложений

Параметр	MS Word 2007	MS MikTeX 2.2	MS Excel 2007	MS Visual C++ 9.0
Количество обращений к ФС, n_2	4725	9375	2631	63125
Среднее время выполнения запросов к ФС, u_2 , мкс	190	475	425	534
Количество обращений к реестру ОС, n_3	4548	1064	2176	17542
Среднее время выполнения запросов к реестру, u_3 , мкс	611	500	130	741
Среднее время выполнения, U_c	5,7	55	5,77	59
Интенсивность потока заявок, λ_0 , 1/с	0,2	0,125	1,2	0,04
Загрузка процессора, Q , %	62	93	22	60
Количество этапов счета, $N=n_2+n_3+1$	9274	10440	4808	80668

Общий вид сетевой модели рабочей станции без системы защиты.

Математическая модель вычислительной системы (рабочей станции) без системы защиты представляет собой разомкнутую сеть массового обслуживания (СМО). Эта СМО состоит из трех узлов, в

свою очередь представляющих собой отдельные системы массового обслуживания (СМО):

- система массового обслуживания «процессор - оперативная память»;
- система массового обслуживания «файловая система»;
- система массового обслуживания «Реестр».

В качестве входного потока прием стационарный пуассоновский поток.

Стационарный пуассоновский поток является простейшим потоком, а для простейшего потока характерно, что поступление заявки через короткий промежуток времени более вероятно, чем через длинный промежуток времени.

Следствием этого свойства является то, что простейший поток создает наиболее тяжелый режим работы для системы [18]. Поэтому простейший поток в моделях позволяет получать предельные значения входных характеристик, и, следовательно, если входной поток в реальной системе отличен от простейшего, то система будет иметь характеристики функционирования, по крайней мере, не хуже, чем при простейшем входном потоке.

Интенсивность входного потока определена экспериментально. Для задания характеристики среднего времени обслуживания в каждом узле сети массового обслуживания рассмотрим эти СМО по отдельности.

Система массового обслуживания «файловая система».

Параметры этой СМО определяются с помощью экспериментальных данных. Для определения закона распределения длительности обслуживания надо построить гистограммы распределения значений длительностей обслуживания для каждого приложения. Все эти гистограммы имеют практически одинаковый вид, причем получаемые распределения при моделировании СМО «файловая система» при определенных оговорках подчиняется экспоненциальному закону [18].

Для определения среднего времени обслуживания в СМО «файловая система» (b) можно использовать следующие соотношение: $u = b / (1 - p)$, соответственно $p = \lambda \cdot b = \alpha \cdot \lambda_0 \cdot b$, тогда получаем:

$$b = u / (1 - \alpha \cdot \lambda_0 \cdot b), \quad (3.42)$$

где α – коэффициент передачи в соответствующий узел СеМО);

λ_0 - интенсивность потока заявок на входе СеМО;

u – среднее время пребывания заявки в СеМО.

Система массового обслуживания «Реестр».

Параметры этой СМО также определяются экспериментально.

Гистограмма распределения длительности обслуживания для всех приложений имеет вид, очень похожий на предыдущую гистограмму. Поэтому, следуя заключениям, сделанным для СМО «файловая система», будем также считать, что распределение длительности обслуживания в СМО «реестр» подчиняется экспоненциальному закону.

Среднее время обслуживания в СМО «реестр» определялось по результатам экспериментов, с использованием соотношения (3.42), и определяется для каждого приложения в отдельности.

Система массового обслуживания «процессор - оперативная память».

Рассмотрим СМО «процессор - оперативная память». Данных, указывающих на закон распределения времени обслуживания в СМО «процессор — оперативная память» нет. Для упрощения расчета модели и по аналогии с рассмотренными ранее СМО предположим что распределение длительности обслуживания в СМО «процессор — оперативная память» подчиняется экспоненциальному закону.

Для определения средней длительности обслуживания будем использовать формулу (3.42) и следующее соотношение $U = Nu_1 + n_2u_2 + n_3u_3$, откуда получим

$$u_1 = (U - n_2u_2 - n_3u_3) / N, \quad (3.43)$$

где u_1 - среднее время пребывания в СМО «процессор - оперативная память»;

u_2 - среднее время пребывания в СМО «файловая система»;

u_3 - среднее время пребывания в СМО «реестр»;

n_2 - количество обращений к файловой системе;

n_3 - количество обращений к реестру;

N – количество этапов счета;

U – среднее время пребывания в СеМО.

В результате, по формуле (3.42) и параметрам приложений, полученных в результате серии экспериментов и последующих расчетов с использованием моделей, определяется для каждого приложения среднее время обслуживания в узлах модели.

Сетевая модель рабочей станции без системы защиты.

Теперь перейдем к рассмотрению сети массового обслуживания (СеМО). Обозначим СМО «процессор — оперативная память» через S1, СМО «файловая система» через S2, а СМО «реестр» через S3. Введем также узел S0, через который в систему поступают заявки на обслуживание. Граф передач такой сети представлен на рис. 3.17.

Соответствующая этому графу матрица вероятностей передач выглядит следующим образом:

$$P = \begin{vmatrix} 0 & 1 & 0 & 0 \\ P10 & 0 & P12 & P13 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix} \quad (3.44)$$

Используя эту матрицу, получаем систему уравнений, связывающую между собой интенсивности потоков в узлах СеМО и вероятности передач:

$$\begin{cases} -\lambda_0 + P10 \cdot \lambda_1 = 0 \\ \lambda_0 - \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ P12 \cdot \lambda_1 - \lambda_2 = 0 \\ P13 \cdot \lambda_1 - \lambda_3 = 0 \end{cases} \quad (3.45)$$

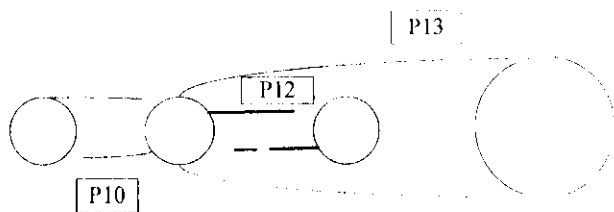


Рис. 3.17. Граф передач СеМО для сетевой модели без системы защиты

Решая эту систему уравнений, получаем выражения для определения коэффициентов передач:

$$\alpha_j = \lambda_j / \lambda_0; \alpha_1 = 1 / P10; \alpha_2 = P12 / P10; \alpha_3 = P13 / P10, \quad (3.46)$$

где: j – номер СМО.

Для нахождения с помощью таких выражений численного значения коэффициентов передач необходимо определить вероятности перехода заявки из одного узла СЕМО в другой.

Очевидно, что $P_{10i} = 1 / N_i$, откуда: $\alpha_{1i} = N_i$,

где N_i – количество этапов счета для i -го типа приложения (в нашем случае $i = 5$).

Вероятность перехода заявки в СМО «файловая система» есть отношение количества обращений к файловой системе к количеству этапов счета, то есть: $P_{12i} = n_{2i} / N_i$, откуда

$$\alpha_{2i} = (n_{2i} / N_i) \cdot N_i = n_{2i}, \quad (3.47)$$

где n_{2i} – количество обращений к файловой системе;

N_i – количество этапов счета;

i – тип приложения.

Расчет характеристик сети далее будет производиться, исходя из условия, что сеть работает в стационарном режиме, то есть вероятностные характеристики сети не зависят от времени. Условие существования стационарного режима в сети определяется существованием стационарного режима во всех узлах этой сети.

Стационарный режим существует в отдельной СМО с одним обслуживающим прибором, если выполняется следующее условие: $\lambda = 1/b$, то есть, если загрузка прибора меньше единицы.

Исходя из этого, можно сформулировать условие существования стационарного режима в рассматриваемой сети:

$$\lambda_0 < \min \left\{ \frac{1}{\alpha_1 b_1}; \frac{1}{\alpha_2 b_2}; \frac{1}{\alpha_3 b_3} \right\}. \quad (3.48)$$

Этим (3.48) надо руководствоваться при выборе максимальной интенсивности входного потока заявок каждого типа в ходе расчета характеристик сети.

Самой важной характеристикой сети для нас является время пребывания заявки в сети, которое определяется по выражению:

$$U = \sum_{i=1}^M \alpha_i u_i, \quad (3.49)$$

де $u_i = b_i / (1 - \rho_i)$; M – число СМО в сети.

Так как $\rho_i = \alpha_i b_i = \alpha_i \lambda_0 b_i$, то выражение (3.49) можно записать в следующем виде:

$$U = \sum_{i=1}^M \alpha_i b_i / (1 - \alpha_i \lambda_0 b_i). \quad (3.50)$$

Модель рабочей станции с системой защиты.

Под системой защиты в данном случае подразумевается система разграничения прав доступа к ресурсам файловой системы и реестра, с учетом «процесса» как самостоятельного субъекта доступа.

Из блок-схемы алгоритма управления доступом с учетом субъекта доступа «процесс», среднюю трудоемкость T алгоритма анализа запроса доступа к ресурсу можно выразить следующим образом:

$$T = (P1+P2)x+2P2x, \quad (3.51)$$

где x - трудоемкость проверки прав доступа;

$P1$ - вероятность поступления запроса от процесса, не упомянутого в разграничениях прав доступа;

$P2$ - вероятность поступления запроса от процесса, имеющего совместный (вместе с субъектом «пользователь») режим проверки прав доступа;

$P3$ - вероятность поступления запроса от процесса, имеющего эксклюзивный режим проверки прав доступа.

Исследование средств добавочной защиты для ОС семейства Windows показало, что вероятность поступления запроса от привилегированного процесса составляет порядка 0,3, процесса с совместным режимом проверки запроса порядка 0,1.

Поэтому для дальнейших расчетов примем среднее время проверки запроса с учетом субъекта «процесс», как самостоятельного субъекта доступа, равным $((1-0,3-0,1) + +0,3)x + 2 \cdot 0,1x = 1,1x$.

Из всех типов запросов, обращающихся к файловой системе и реестру, проверке (анализу прав доступа) подлежит лишь некоторая часть. Очевидно, что бессмысленно проверять, например, операцию закрытия файла или операцию сброса буферов ввода-вывода. Эксперименты показывают [18], что контролировать целесообразно 90 % запросов (в общем потоке) к ресурсам реестра и 35 % запросов к файловой системе. Экспериментально было определено время, требуемое на проведение проверки (контроля прав доступа) для

одного запроса [18]. В среднем, это время составляет 130 мкс. Исходя из вышеизложенного, для дальнейших расчетов примем следующее выражение для определения суммарного среднего времени обслуживания в системах массового обслуживания:

$$b_4 = 130 \times (0,9 + 0,340)/2. \quad (3.52)$$

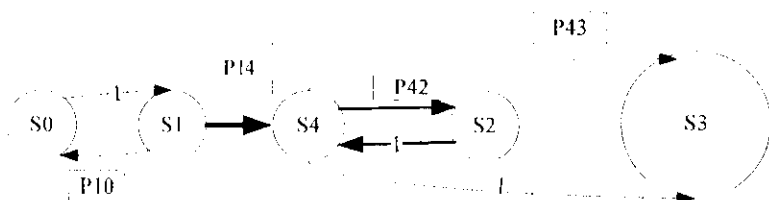


Рис. 3.18. Граф передач СеМО для сетевой модели с системой защиты

Модель рабочей станции с системой защиты представляет собой разомкнутую сеть массового обслуживания (СеМО). По сравнению с рассматриваемой ранее моделью без системы защиты (рис. 3.17), в этой СеМО появилась новая система массового обслуживания – СМО «система защиты». Граф передач такой сети представлен на рис. 3.18.

Соответствующая этому графу матрица вероятностей передач будет следующая:

$$P = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 \\ P10 & 0 & 0 & 0 & P14 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & P42 & P43 & 0 \end{vmatrix} \quad (3.53)$$

Используя эту матрицу, получаем систему уравнений, связывающую между собой интенсивности потоков в узлах СеМО и вероятности передач:

$$\begin{cases} -\lambda_0 + P10 \cdot \lambda_1 = 0 \\ \lambda_0 - \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ P42 \cdot \lambda_4 - \lambda_2 = 0 \\ P43 \cdot \lambda_4 - \lambda_3 = 0 \\ P14 \cdot \lambda_1 - \lambda_4 = 0 \end{cases} \quad (3.54)$$

Решая эту систему уравнений, получаем выражение для определения коэффициентов передач:

$$\alpha_i = \lambda_i / \lambda_0, \quad (3.55)$$

где $i = 1 \dots 4$ – номер СМО, тогда:

$$\alpha_1 = 1/P10; \alpha_4 = P14/P10; \alpha_2 = P42/P10; \alpha_3 = P43/P10 \quad (3.56)$$

Для нахождения с помощью данных выражений численных значений коэффициентов передач, необходимо определить вероятности перехода заявки из одного узла СеМО в другой. Очевидно, что: $P10i = 1/Ni$, откуда $\alpha_{1i} = Ni$, где: Ni – количество этапов счета; $i = 1 \dots I$ – тип приложения (у нас $I=5$).

Исходя из этого, и так как: $P14 = 1 - P10 = 1 - 1/Ni$, тогда получим: $\alpha_{4i} = Ni - 1$.

Вероятность перехода заявки в СМО «файловая система» - это есть отношение количества обращений к файловой системе к количеству этапов счета, то есть: $P42i = n_{2i}/Ni$, откуда

$$\alpha_{2i} = n_{2i}/Ni \cdot Ni = n_{2i}, \quad (3.57)$$

где n_{2i} – количество обращений к файловой системе;

Ni – количество этапов счета;

$i = 1 \dots I$ – тип приложения (у нас $I=5$).

Аналогично, определяется вероятность перехода заявки в СМО «реестр»: $P32i = n_{3i}/Ni$, откуда:

$$\alpha_{3i} = n_{3i}/Ni \cdot Ni = n_{3i}, \quad (3.58)$$

где n_{3i} – количество обращений к файловой системе;

Ni – количество этапов счета;

$i = 1 \dots I$ – тип приложения (у нас $I=5$).

Тогда, принимая во внимание все сказанное выше, получаем для проведения дальнейших расчетов следующее выражение,

позволяющее определять среднее время обслуживания в СМО «система защиты»:

$$b_4 = 180 \cdot (0,9 \cdot n_{3i} / Ni + 0,34 \cdot n_{2i} / Ni) / 2. \quad (3.59)$$

Таким образом, можно сделать вывод, что влияние на загрузку вычислительной системы при реализации механизма управления доступом к ресурсам пропорционально количеству решаемых задач и обратно пропорционально трудоемкости задачи. Поэтому наибольшее влияние в данном случае оказывается при загрузке системы задачами с низкой трудоемкостью этапа счета и большим количеством обращений к ресурсам при выполнении задачи.

Анализ эффективности механизма управления доступом.

Были рассмотрены три модели:

1. Модель без системы защиты;
2. Модель с управлением доступом к ресурсам для субъекта доступа «пользователь»;
3. Модель с управлением доступом к ресурсам для субъектов доступа «пользователь» и «процесс».

Характеристика времени пребывания заявки в системе для рассматриваемых типовых приложений, получаемая подстановкой экспериментально измеренных данных в приведенные выражения, позволяет сделать следующие выводы [18]:

1. Эффективность использования вычислительного ресурса при реализации механизма управления доступом незначительно зависит от используемых приложений (типа используемого приложения);

2. Дополнительное повышение загрузки вычислительного ресурса системы, вызванное использованием в схеме управления доступом к ресурсам дополнительного субъекта «процесс», составляет единицы и доли единицы процентов, что является весьма низкой ценой за совокупность принципиально новых свойств защиты, обеспечиваемых при использовании в схеме управления доступом к ресурсам субъекта доступа «процесс»;

3. Влияние на загрузку вычислительной системы при реализации механизма управления доступом к ресурсам пропорционально количеству решаемых задач и обратно пропорционально трудоемкости задачи. Поэтому наибольшее влияние в данном случае оказывается при загрузке системы задачами с низкой трудоемкостью этапа счета и большим количеством обращений к ресурсам при выполнении задачи.

3.3.4.4. Особенности реализации механизмов добавочной защиты

Организация добавочной защиты операционной системы.

Механизм управления доступом к ресурсам (диспетчер доступа) должен выполняться в виде системного драйвера и функционально располагаться между приложением и ядром ОС. Это вызвано следующим [18]. На уровне приложения невозможно осуществить разграничительную политику доступа в принципе. Здесь можно только регистрировать факт уже свершившегося события и осуществлять противодействие, если событие несанкционированное. Реализация диспетчера на уровне ядра, во-первых, практически невозможна для коммерческих систем (без наличия исходных текстов), а во-вторых, может быть связана с нарушением лицензионных соглашений разработчика.

Любой запрос на доступ к ресурсам от приложения к ядру перехватывается диспетчером доступа и анализируется в соответствии с заданными правами доступа к объектам от субъектов. В случае противоречия запрашиваемого доступа разграничительной политике, он отвергается диспетчером, в противном случае доступ к ресурсу разрешается - транслируется в ядро ОС.

При наличии в системе встроенного диспетчера доступа механизм добавочной защиты должен располагаться перед ним и первым анализировать запрос. Это вызвано необходимостью реализации перенаправления запросов при доступе к общим каталогам («Корзина» и т.д.). Т.е. обработка запроса на доступ к ресурсам в этом случае должна осуществляться по схеме, приведенной на рис.3.18.

Особенностью реализации механизма управления доступом (диспетчера доступа) к ресурсам добавочной защиты является то, что он полностью должен быть развязан с соответствующим механизмом встроенной защиты. В частности, не должен использоваться механизм хранения атрибутов доступа файловой системой (например, NTFS). В противном случае, настройки механизма добавочной защиты могут быть изменены средствами настройки встроенного механизма защиты. Кроме того, в этом случае невозможно говорить о резервировании механизмов защиты.

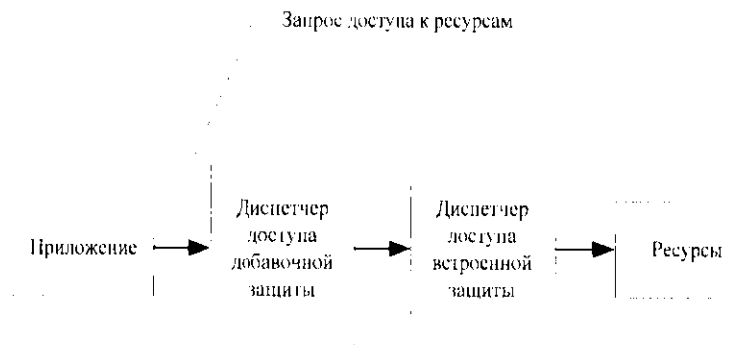


Рис.3.19. Схема обработки запроса доступа к ресурсам

Остается единственный способ хранения прав доступа к ресурсам - матрицы доступа (либо соответственно, меток конфиденциальности). Этот способ предусматривает хранение прав доступа в файле (либо в реестре), доступ к которому также соответствующим образом разграничивается. Кстати говоря, реализация данного подхода позволяет строить диспетчер доступа с едиными принципами построения для различных типов файловых систем и для различных видов ресурсов. Принципиальным отличием хранения матрицы доступа в файле является то, что на производительности системы сказывается величина таблицы прав разграничения доступа, анализируемой при каждом доступе к ресурсам.

Пути уменьшения потерь производительности вычислительной системы из-за средств защиты.

Так как длину списка в 100 строк в общем случае нельзя считать достаточной для задания правил разграничения доступа (в реальных системах длина списка прав разграничения доступа может достигать 150...200 строк), то рассмотрим некоторые пути уменьшения потерь из-за средств защиты. Ясно, что бороться с потерями от введения средств добавочной защиты можно следующими путями:

- путем уменьшения списка правил разграничения доступа;
- путем уменьшением времени проверки одного запроса;
- сразу обоими методами.

Первый способ интуитивно очевиден: сократить длину имени ресурса (т.е. среднюю длину строки в списке правил разграничения доступа). Например, ресурсы файловой системы, доступ к которым подлежит разграничению, следует располагать как можно ближе к корневому каталогу. Это естественно уменьшит длину полного имени ресурса, т.е. длину строки в списке.

Недостатком данного подхода является то, что, во-первых, данное ограничение (по-сути, разграничение доступа к каталогам) не всегда выполнимо в реальной системе, во-вторых, такой способ мало применим для остальных ресурсов вычислительной системы, например реестра или сетевых ресурсов, так как в этом случае администратор безопасности не может изменять полные имена ресурсов.

Второй способ состоит в использовании масок Маска - это регулярное выражение, содержащее метасимволы «*», «?» и т.п., покрывающие несколько имен ресурсов сразу. Таким образом, вместо внесения некоторого количества очень похожих имен ресурсов в списки правил разграничения доступа вносится только одна маска, содержащая общую часть имен этих ресурсов и метасимволы, задающие правила последующего сравнения маски и имен ресурсов [18].

При использовании механизма масок в ОС семейства MS Windows есть своя особенность. Для таких ОС характерно, что имена файловых ресурсов не подходящие под формат «8.3» (так называемые, «длинные имена») имеют фактически два имени - длинное и короткое в формате «8.3». Это вынуждает либо вносить в списки правил разграничения доступа оба имени, либо использовать в качестве имен ресурсов в этих списках маски.

Так например, в ОС MS Windows 2000/XP, в случае, если длинное имя, содержащее символы, не входящие в латинский алфавит, располагается на файловой системе NTFS, короткое имя формируется с использованием четырехзначного шестнадцатеричного числа, вместо части пути, содержащего символы, не входящие в латинский алфавит. То есть, короткое имя в таких условиях будет выглядеть так: C:\Progra~1\C6F5~1\abc.

Понятно, что попытка покрытия этих двух имен (длинного и короткого) простой маской обречена на неудачу, так как часть пути к ресурсу, содержащего символы, не входящие в латинский алфавит, выглядит различно в длинном и коротком имени (не имеет ни одного общего символа). Требуемую маску создать можно, но помимо

упомянутых имен такая маска обязательно покрывает еще некоторые имена ресурсов.

Подобная ситуация исправляется в случае применения более сложных регулярных выражений для масок. Однако очевидно, что проще организовывать структуру файловой системы NTFS, избегая использования длинных имен, содержащих символы, не входящие в латинский алфавит (что под силу администратору безопасности при настройке системы защиты).

Таким образом, уменьшение времени проверки одного запроса достигается применением усовершенствованного алгоритма сравнения строк. Кроме того, можно использовать различные математические методы ускорения поиска (организация списков прав разграничения доступа в виде сбалансированных деревьев и т.п.).

3.4. Криптографические методы защиты информации в информационных системах

3.4.1. Симметричное шифрование

Процесс симметричного шифрования заключается в следующем [19]: исходное осмысленное сообщение, обычно называемое *открытым текстом*, преобразуется в бессмысленную на вид последовательность символов, называемую *шифрованным текстом*. Процесс шифрования состоит в использовании алгоритма и некоторого ключа. Ключ - это значение, не зависящее от открытого текста. Результат, достигаемый при выполнении алгоритма, зависит от применяемого при этом ключа. Изменение ключа приводит к изменению результата выполнения алгоритма.

Полученный шифрованный текст можно пересылать получателю. После получения шифрованного текста адресатом текст можно снова преобразовать в открытый с помощью соответствующего алгоритма дешифрования и того же ключа, который применялся при шифровании.

Надежность симметричного шифрования зависит от нескольких факторов. Во-первых, алгоритм шифрования должен быть достаточно сложным, чтобы невозможно было расшифровать сообщение при наличии только шифрованного текста. Во-вторых, основным фактором надежности традиционного шифрования является секретность ключа, в то время как сам алгоритм может быть и несекретным. Поэтому предполагается, что должна быть

обеспечена практическая невозможность расшифровки сообщения на основе знания шифрованного текста, *даже если* известен алгоритм шифрования/дешифрования. Другими словами, не требуется обеспечивать секретность алгоритма - достаточно обеспечить секретность ключа.

Именно эта особенность схемы симметричного шифрования обуславливает ее широкую популярность и признание. Отсутствие необходимости хранить в секрете алгоритм дает производителям возможность реализовать алгоритмы шифрования данных в виде дешевых общедоступных микросхем, которыми оснащены сегодня многие современные системы. При использовании симметричного шифрования основная проблема обеспечения безопасности заключается в надежном сохранении секретности ключа.

Основные элементы схемы симметричного шифрования: источник создает сообщение в форме открытого текста $X = [X_1, X_2, \dots, X_M]$. Элементами X_i открытого текста X являются символы некоторого конечного алфавита. Традиционно использовался алфавит, состоящий из 26 прописных букв английского языка, но сегодня чаще применяется двоичный алфавит $\{0, 1\}$. Для шифрования генерируется ключ в форме $K = [K_1, K_2, \dots, K_J]$. Если ключ генерируется там же, где и само сообщение, то ключ тоже необходимо переправить получателю сообщения по каким-то секретным каналам. Другим решением может быть создание ключа третьей стороной, которая должна защищенным способом обеспечить доставку ключа как отправителю, так и получателю сообщения.

При наличии в качестве исходных данных сообщения X и ключа шифрования K с помощью алгоритма шифрования формируется шифрованный текст $Y = [Y_1, Y_2, \dots, Y_M]$. Это можно записать в виде формулы $Y = E_K(X)$.

Данная нотация означает, что Y получается путем применения алгоритма шифрования E к открытому тексту X при использовании ключа K .

Предполагаемый получатель сообщения, располагая ключом K , должен иметь возможность выполнить обратное преобразование $X = D_K(Y)$.

Противник, обладающий возможностью ознакомиться с Y , но не имеющий доступа ни к K , ни к X , может попытаться восстановить X или K или сразу оба эти объекта. При этом подразумевается, что противник знает и алгоритм шифрования (E), и алгоритм дешифрования (D). Если противник заинтересован распознать только

одно конкретное сообщение, ему следует сосредоточить свои усилия на восстановлении X путем построения вероятно соответствующего исходному открытого текста X . Однако чаще противник бывает заинтересован в получении возможности читать и все последующие сообщения. В этом случае его основные усилия должны быть сосредоточены на восстановлении K путем построения вероятно соответствующего исходному ключа K .

Классификация криптографических систем в общем случае строится на основе следующих трех независимых характеристик:

1. *Тип операций по преобразованию открытого текста в шифрованный.* Все алгоритмы шифрования основываются на использовании двух операций: *замены*, означающей замещение каждого элемента открытого текста (бита, буквы, группы битов или группы букв) некоторым другим элементом, и *перестановки*, означающей изменение порядка следования элементов открытого текста. При этом главным требованием оказывается отсутствие потерь информации (т.е. обратимость всех операций). В большинстве реальных систем шифрования применяют не одну, а комбинацию нескольких операций замены и перестановки. Соответствующие шифры называются продукционными.

2. *Число применяемых ключей.* Если и отправитель, и получатель используют один и тот же ключ, система называется симметричной, системой с одним ключом, системой с секретным ключом или схемой симметричного шифрования. Если отправитель и получатель используют разные ключи, система называется асимметричной, системой с двумя ключами или схемой шифрования с открытым ключом.

3. *Метод обработки открытого текста.* *Блочное шифрование* предполагает обработку открытого текста блоками, так что в результате обработки каждого блока получается блок шифрованного текста. *Поточное шифрование* подразумевает шифрование всех элементов открытого текста последовательно, одного за другим, в результате чего на каждом этапе получается по одному элементу шифрованного текста.

Рассмотрим семейство наиболее широко используемых алгоритмов шифрования, получивших название DES (Data Encryption Standard - стандарт шифрования данных).

В сравнении со схемами на основе открытого ключа, например в сравнении с RSA, структура DES, равно как и большинства других алгоритмов симметричной схемы, очень сложна

и поэтому не может быть описана так просто, как структура RSA и ему подобных алгоритмов. Ввиду этого сначала рассмотрим упрощенную версию DES.

Упрощенный DES.

Упрощенный DES - это алгоритм шифрования, имеющий, скорее, учебное, чем практическое значение. По свойствам и структуре он подобен DES, но имеет гораздо меньше параметров. Данный алгоритм был разработан профессором Эдвардом Шейфером (Edward Schaefer) из Университета Санта-Клара [19].

Общие сведения.

На рис.3.20 показана общая структура упрощенного алгоритма DES, который называют еще S-DES. Данный алгоритм получает на входе 8-битовый блок открытого текста (например, 10111101) и 10-битовый ключ, а на выходе генерируется 8-битовый блок шифрованного текста. Алгоритм дешифрования S-DES в качестве исходных данных использует 8-битовый блок шифрованного текста и тот же 10-битовый ключ, который применялся для шифрования, а в результате работы алгоритм дешифрования должен генерировать 8-битовый блок открытого текста.

Алгоритм шифрования включает последовательное выполнение пяти операций: начальной перестановки IP , сложной функции f_k , являющейся композицией операций перестановки и подстановки и зависящей от полученного ключа, перестановки SW , при которой две половинки последовательности данных просто меняются местами, еще раз функции f_k , и, наконец, перестановки, обратной начальной (IP^{-1}). Очевидно, что использование нескольких последовательных перестановок и подстановок приводит к получению алгоритма, значительно более сложного для криптоанализа.

Функция f_k использует в качестве исходных данных не только шифруемый текст, но и 8-битовый ключ. Алгоритм можно построить так, чтобы он работал с 16-битовым ключом, состоящим из двух 8-битовых подключей, применяемых по отдельности каждый для своего вызова функции f_k . Можно использовать и 8-битовый ключ, для чего просто следует ввести его дважды. Наконец, можно прибегнуть к комбинированному решению, когда требуется 10-битовый ключ, из которого генерируются два 8-битовых, как показано на рис.3.20. В этом случае ключ сначала преобразуется путем перестановки (P_{10}).

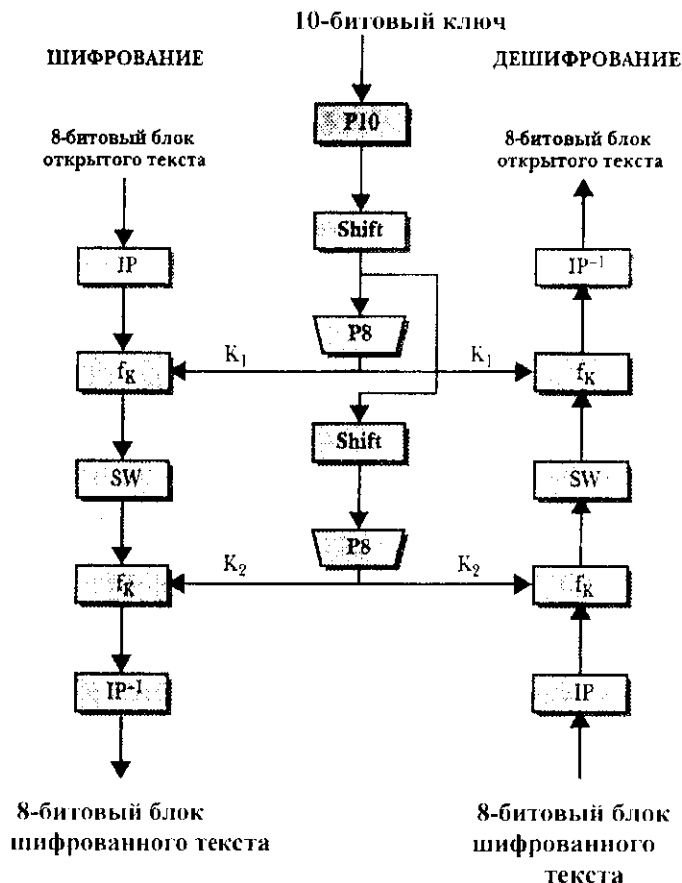


Рис. 3.20. Схема упрощенного алгоритма DES

После этого применяется операция сдвига, а полученные в ее результате данные поступают на вход перестановки (P8), которая генерирует первый 8-битовый подключ (K_1). Те же полученные в результате операции сдвига данные поступают на вход другой операции сдвига и другой функции перестановки (P8), в результате чего генерируется второй подключ (K_2).

Разберем элементы алгоритма S-DES более подробно.

Вычисление ключей S-DES.

В алгоритме S-DES используется 10-битовый ключ, который должен быть как у отправителя, так и у получателя сообщения. Из этого ключа на определенных этапах шифрования и дешифрования

генерируется два 8- битовых подключа. На рис.3.21 показана схема процедуры создания этих подключей. Сначала выполняется перестановка битов ключа следующим образом. Если 10-битовый ключ представить в виде $(k_1, k_2, \dots, k_{10})$, то перестановку P10 можно задать формулой $P10(k_1, k_2, \dots, k_{10}) = (k_5, k_2, k_9, k_1, \dots, k_{10})$, где каждый элемент идентифицирует позицию бита исходных данных в генерируемой выходной последовательности.

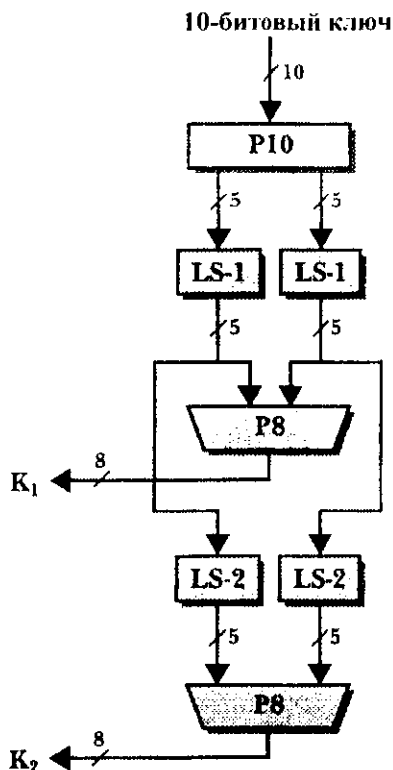


Рис.3.21. Вычисление ключей S-DES

Затем применяется перестановка P8, в результате которой из 10-битового ключа сначала выбираются, а затем переставляются 8 битов по определенному правилу. В результате этой операции получается первый подключа (K_1).

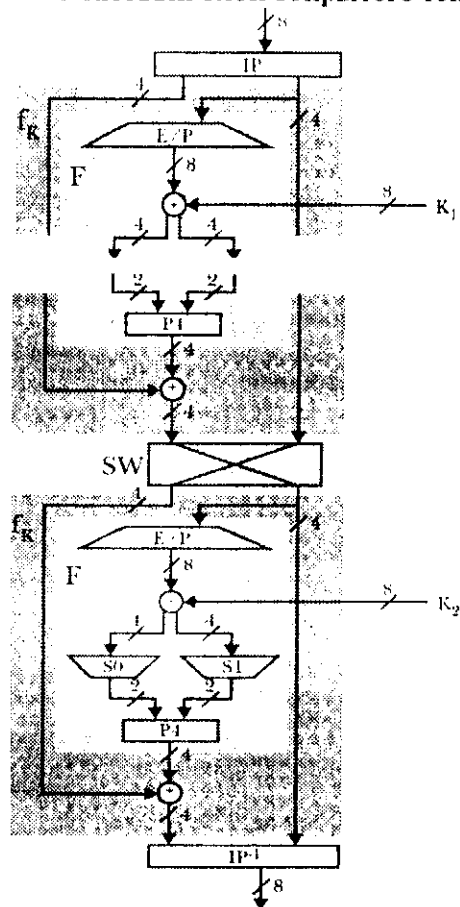
Теперь нужно вернуться к двум 5-битовым строкам, полученным в результате применения функций LS-1, и выполнить с 268

каждой из этих строк циклический сдвиг влево на две позиции (LS-2).
Наконец, применив к полученной в результате последовательности перестановку P8, получим подключ K_2 .

Шифрование S-DES.

На рис. 3.22 представлена более подробная схема.

8-битовый блок открытого текста



8-битовый блок шифрованного текста

Рис. 3.22. Подробная схема шифрования S-DES

алгоритма шифрования S-DES. Как уже упоминалось, процесс шифрования представляет собой последовательное выполнение пяти операций, которые мы рассмотрим здесь каждую в отдельности.

Начальная и завершающая перестановки.

На вход алгоритма поступает 8-битовый блок открытого текста, к которому применяется начальная перестановка, заданная функцией IP. Все 8 битов открытого текста сохраняют свои значения, но меняется порядок их следования. На завершающей стадии алгоритма выполняется обратная перестановка.

Функция f_k .

Самым сложным компонентом S-DES является функция f_k , представляющая собой комбинацию перестановки и подстановки. Пусть L и R означают соответственно первые 4 бита и последние 4 бита 8-битовой последовательности, подаваемой на вход f_k , и пусть F - некоторое отображение пространства 4-битовых строк в себя, не обязательно являющееся взаимно однозначным. Тогда положим

$$f_k(L, R) = (L \oplus F(R, SK), R),$$

где SK обозначает подключ, а $\oplus$ - операцию XOR (побитовое исключающее "ИЛИ").

Теперь опишем отображение F . На входе этого отображения имеем 4-битовое значение $(n_1 \ n_2 \ n_3 \ n_4)$. Первой операцией является операция расширения/перестановки, то есть 4-битовое значение $(n_1 \ n_2 \ n_3 \ n_4)$ удваивается.

Для дальнейшего рассмотрения удобнее представить результат в следующей форме:

$$\begin{array}{cc|cc} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{array}$$

К этому значению с помощью операции XOR добавляется 8-битовый подключ $K_1 = (k_{11}, k_{12}, \dots, k_{18})$:

$$\begin{array}{cc|cc} n_4+k_{11} & n_1+k_{12} & n_2+k_{13} & n_3+k_{14} \\ n_2+k_{15} & n_3+k_{16} & n_4+k_{17} & n_1+k_{18} \end{array}$$

Переименуем полученные 8 битов так:

$$\begin{array}{cc|cc} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \end{array}$$

Первые четыре бита (первая строка приведенной выше матрицы) поступают на вход модуля S_0 , на выходе которого получается 2-битовая последовательность, а оставшиеся четыре бита (вторая строка матрицы) - на вход модуля S_1 , на выходе которого получается другая 2-битовая последовательность. Модули S_0 и S_1 (матрицы кодирования) работают так.

Первый и четвертый биты входной последовательности рассматриваются как 2-битовые числа, определяющие строку, а второй и третий - как числа, определяющие столбец S-матрицы. Элементы, находящиеся на пересечении соответствующих строки и столбца, задают 2-битовые выходные значения.

Теперь 4 бита, полученные на выходе модулей S0 и S1, преобразуются с помощью перестановки P4 по определенному правилу.

Результат применения перестановки P4 и является результатом функции F.

Функция – переключатель SW.

Функция f_k изменяет только четыре левых бита. Поэтому следующей операцией в алгоритме шифрования является использование функции SW, которая меняет местами первые и последние четыре бита последовательности, чтобы при следующем вызове функции f_k последняя работала уже с другой четверкой битов. При втором вызове f_k функции E/P, SO, S1 и P4 остаются теми же, что и при первом, но вместо подключа K_1 используется подключ K_2 .

Связь с DES.

На вход алгоритма DES подаются блоки по 64 бита. Для шифрования используется 56-битовый ключ, на основе которого генерируется шестнадцать 48-битовых подключей. После начальной перестановки 56-битовой последовательности выполняется цепочка операций сдвига и перестановки 48-битовых последовательностей.

В самом алгоритме шифрования функция F имеет дело не с 4-битовыми последовательностями (n_1, n_2, n_3, n_4), а с 32-битовыми последовательностями ($n_1, n_2, \dots, n_{32}$). После первой операции расширения/перестановки (E/P) получается выходная последовательность размером 48 битов (матрица).

Определяемое данной матрицей значение складывается (с помощью операции XOR) с 48-битовым подключом. В данной матрице 8 строк, каждая из которых задает свою S-матрицу. Каждая из S-матриц состоит из 4 строк и 16 столбцов. По первому и последнему битам строки представленной выше матрицы выбирается строка S-матрицы, а по оставшимся 4 битам - столбец.

Поточные и блочные шифры.

Поточными называются шифры, в которых поток цифровых данных шифруется последовательно бит за битом или байт за байтом. Примерами классических поточных шифров являются шифры

Виженера (с автоматическим выбором ключа) и Вернама. Блочными называются шифры, в которых логической единицей шифрования является некоторый блок открытого текста, после преобразований которого получается блок шифрованного текста такой же длины. Обычно используются блоки размером 64 бита. В некоторых режимах шифрования блочные шифры оказываются такими же эффективными, как и поточные.

Шифр Файстеля.

Файстель предложил аппроксимировать подстановочный шифр продукционными шифрами, которые строятся на последовательном применении как минимум двух базовых шифров с тем, чтобы полученный результат обладал более высокой стойкостью по сравнению с любым из этих базовых шифров в отдельности. В частности, Файстель предложил шифр, в котором попеременно используются и подстановки, и перестановки. Фактически данное предложение является практическим применением идеи Клода Шеннона (Claude Shannon) разработать продукционный шифр, в котором попеременно использовались бы функции *диффузии* и *конфузии*. Рассмотрим понятия диффузии и конфузии, а затем перейдем к обсуждению шифра Файстеля. Но прежде всего стоит упомянуть один весьма примечательный факт: структура шифра Файстеля, разработанная четверть века тому назад и, в свою очередь, опирающаяся на идею Шеннона, высказанную еще в 1945 г., сегодня является структурой, на основе которой построены все практически значимые симметричные схемы блочного шифрования.

Диффузия и конфузия.

Термины *диффузия* (diffusion) и *конфузия* (confusion) были введены в шифрование Клодом Шенноном для того, чтобы охарактеризовать два основных строительных блока криптографических систем [19]. Основной задачей, которую ставил перед собой Шеннон, было воспрепятствовать попыткам криптоанализа, основанным на статистическом анализе сообщений. Шеннон использовал следующие аргументы. Предположим, противник обладает некоторыми сведениями о статистических характеристиках открытого текста. Например, для обычных текстовых сообщений могут быть известны данные о распределении частот использования букв соответствующего языка. Или могут быть известны отдельные слова или фразы, вероятность присутствия которых в сообщении достаточно высока (вероятные слова). Если подобные статистически выявляемые закономерности каким-либо

образом проявятся в зашифрованном тексте, у криптоаналитика появится возможность определить ключ шифрования, или его составляющие, или хотя бы сузить пространство вероятных ключей. Шеннон вводит понятие идеального шифра - шифра, который полностью скрывает в зашифрованном тексте все статистические закономерности открытого текста.

Помимо обращения к идеальным системам, Шеннон предложил два метода, задачей которых является затруднение криптоанализа: диффузию и конфузию. *Суть диффузии* заключается в рассеянии статистических особенностей открытого текста по широкому диапазону статистических характеристик зашифрованного текста. Это достигается тем, что значение каждого элемента открытого текста влияет на значения многих элементов зашифрованного текста или, что оказывается эквивалентным сказанному, любой из элементов зашифрованного текста зависит от множества элементов открытого текста.

В любом блочном шифре используется зависящее от ключа преобразование блока открытого текста в блок зашифрованного текста. Механизм диффузии призван сделать статистическую взаимосвязь между открытым и зашифрованными текстами как можно сложнее, чтобы в максимальной степени усложнить задачу определения ключа из такой взаимосвязи. Что касается *конфузии*, то перед ней ставится задача в максимальной степени усложнить статистическую взаимосвязь между зашифрованным текстом и ключом опять же с целью противостояния попыткам определить ключ. Таким образом, даже если противник сумеет определить какие-либо статистические особенности зашифрованного текста, сложность использования ключа для получения зашифрованного текста должна оказаться достаточной для того, чтобы попытки определить ключ на основании этих статистических особенностей оказались безрезультатными. Это достигается использованием сложных подстановочных алгоритмов: простые линейные подстановочные функции увеличивают беспорядок лишь в незначительной степени.

Понятия диффузии и конфузии оказались настолько удачными с точки зрения описания сути желаемых характеристик блочных шифров, что эти термины стали базовыми для всех разработчиков современных шифров этого типа.

Структура шифра Файстеля.

На рис. 3.23 показана структура шифра, предложенного Файстелем. На вход алгоритма шифрования подается блок открытого

текста длиной $2w$ битов и ключ K . Блок открытого текста разделяется на две равные части, L_0 и R_0 , которые последовательно проходят через p раундов обработки, а затем объединяются снова для получения блока шифрованного текста соответствующей длины. Все раунды обработки проходят по одной и той же схеме. Сначала для левой половины блока данных выполняется операция подстановки.

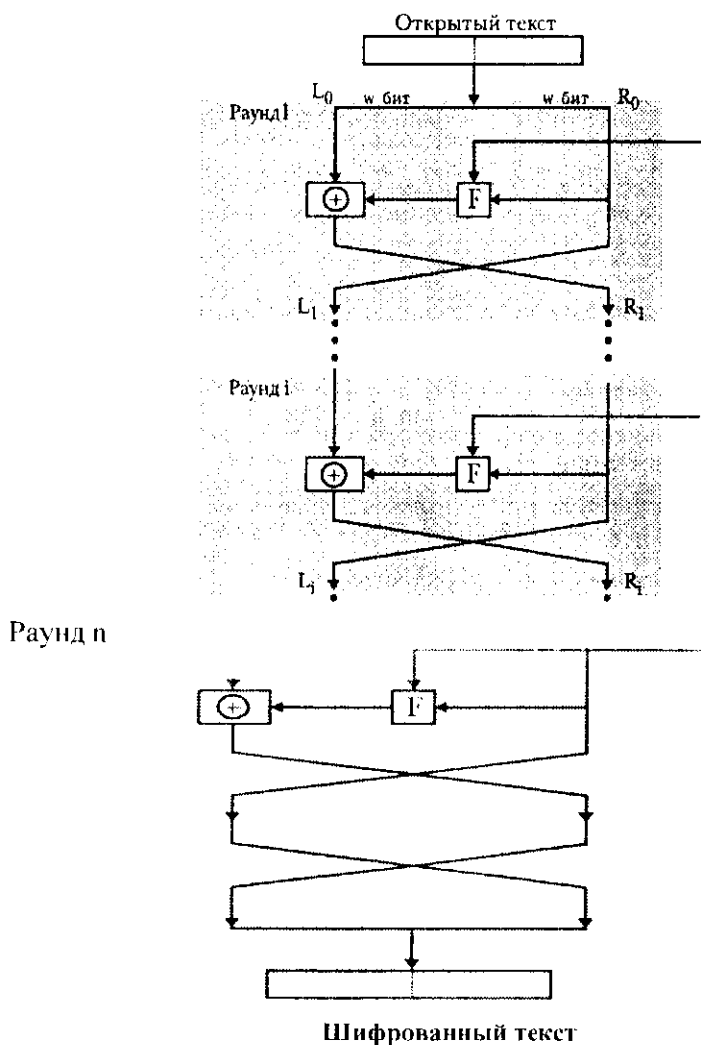


Рис. 3.23. Классическая схема Файстеля

Она заключается в применении к правой половине блока данных некоторой функции раунда F и последующем сложении полученного результата с левой половиной блока данных с помощью операции XOR (исключающего "ИЛИ"). Для всех раундов функция раунда имеет одну и ту же структуру, но зависит от параметра – подключа K_r . После подстановки выполняется перестановка, представляющая собой обмен местами двух половин блока данных.

Стандарт шифрования данных DES.

Официальная история стандарта шифрования США началась в 1972-ом году с того, что национальное бюро стандартов (НБС, National Bureau of Standards, NBS) США выдвинуло программу разработки системы стандартов по защите от несанкционированного доступа данных, хранящихся и обрабатываемых на электронно-вычислительных машинах (ЭВМ). Это направление было признано одной из самых приоритетных областей, остро нуждающейся в регламентирующих документах. Выполнение программы было возложено на Институт Информатики и Вычислительной Техники (ИИВТ), являвшийся одним из ведущих подразделений НБС в областях, связанных с компьютерной техникой.

Разработка любого стандарта должна начинаться с планирования его места в ряду взаимосвязанных нормативных документов и выбора его уровня. Так как стандарты могут принадлежать весьма широкому спектру – от общих стандартов, устанавливающих, как следует из их названия, лишь общие подходы к решению задачи, до стандартов реализации, регламентирующих все до мелочей и часто не оставляющих никакой свободы маневра в их использовании. DES (Data Encryption Standard) изначально разрабатывался как стандарт функциональной совместимости, предусматривающий спецификацию стандартизируемой функции достаточно конкретно для того, чтобы избежать возможных нестыковок, и вместе с тем без излишних деталей, которые ограничили бы способы его физической реализации.

В рамках выработки серии нормативных документов по защите данных ЭВМ от несанкционированного доступа ИИВТ выделил ряд направлений работы. Одним из важнейших направлений была признана разработка стандартного алгоритма шифрования. Деятельность по разработке и утверждению стандарта началась в мае 1973 года, когда НБС опубликовало в Федеральном Реестре США обращение с призывом к учреждениям и фирмам США предлагать

свои алгоритмы шифрования в качестве кандидатов на место стандарта. Однако откликов с конкретными предложениями не последовало.

Но уже к началу семидесятых годов двадцатого столетия компьютеры получили массовое распространение и проблема защиты данных, хранимых и обрабатываемых на них, стала осознаваться все большим числом специалистов. Многие крупные корпорации, не говоря уже о государственных службах, в закрытых ведомственных центрах, находящихся под эгидой спецслужб, проводили собственные исследования в данной области. Одним из самых известных исследовательских центров такого рода в те времена являлась научная лаборатория фирмы IBM, возглавляемая доктором Хорстом Файстелем. Проводимая в ней исследовательская работа привела к созданию практической системы шифрования, получившей название «Люцифер». Была проведена работа по разработке архитектурных принципов, позволяющих создавать эффективные и надежные шифры, хорошо подходящие для реализации на компьютерных устройствах. Архитектура шифров, базирующаяся на этих принципах, позже получила название «сеть Файстеля» по имени своего создателя. Доктор Файстель в своей известной работе «Криптография и компьютерная безопасность» изложил новый подход к созданию стойких шифров для компьютерного применения.

В августе 1974 года, национальное бюро стандартов повторило свое обращение. Именно в ответ на него фирма IBM передала НБС и согласилась предоставить всем заинтересованным сторонам исключительные права на предложенный ею алгоритм, что позволило бы им производить и продавать реализующие его изделия без лицензионных отчислений фирме. Сразу после этого НБС обратилось в Агентство Национальной Безопасности (АНБ, National Security Agency, NSA) США с просьбой провести исследование алгоритма и дать заключение о его соответствии требованиям, предъявляемым к стандарту шифрования. Именно во взаимодействии трех указанных сторон (IBM, НБС и АНБ) и родился стандарт шифрования DES.

В марте 1975 года, спустя неполных два года после публикации в Федеральном Реестре своего первого обращения, НБС там же полностью опубликовало предложенный фирмой IBM алгоритм шифрования, а вслед за ним — просьбу ко всем заинтересованным сторонам высказывать свои замечания. Так

началось "всемирное обсуждение" стандарта.

Первые критические замечания в адрес предложенного алгоритма появились практически сразу после его публикации. Одними из наиболее суровых критиков пока еще не утвержденного стандарта были М.Хеллман и У.Диффи, год спустя прославившие себя изобретением асимметричной криптографии. М.Хеллман писал: «Уит Диффи и я озабочены тем, что предлагаемый стандарт данных, хотя, вероятно, и обеспечивает защиту от коммерческих посягательств, в то же время может оказаться крайне уязвимым при действиях разведывательной организации». Основным объектом критики была слишком малая длина ключа - всего 56 бит. По оценкам М.Хеллмана, стоимость устройства для взлома шифра путем полного перебора ключей, содержащего миллион узлов, способных опробовать миллион ключей в секунду, не должна превышать \$20,000,000. Такая сумма уже в то время была вполне по силам разведывательной службе крупного государства. С тех пор эта сумма уменьшилась на несколько порядков благодаря бурному развитию микроэлектроники.

Другим направлением критики предложенного стандарта было отсутствие в открытой печати критериев проектирования отдельных его решений, главным образом это относилось к узлам замены или S-блокам, как они названы в стандарте. Скептики отмечали, что поскольку критерии выбора узлов замены не были опубликованы, они (узлы) могли быть сконструированы специальным образом, чтобы те, кто обладает этими секретными знаниями, могли подвергнуть шифр криптоанализу.

Тем не менее, несмотря на критику, стандарт был принят в качестве 46-го параграфа Федерального стандарта обработки информации США (Federal Information Processing Standard, FIPS) и вступил в действие с момента его опубликования 15 января 1977 года. Позже М.Хеллман инициировал сенатское расследование обстоятельств разработки и утверждения стандарта, так как считал, что его принятие наносит ущерб национальной безопасности США. Это расследование закончилось ничем, однако, в его ходе вскрылись интересные факты. Оказалось, что в первоначально предложенном фирмой IBM варианте шифра длина ключа была большей - 128-разрядов, и именно АНБ настояло на ее уменьшении до 56 бит. Второе изменение, предложенное АНБ, касалось таблиц шифрования S-box данного алгоритма. Некоторые аналитики опасались, что

изменения в S-box могли бы привести к появлению обходных путей, зная которые, взломщик мог расшифровать сообщения DES, не перебирая все возможные ключи.

По существу, любое ослабление значительно сокращает число ключей, которое не обязательно проверить злоумышленнику, чтобы взломать DES. Опасения еще больше усилились, когда NSA рекомендовало IBM не описывать критерии, используемые при составлении S-box. Это дало серьезную почву для подозрений, что АНБ обладает возможностью читать зашифрованные с помощью DES сообщения.

Впрочем, интенсивные исследования шифра не обнаружили очевидных слабостей в нем, а выбранная длина ключа в то время была достаточной и взлом алгоритма "грубой силой", т.е. перебором по всему ключевому пространству, был за гранью экономической целесообразности, так как требовал бы чрезвычайно высоких затрат. Не следует забывать и то, что стандарт определяет алгоритм шифрования несекретных данных - в совокупности с предыдущим это оправдывает отсутствие запаса прочности в нем. Исследователи отметили, что существующей длины ключа будет вполне достаточно на 10-15 лет, и в этом они не ошиблись. На всякий случай было решено пересматривать стандарт каждые пять лет.

Такие пересмотры были выполнены в 1983, 1988 и 1993 годах, тогда стандарт был оставлен без изменений.

Дифференциальный и линейный криптоанализы.

Применение методов *дифференциального* криптоанализа на практике является непростым делом [19].

Процедура начинается с рассмотрения двух сообщений открытого текста m и m' с заданной разностью и имеет своей целью получение вероятностных оценок разностей промежуточных результатов последовательно раунд за раундом с тем, чтобы определить вероятностную оценку для разности соответствующих зашифрованных текстов. На самом деле получаются вероятностные оценки для двух 32- битовых половинок сообщения ($m_{17} \parallel m_{16}$). После этого выполняется шифрование m и m' , чтобы определить реальные разности при неизвестном ключе, а затем сравнить результат с вычисленными вероятностными оценками. Если результаты совпадают, т.е. $E_K(m) \oplus E_K(m') = (\Delta m_{17} \parallel m_{16})$, то можно ожидать, что вероятностные оценки для всех раундов соответствуют реальности. Это позволяет сделать определённые заключения о некоторых битах

ключа. Чтобы определить все биты ключа, процедуру повторяют много раз.

Метод линейного криптоанализа заключается в построении линейной аппроксимации преобразования, выполняемого в ходе шифрования DES. Данный метод позволяет найти ключ DES при наличии 2^{47} известных фрагментов открытого текста, тогда как для дифференциального криптоанализа требуется 2^{47} фрагментов избранного открытого текста. Но хотя это и упрощает задачу криптоаналитика, поскольку легче раздобыть какой-нибудь известный открытый текст, чем избранный, с такими ограничениями линейный криптоанализ все же остается практически нереальным в отношении DES. Поэтому мало кто пытается практически реализовать методику линейного криптоанализа.

Стандарт шифрования данных AES.

Однако вскоре слабость шифра стала очевидной, и для увеличения стойкости специалисты рекомендовали при его использовании выполнять шифрование два или три раза с различными ключами. В 1998 году, когда всем стало окончательно ясно, что стандарт шифрования должен быть заменен, Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST), правопреемник прежнего НБС, выпустил запрос на комментарий (Request For Comment — RFC), где описывался предполагаемый «Усовершенствованный стандарт шифрования» (Advanced Encryption Standard - AES), который должен прийти на смену DES.

Специалистам по стандартизации предстояло, интенсивно сотрудничая с представителями отрасли и специалистами по криптографии, разработать следующее поколение алгоритмов шифрования частным ключом. При шифровании частным ключом применяется один секретный ключ, как для шифрования, так и для дешифрования. Алгоритм предусматривает выполнение нескольких итераций, или раундов. В каждом раунде используется подключ, полученный из базового ключа. Преобразование из обычного текста в зашифрованный и обратно выполняется в несколько раундов и предусматривает применение подключа. Выбор или генерация подключей называется графиком, планированием или расширением ключа (key schedule). Обычно при шифровании и дешифровании применяется один и тот же алгоритм, но с различными графиками ключа.

Критерии AES.

Для того чтобы алгоритм AES стал достойной заменой DES, его архитектура должна удовлетворять нескольким критериям: предлагать высокую степень защиты, обладать простой структурой и высокой производительностью.

Очевидно, что наивысшим приоритетом для алгоритма AES является защита. Уже на уровне внутренней архитектуры он должен обладать надежностью, достаточной для того, чтобы противостоять будущим попыткам его взлома. Вместе с тем, структура алгоритма, в противовес традиционным воззрениям, должна быть настолько простой, чтобы гарантировать эффективную процедуру шифрования.

Следующим в списке требований, предъявляемых к AES, стоит высокая производительность. Широкое распространение алгоритма на рынке потребует приемлемой производительности при работе на самых разных платформах, от смарт-карт до крупных серверов. Хорошая производительность алгоритма предполагает высокую скорость работы при шифровании и дешифровании, а также при реализации графика ключа.

Требования и процедура.

В 1998 году NIST объявил конкурс на создание алгоритма, удовлетворяющего выдвинутым Институтом требованиям. Он опубликовал все несекретные данные о тестировании кандидатов на роль AES и потребовал от авторов алгоритмов сообщить о базовых принципах построения используемых в них констант, таблиц S-box. В отличие от ситуации с DES, NIST при выборе AES не стал опираться на секретные и, как следствие, запрещенные к публикации данные об исследовании алгоритмов-кандидатов.

Чтобы быть утвержденным в качестве стандарта, алгоритм должен:

- реализовать шифрование частным ключом;
- представлять собой блочный шифр;
- работать со 128-разрядными блоками данных и ключами трех размеров (128, 192 и 256 битов).

Дополнительно кандидатам рекомендовалось:

- использовать операции, легко реализуемые как аппаратно (в микрочипах), так и программно (на персональных компьютерах и серверах);
- ориентироваться на 32-разрядные процессоры;
- не усложнять, без необходимости, структуру шифра для того,

чтобы все заинтересованные стороны были в состоянии самостоятельно провести независимый криптоанализ алгоритма и убедиться, что в нем не заложено каких-либо недокументированных возможностей.

Кроме того, алгоритм, претендующий на то, чтобы стать стандартом, должен распространяться по всему миру на не эксклюзивных условиях и без платы за пользование патентом.

Перед проведением первого тура конкурса в NIST поступило 21 предложение, из которых 15 удовлетворяли выдвинутым критериям. Затем были проведены исследования этих решений, в том числе связанные с дешифрованием и проверкой производительности, и получены экспертные оценки специалистов по криптографии. В августе 1999 года NIST объявил пять финалистов, краткие сведения о которых приводятся в таблице 3.19, которые получили право на участие во втором этапе обсуждений.

При окончательном тестировании учитывались следующие девять характеристик: две касались защиты (общий уровень защиты и защищенность реализации), одна характеризовала гибкость, а остальные были связаны с эффективностью реализации.

Победитель Rijndael - быстрый и компактный алгоритм с простой математической структурой. благодаря чему, он оказался прост для анализа при оценке уровня защиты, и никаких претензий специалисты NIST при этом не высказали. С другой стороны, из-за этой простоты хакерам потребуется изучить более ограниченный математический аппарат и, если где-то в Rijndael есть скрытые проблемы, то рано или поздно их кто-нибудь обнаружит. Атаки на версию с сокращенным числом раундов показали, что Rijndael не имеет такого запаса прочности, как другие кандидаты, а увеличение числа раундов замедляет его работу.

Кроме того, Rijndael продемонстрировал хорошую устойчивость к атакам на реализацию, при которых хакер пытается декодировать зашифрованное сообщение, анализируя внешние проявления алгоритма, в том числе уровень энергопотребления и время выполнения.

В NIST были проверены уязвимости всех кандидатов к таким атакам и их способность противостоять им, обычно за счет специального кодирования, для выравнивания уровня энергопотребления. Rijndael можно легко защитить от таких атак, поскольку он опирается в основном на булевы операции.

Таблица 3.19

Финалисты

Алгоритм	Предложен	Основное достоинство	Основной недостаток	Страна	Быстродействие (asm, 200 МГц)
MARS	Корпорацией IBM	Высокий уровень защиты	Сложная реализация	US	8 Мбайт/с
RC6	Компанией RSA Security	Очень простой	Недостаточный уровень защиты	US	12 Мбайт/с
Rijndael	Джоаном Дименом и Винсентом Риджменом	Простая архитектура, хорошие общие характеристики	Нейдовлительный график	BE	7 Мбайт/с
Serpent	Россом Андерсоном, Эли Бихам и Ларсом Кнудсенем	Высокий уровень защиты	Сложная архитектура, невысокая производительность	IS, UK, NO	2 Мбайт/с
Twofish	Брюсом Шнайером и другими сотрудниками компании Counterpane Internet Security	Приемлемая производительность и уровень защиты	Сложная архитектура	US	11 Мбайт/с

Общая производительность программных реализаций Rijndael оказалась наилучшей. Он прекрасно прошел все тесты со смарт-картами и в аппаратных реализациях. Алгоритму в значительной степени присущ внутренний параллелизм, что позволяет без труда обеспечить эффективное использование процессорных ресурсов. Увеличение длины ключа несколько замедляет его работу, поскольку при обработке ключей большей длины алгоритм предусматривает выполнение дополнительных раундов шифрования.

NIST остановил свой выбор на Rijndael, поскольку тот сочетает в себе простоту и высокую производительность. Хотя Rijndael обладает меньшим запасом прочности, чем другие финалисты, это не несет в себе никакого практического риска.

Победитель AES – шифр Rijndael.

2 октября 2000 года NIST объявил о своем выборе – победителем конкурса стал алгоритм RIJNDAEL (произносится как "райндол") бельгийских криптографов Винсента Раймана и Йоана Дамана, который зарегистрирован в качестве официального федерального стандарта как FIPS 197 (Federal Information Processing Standard).

Министр торговли Норман Минета официально объявил об этом на встрече с руководителями компаний IT-индустрии. Министерство торговли высоко оценило заслуги разработчиков Rijndael, а особенно то, что они согласились предоставить алгоритм для свободного использования без каких-либо авторских отчислений.

Доктор Даман работает в группе архитектуры и криптографии научно-исследовательского отдела компании Proton World, а его соавтор, доктор Райман, руководит исследованиями на факультете электроники Левенского католического университета.

Высочайшую надежность AES NIST подтверждает астрономическими числами. 128-битный ключ обеспечивает 340 андециллионов ($340 \cdot 10^{36}$) возможных комбинаций, а 256-битный ключ увеличивает это число до $11 \cdot 10^{76}$. Для сравнения, старый алгоритм DES, дает общее число комбинаций в $72 \cdot 10^{15}$. На их перебор у специально построенной машины «DES Cracker» уходит несколько часов. Но даже если бы она делала это всего за одну секунду, то на перебор 128-битного ключа машина потратила бы 149 триллионов лет. Между тем, возраст всей Вселенной ученые оценивают в менее, чем 20 миллиардов лет.

Структура шифра AES.

Формат блоков данных и число раундов.

RIJNDAEL - это симметричный блочный шифр, оперирующий блоками данных размером 128 и длиной ключа 128, 192 или 256 бит - название стандарта соответственно «AES-128», «AES-192», и «AES-256».

Введем следующие обозначения:

Nb – число 32-битных слов содержащихся во входном блоке,
 $Nb = 4$;

Nk - число 32-битных слов содержащихся в ключе шифрования $Nk=4, 6, 8$;

Nr - число раундов шифрования, как функция от Nb и Nk , $Nr=10, 12, 14$.

Входные (*input*), промежуточные (*state*) и выходные (*output*) результаты преобразований, выполняемых в рамках криптоалгоритма, называются *состояниями* (*State*). Состояние можно представить в виде матрицы $4 \times Nb$, элементами которой являются байты (четыре строки по Nb байт) в порядке $S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, S_{11}, S_{21}, S_{31}, \dots$

Рисунок 3.24 демонстрирует такое представление, носящее название архитектуры «Квадрат».

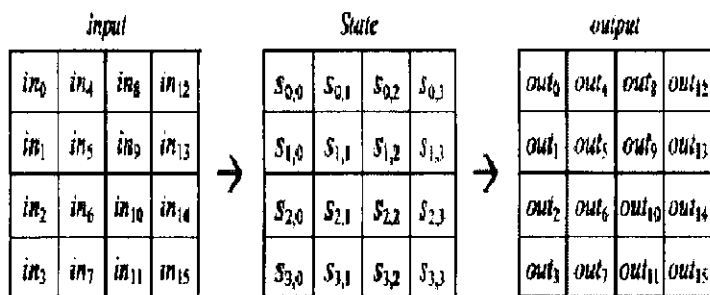


Рис.3.24. Пример представления блока в виде матрицы $4 \times Nb$

На старте процессов шифрования и дешифрования массив входных данных $in_0, in_1, \dots, in_{15}$ преобразуется в массив *State* по правилу $s[r,c] = in[r+4c]$, где $0 \leq r < 4$ и $0 \leq c < Nb$. В конце действия алгоритма выполняется обратное преобразование $out[r+4c] = s[r,c]$, где $0 \leq r < 4$ и $0 \leq c < Nb$ - выходные данные получаются из байтов состояния в том же порядке.

Четыре байта в каждом столбце состояния представляют собой 32-битное слово, если r - номер строки в состоянии, то одновременно он является индексом каждого байта в этом слове. Следовательно состояние можно представить как одномерный массив 32-битных слов, $w_0, \dots, w_{Nb}$, где номер столбца состояния c есть индекс в этом массиве. Тогда, состояние можно представить так:

$w_0 = s_{0,0}, s_{1,0}, s_{2,0}, s_{3,0}$	$w_2 = s_{0,2}, s_{1,2}, s_{2,2}, s_{3,2}$
$w_1 = s_{0,1}, s_{1,1}, s_{2,1}, s_{3,1}$	$w_3 = s_{0,3}, s_{1,3}, s_{2,3}, s_{3,3}$

Ключ шифрования также как и массив *State* представляется в виде прямоугольного массива с четырьмя строками. Число столбцов этого массива равно Nk .

Для алгоритма AES число раундов Nr определяется на старте в зависимости от значений Nk и Nb :

	Nk	Nb	Nr
AES – 128	4	4	10
AES – 192	6	4	12
AES - 256	8	4	14

Функция зашифрования.

Введем следующие обозначения:

SubBytes() – замена байтов – побайтовая нелинейная подстановка в *State*-блоках (SBox) с использованием фиксированной таблицы замен размерностью 8×256 (affain map table);

ShiftRows() – сдвиг строк – циклический сдвиг строк массива *State* на различное количество байт;

MixColumns() – перемешивание столбцов – умножение столбцов состояния, рассматриваемых как многочлены над $(GF(2^8))$;

AddRoundKey() – сложение с раундовым ключом – поразрядное XOR содержимого *State* с текущим фрагментом развернутого ключа.

Операция зашифрования, реализованная на псевдокоде, представлена на рис. 3.25.

После заполнения массива *State* элементами входных данных к нему применяется преобразование *AddRoundKey()*, далее, в зависимости от величины Nk , массив *State* подвергается раундовой трансформации 10, 12 или 14 раз, причем в финальный раунд является несколько укороченным - в нем отсутствует преобразование *MixColumns()*. Выходными данными описанной последовательности операций является шифротекст – результат действия функции зашифрования AES.

```

Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]

  state = in

  AddRoundKey(state, w[0, Nb-1])

  for round = 1 step 1 to Nr-1
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
  end for

  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

  out = state
end

```

Рис. 3.25. Операция зашифрования, реализованная на псевдокоде

Функции расшифрования.

В спецификации алгоритма AES предлагаются два вида реализаций функции рас шифрования отличающихся друг от друга последовательностью приложения преобразований обратных преобразования функции зашифрования и последовательностью планирования ключей (см. ниже).

Введем следующие обозначения:

InvSubBytes() — обратная *SubBytes()* замена байтов — побайтовая нелинейная подстановка в *State*-блоках с использованием фиксированной таблицы замен размерностью 8×256 (inverse affain map);

InvShiftRows() — обратный сдвиг строк *ShiftRows()* — циклический сдвиг строк массива *State* на различное количество байт;

InvMixColumns() — восстановление значений столбцов — умножение столбцов состояния, рассматриваемых как многочлены над $GF(2^8)$;

Функция обратного расшифрования.

Если вместо *SubBytes()*, *ShiftRows()*, *MixColumns()* и *AddRoundKey()* в обратной последовательности выполнить

инверсные им преобразования, можно построить функцию обратного расшифрования. При этом порядок использования раундовых ключей является обратным по отношению к тому, который используется при зашифровании.

Операция обратного расшифрования, реализованная на псевдокоде, представлена на рис. 3.26.

```

InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nr*(Nr+1)])
begin
  byte state[4,Nb]

  state = in

  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

  for round = Nr-1 step -1 downto 1
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
    InvMixColumns(state)
  end for

  InvShiftRows(state)
  InvSubBytes(state)
  AddRoundKey(state, w[0, Nb-1])

  out = state
end

```

Рис 3.26. Операция обратного расшифрования, реализованная на псевдокоде

Функция прямого расшифрования.

Алгоритм обратного расшифрования, описанный выше имеет порядок приложения операций-функций обратный порядку операций в алгоритме прямого зашифрования, но использует те же параметры развёрнутого ключа. Изменив определенным образом последовательность планирования ключа можно построить еще один алгоритм – алгоритм *прямого* расшифрования (рис.3.27).

Два следующих свойства позволяют сделать это:

- порядок приложения функций *SubBytes()* и *ShiftRows()* не играет роли. То же самое верно и для операций *InvSubBytes()* и *InvShiftRows()*. Это происходит потому, что функции *SubBytes()* и

InvSubBytes() работают с байтами, а операции *ShiftRows*() и *InvShiftRows*() сдвигают целые байты, не затрагивая их значений.

• операция *MixColumns*() является линейной относительно входных данных, что означает $InvMixColumns(State \oplus RoundKey) = InvMixColumns(State) \oplus InvMixColumns(RoundKey)$.

```

BqInvCipher(byte in[4*Nb], byte out[4*Nb], word dw[Nb*(Nr+1)])
begin
    byte state[4,Nb]

    state = in

    AddRoundKey(state, dw[Nr*Nb, (Nr+1)*Nb-1])

    for round = Nr-1 step -1 downto 1
        InvSubBytes(state)
        InvShiftRows(state)
        InvMixColumns(state)
        AddRoundKey(state, dw[round*Nb, (round+1)*Nb-1])
    end for

    InvSubBytes(state)
    InvShiftRows(state)
    AddRoundKey(state, dw[0, Nb-1])

    out = state
end

```

Рис. 3.27. Операция прямого расшифрования реализованная на псевдокоде

Эти свойства функций алгоритма шифрования позволяют изменить порядок применения функций *InvSubBytes*() и *InvShiftRows*(). Функции *AddRoundKey*() и *InvMixColumns*(), также могут быть применены в обратном порядке, но при условии, что столбцы (32-битные слова) развёрнутого ключа расшифрования предварительно пропущены через функцию *InvMixColumns*().

Таким образом, можно реализовать более эффективный способ расшифрования с тем же порядком приложения функций, как и в алгоритме шифрования.

Алгоритм выработки ключей (Key Schedule).

Введем следующие обозначения:

Rcon[] – массив 32-битных раундовых констант;

RotWord() – операция циклической перестановки входного 4-байтного слова в выходное по следующему правилу

$$[a_0, a_1, a_2, a_3] \rightarrow [a_1, a_2, a_3, a_0];$$

SubWord() – операция замены в 4-байтном слове с помощью S-Box каждого байта.

Раундовые ключи получаются из ключа шифрования посредством алгоритма выработки ключей. Он содержит два компонента: *расширение ключа* (Key Expansion) и *выбор раундового ключа* (Round Key Selection). Основополагающие принципы алгоритма выглядят следующим образом (Рис. 3.28):

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
    word temp

    i = 0

    while (i < Nk)
        w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
        i = i+1
    end while

    i = Nk

    while (i < Nb * (Nr+1))
        temp = w[i-1]
        if (i mod Nk = 0)
            temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
        else if (Nk > 6 and i mod Nk = 4)
            temp = SubWord(temp)
        end if
        w[i] = w[i-Nk] xor temp
        i = i + 1
    end while
end
```

Рис. 3.28. Операция планирования (расширения) ключа реализованная на псевдокоде

- общее число битов раундовых ключей равно длине блока, умноженной на число раундов, плюс 1;
- ключ шифрования расширяется в *расширенный ключ* (Expanded Key);
- раундовые ключи берутся из расширенного ключа следующим образом: первый раундовый ключ содержит первые Nb слов, второй – следующие Nb слов и т. д.

Расширение (планирование) ключа.

Расширенный ключ (Рис.3.29) представляет собой линейный массив $w[i]$ состоящий из $4(Nr+1)$ 4-байтовых слов, $i=0, 4(Nr+1)$

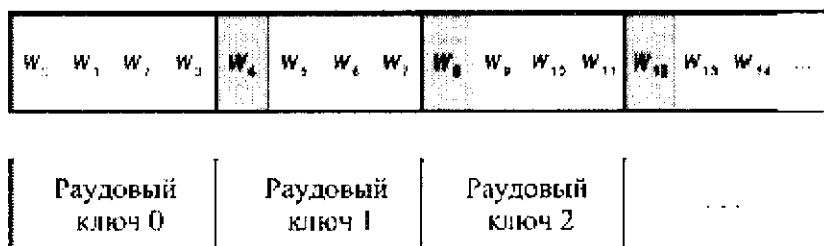


Рис. 3.29. Процедуры расширения и выборки раундового ключа для $Nk=4$. (Светло-серым цветом выделены слова расширенного ключа, которые формируются без использования функций $SubWord()$ и $RotWord()$. Темно-серым цветом, выделены слова расширенного ключа, при вычислении которых используются преобразования $SubWord()$ и $RotWord()$)»

Первые Nk слов содержат ключ шифрования. Каждое последующее слово $w[i]$ и i получается посредством XOR предыдущего слова $w[i-1]$ и слова на Nk позиций ранее $w[-Nk]:w[i-1] XOR w[i-Nk]$

Для слов, позиция которых кратна Nk , перед XOR применяется преобразование к $w[i-1]$, а затем еще прибавляется раундовая константа $Rcon[i]$. Преобразование реализуется с помощью двух дополнительных функций: $RotWord()$ и $SubWord()$.

Значение $Rcon[i]$ равно 2^{i-1} .

Значение $w[i]$ в этом случае определяется выражением $w[i]=SubWord(RotWord(w[i-1]))xor(Rcon[i/Nk]))xor(w[i-Nk])$

Выбор раундового ключа.

i -тый раундовый ключ выбирается из слов массива расширенного ключа в промежутке от $W[Nb*i]$ до $W[Nb*(i+1)]$.

Для функции зашифрования расширенный ключ генерируется алгоритмом Рисунок 3.28. Для функции обратного расшифрования

используется этот же ключ, но в обратной последовательности начиная с последнего раундового подключа зашифрования.

Для функции прямого расшифрования используется несколько модифицированный алгоритм планирования ключа. При формировании развёрнутого ключа в процедуру планирования необходимо добавить в конце дополнительное преобразование (рис. 3.30), причем расширенный ключ используется при прямом расшифровании в той же последовательности, что и при зашифровании.

```

for i = 0 step 1 to (Nr+1)*Nb-1
    dw[i] = v[i]
and for

for round = 1 step 1 to Nr-1
    InvMixColumns(dw[round*Nb, (round+1)*Nb-1])
and for
    
```

Рис. 3.30. Дополнительное преобразование расширенного ключа для функции прямого расшифрования

Раундовое преобразование

Раундовое преобразование состоит из последовательного применения к массиву *State* ряда трансформаций. Обсудим детали его реализации.

Замена байтов.

Нелинейная замена байтов массива состояния посредством трансформации *SubBytes()* имеет вид:

$$\lambda(f) \equiv ((X^4 + X^3 + X^2 + X + 1) \cdot f + X^6 + X^5 + X + 1) \bmod (X^8 + 1)$$

Многочленное вычисление в процессе зашифрования данного выражения оказывало бы неоправданную вычислительную нагрузку на исполняющую систему, поэтому для практической реализации наиболее приемлемым решением является использование предварительно вычисленной таблицы замены *S-Box*. Логика работы *S-Box* при преобразовании байта {xy} отражена в шестнадцатеричном виде на рис. 3.31.

Ее использование сводит операцию *SubBytes()* к простейшей выборке байта из массива $\lambda(f) = Sbox[f]$. В функциях

расшифрования применяется операция обратная *SubBytes()* - *InvSubBytes()*. Математическая интерпретация которой выражается следующей формулой

$$\lambda^{-1}(f) \equiv ((X^6 + X^3 + X) \cdot f + X^2 + 1) \bmod (X^8 + 1),$$

но реализуется так же просто, как и предыдущая посредством инверсной таблицы S-Box - $\lambda^{-1}(f) = \text{InvSbox}[f]$, ее логика работы при преобразовании байта {xy} отражена в шестнадцатеричном виде на рис. 3.32.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3e	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	4e	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	20	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рис. 3.31. Таблица S-Box замены байт

Рисунок 3.33 иллюстрирует применение преобразования замены байт к состоянию в функциях зашифрования и расшифрования:

Сдвиг строк.

В преобразовании сдвига строк (*ShiftRows*) последние 3 строки состояния циклически сдвигаются ВЛЕВО на различное число байтов. Строка 1 сдвигается на C1 байт, строка 2 – на C2 байт, и строка 3 – на C3 байт. Значения сдвигов C1, C2 и C3 в *Rijndael*

зависят от длины блока Nb . Их величины приведены в таблице 3.20.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9a	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ae	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	0b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	a4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	ae	73
	9	96	ac	74	22	e7	ad	35	85	a2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fa	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Рис. 3.32. Таблица S-Box инверсной замены байт

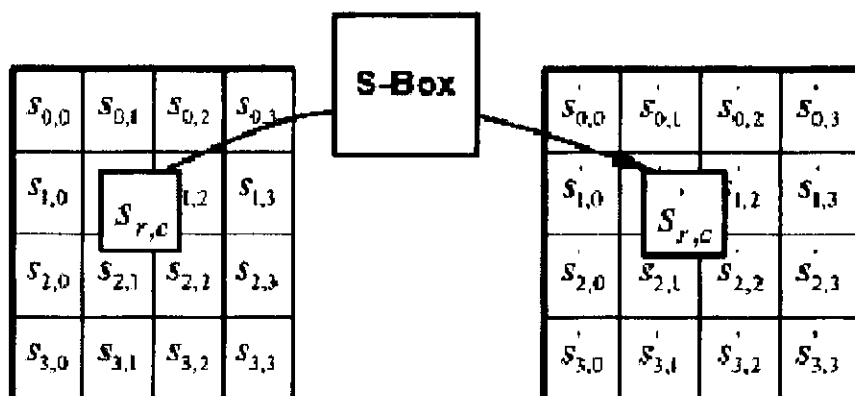


Рис. 3.33. Преобразование состояния посредством таблицы замены S-Box. Сдвиг строк

Величина сдвига строк для разной длины блоков

N_b	$shift(0, Nb) = C_0$	$shift(1, Nb) = C_1$	$shift(2, Nb) = C_2$	$shift(3, Nb) = C_3$	
4	0	1	2	3	AES
6	0	1	2	3	
8	0	1	3	4	

В стандарте *AES*, где определен единственный размер блока, равный 128 битам, $C_1 = 1$, $C_2 = 2$ и $C_3 = 3$.

Операция сдвига содержимого состояния может быть представлена следующим выражением - $S'_{r,c} = S_{r,c - shift(r, Nb) \bmod Nb}$ для $0 < r < 4$ и $0 < c < Nb$, где значение $shift(r, Nb)$ зависит от номера строки r .

Рисунок 3.34 показывает влияние преобразования *ShiftRows()* на состояние.

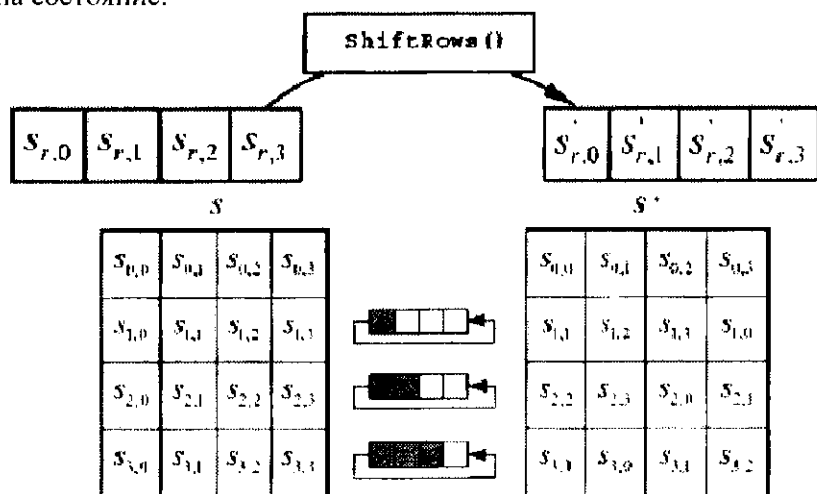


Рис. 3.34. Преобразование сдвига строк в функции зашифрования

В преобразовании обратного сдвига строк *InvShiftRows* последние 3 строки состояния циклически сдвигаются **ВПРАВО** на различное число байтов. Строка 1 сдвигается на C1 байт, строка 2 – на C2 байт, и строка 3 – на C3 байт. Значения сдвигов C1, C2 и C3 зависят от длины блока *Nb*. Их величины естественно соответствуют значениям приведенным в таблице 3.20.

Операция обратного сдвига *InvShiftRows()* содержимого состояния представлена выражением $S'_{r,c} = \text{shift}(r, Nb) \bmod Nb + S_{r,c}$ для $0 < r < 4$ и $0 < c < Nb$, где значение *shift*(*r*, *Nb*) зависит от номера строки *r*. Рисунок 3.35 иллюстрирует преобразования обратного сдвига

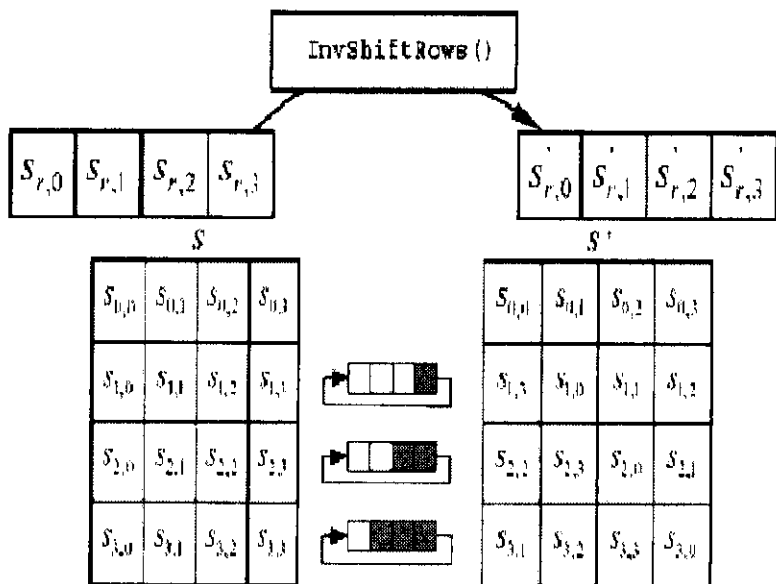


Рис. 3.35. Преобразование обратного сдвига строк в функции расшифрования

Перемешивание столбцов.

В преобразовании перемешивания столбцов (*MixColumns*) столбцы состояния рассматриваются как многочлены над $GF(2^8)$ и подвергаются преобразованию $\mu(g) \equiv c \cdot g \bmod(Y^4 + 1)$, где $C=(X,1,1,X+1)$ т.е умножаются по модулю $x^4 + 1$ на многочлен $c(x)$, выглядящий, как: $c(x)=\{03\}x^3+\{01\}x^2+\{01\}x+1$

Это преобразование может быть представлено в матричном

виде следующим образом:

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix}, \quad 0 \leq c \leq 3, \text{ где } c - \text{номер столбца массива State.}$$

В результате такого умножения байты столбца $s_{0c}, s_{1c}, s_{2c}, s_{3c}$ заменяются соответственно на байты

$$\begin{aligned} s'_{0c} &= (\{02\} \bullet s_{0c}) \oplus (\{03\} \bullet s_{1c}) \oplus s_{2c} \oplus s_{3c}, \\ s'_{1c} &= s_{0c} \oplus (\{02\} \bullet s_{1c}) \oplus (\{03\} \bullet s_{2c}) \oplus s_{3c}, \\ s'_{2c} &= s_{0c} \oplus s_{1c} \oplus (\{02\} \bullet s_{2c}) \oplus (\{03\} \bullet s_{3c}), \\ s'_{3c} &= (\{03\} \bullet s_{0c}) \oplus s_{1c} \oplus s_{2c} \oplus (\{02\} \bullet s_{3c}). \end{aligned}$$

Применение этой операции ко всем четырём столбцам состояния обозначается, как *MixColumns(State)*. Рисунок 3.36 демонстрирует применение преобразования *MixColumns()* к столбцу состояния.

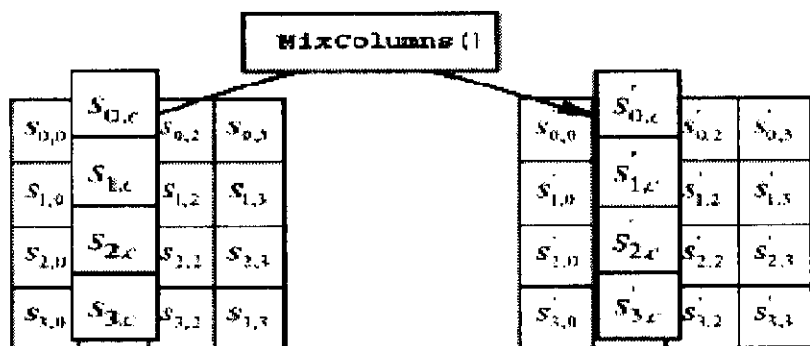


Рис. 3.36. Операция перемешивания действует на столбцы состояния

В обратном преобразовании *InvMixColumns()* столбцы состояния рассматриваются как многочлены над $GF(28)$, но, естественно, подвергаются обратному преобразованию

$$V(g) = \mu^{-1}(g) \equiv d \cdot g \bmod (T^4 - 1), \text{ где } d = (X^3 - X^2 - X \cdot X^3 - 1 \cdot X^3 + X^2 + 1 \cdot X^2 + X - 1).$$

т.е. умножаются по модулю $x^4 + 1$ на многочлен $d(x)$, выглядящий

следующим образом:

$$d(x) = \{0b\}x^3 - \{0a\}x^2 + \{09\}x + \{0e\}.$$

Это может быть представлено в матричном виде следующим образом:

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \cdot \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix}, \quad 0 \leq c \leq 3, \text{ где } c - \text{номер столбца массива } State.$$

В результате на выходе получаются следующие байты:

$$s'_{0c} = (\{0e\} \bullet s_{0c}) \oplus (\{0b\} \bullet s_{1c}) \oplus (\{0d\} \bullet s_{2c}) \oplus (\{09\} \bullet s_{3c}),$$

$$s'_{1c} = (\{09\} \bullet s_{0c}) \oplus (\{0e\} \bullet s_{1c}) \oplus (\{0b\} \bullet s_{2c}) \oplus (\{0d\} \bullet s_{3c}),$$

$$s'_{2c} = (\{0d\} \bullet s_{0c}) \oplus (\{09\} \bullet s_{1c}) \oplus (\{0e\} \bullet s_{2c}) \oplus (\{0b\} \bullet s_{3c}),$$

$$s'_{3c} = (\{0b\} \bullet s_{0c}) \oplus (\{0d\} \bullet s_{1c}) \oplus (\{09\} \bullet s_{2c}) \oplus (\{0e\} \bullet s_{3c}).$$

Рисунок 3.36 может также являться демонстрацией применения обратного преобразования *InvMixColumns()* к столбцу состояния в функции расшифрования.

Добавление раундового ключа AddRoundKey().

В данной операции раундовый ключ добавляется к состоянию посредством поразрядного XOR. Длина ключа (в 32-разрядных словах) равна длине блока *Nb*.

Преобразование, содержащее добавление раундового ключа к состоянию представляется выражением

$$[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus [w_{r(Nb+c)}], \quad \text{где } 0 \leq c \leq Nb \text{ и } 0 \leq r \leq Nr$$

Рисунок 3.37 иллюстрирует действие данной операции на состояние. Это преобразование обозначается как *AddRoundKey(State, RoundKey)*.

Основные особенности AES.

В заключении сформулируем *основные особенности AES*:

- новая архитектура «Квадрат», обеспечивающая быстрое рассеивание и перемешивание информации, при этом за один раунд преобразованию подвергается весь входной блок;

- байт-ориентированная структура, удобная для реализации на 8-разрядных микроконтроллерах;
- все раундовые преобразования суть операции в конечных полях, допускающие эффективную аппаратную и программную реализацию на различных платформах.

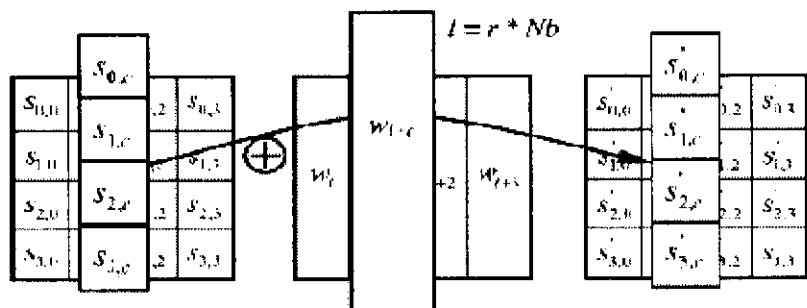


Рис. 3.37. $\text{AddRoundKey}(\text{State}, \text{RoundKey})$. действует на столбцы состояния

Атаки на AES.

Оказывается непривилегированный пользователь сервера, работающего с AES-ключами, может эти ключи украсть. Это оказывается возможным, если в качестве процессора в сервере используется Pentium 4/Xeon с включенной поддержкой HyperThreading. И возможность эта появляется именно из-за наличия HT, не зависит от используемой операционной системы и не связана с ошибками в ПО.

Собственно, угрозы данного типа не новы. Они носят более общий характер и связаны с некоторыми особенностями современных компьютерных архитектур. Просто для Pentium 4/Xeon с поддержкой HT были написаны конкретные коды, демонстрирующие, как при работе с OpenSSL в многопользовательской среде можно украсть криптографический ключ, а соответствующая информация стала доступной в Internet. Вообще же данный тип криптографических атак, основанных на тонких замерах времени выполнения, изучался достаточно давно (насколько известно, с середины 90-х годов), однако «широкая компьютерная общественность» про это слышала мало. В ноябре 2004 года появилась работа Даниэля Бернштейна из Чикагского университета, посвященная атакам на AES, которые использовали замеры времени, связанного с обращением в кэш-память. В качестве иллюстрации Бернштейн показал, как «незаконно»

получить AES-ключ при работе с OpenSSL на платформе Pentium III, отметив, что аналогичную процедуру можно проделать и с другими процессорами, например AMD Athlon, IBM PowerPC RS64 IV и Sun UltraSPARC III. Источником проблемы в этом случае являются изменяющиеся (неодинаковые) времена выполнения отдельных функций, применяемых для быстрой работы с AES.

Схожая проблема, вероятно, возникнет на любом современном микропроцессоре, и чтобы от нее избавиться, желательно иметь высокопроизводительный программный инструментарий для AES с постоянным временем выполнения. Однако разработка такого инструментария очень сложна: постоянные времена выполнения сегодня достигаются только при работе на относительно медленных алгоритмах. В качестве возможного выхода Бернштейн, как и ряд других специалистов, предложил разработчикам процессоров включать в набор команд специальную команду для работы с AES, что способно дать практически постоянное время выполнения.

Что же касается проблем с HT, то группа норвежских специалистов еще в марте сообщила, что они в течение одной минуты смогли установить 45 из 128 разрядов AES-ключа, но детали их атаки, насколько известно, не раскрывались. Норвежцы предложили попросту отключать HT.

Общим методом борьбы с атаками, основанными на измерении времени доступа в кэш, может стать запрещение использования в непривилегированном режиме команд замера числа тактов наподобие RDTSC для x86, которые нужны для точного замера интервалов времени. Однако это нехорошо, в частности, потому, что эти команды широко используются при профилировании программ.

В практическом плане очень большой опасности эта проблема не создает, поскольку для атаки требуется сначала войти на сервер в качестве пользователя. Можно организовать работу так, чтобы не иметь пользователей на SSL- и Web-серверах, кроме root, nobody, apache и т. п. Впрочем, простейший выход на ближайшее время — вообще отключить HT (например, в BIOS). Это, как правило, не страшно — выигрыш за счет HT на большинстве приложений невелик. Выигрыш от HT может быть, например, при работе с базами данных. Некоторые приложения в многопользовательской среде даже проигрывают от использования HT, и этот режим могли уже отключить.

3.4.2. Криптография с открытым ключом

Алгоритмы криптографии с открытым ключом используют математические функции, отличные от подстановок и перестановок [19]. Но более важно то, что методы криптографии с открытым ключом являются асимметричными в том смысле, что они предполагают использование двух разных ключей, в отличие от методов симметричного шифрования, где предполагается только один ключ. Идея применения двух ключей повлекла глубокие изменения и в подходах к обеспечению конфиденциальности, и в области распределения ключей, и в процедурах аутентификации.

Но не должно быть заблуждений, касающихся шифрования с открытым ключом. Одним из таких заблуждений является утверждение, что шифрование с открытым ключом более защищено от криптоанализа, чем симметричное шифрование. На самом же деле защита любой схемы шифрования зависит от длины ключа и объема вычислительной работы, требуемой для взлома шифра. В этом смысле нет принципиального различия между симметричным шифрованием и шифрованием с открытым ключом, и ни одна из этих схем не имеет преимущества перед другой с точки зрения криптоанализа.

Вторым заблуждением является утверждение, что шифрование с открытым ключом оказывается универсальным подходом, делающим симметричное шифрование безнадежно устаревшим. Напротив, ввиду слишком высоких требований со стороны схем шифрования с открытым ключом к вычислительным ресурсам, отказ от схем симметричного шифрования кажется весьма маловероятным. Поэтому метод шифрования с открытым ключом ограничивается сферой управления ключами и приложениями цифровой подписи.

В-третьих, считается, что распределение ключей при шифровании с открытым ключом является тривиальной задачей по сравнению с достаточно запутанной процедурой квитирования (подтверждение установления связи), используемой в случае симметричного шифрования. На самом деле в случае шифрования с открытым ключом для этого требуется специальный протокол, вообще говоря, предполагающий существование некоторого центрального агента, а применяемые при этом процедуры не являются ни более простыми, ни более эффективными, чем те, которые требуются для традиционного шифрования.

Применение криптосистем с открытым ключом.

Криптосистемы с открытым ключом характеризуются использованием криптографического алгоритма с двумя ключами, один из которых остается в личном пользовании, а второй открыт для всех. В зависимости от приложения отправитель использует либо свой личный ключ, либо открытый ключ получателя, либо же оба, если требуется выполнить какую-то специальную криптографическую функцию. В самых широких пределах использование криптосистем с открытым ключом можно отнести к трем категориям.

■ Шифрование/дешифрование. Отправитель шифрует сообщение с использованием открытого ключа получателя.

■ Цифровая подпись. Отправитель «подписывает» сообщение с помощью своего личного ключа. Подпись получается в результате применения криптографического алгоритма к сообщению или к небольшому блоку данных, являющемуся функцией сообщения.

■ Обмен ключами. Две стороны взаимодействуют, чтобы обменяться сеансовым ключом. При этом возможно несколько различных подходов, предполагающих применение личных ключей одной или обеих сторон.

Условия применения методов криптографии с открытым ключом.

Криптосистема зависит от криптографического алгоритма, предполагающего применение двух связанных ключей. Диффи и Хеллман предположили без доказательства, что такие алгоритмы существуют. Однако они указали условия, которым должны удовлетворять такие алгоритмы [9]:

1. Для стороны В процесс генерирования пары ключей (открытый ключ KU_b , личный ключ KR_b) не должен вызывать вычислительных трудностей.

2. Для отправителя А не должен вызывать вычислительных трудностей процесс создания шифрованного текста при наличии открытого ключа и сообщения М, которое требуется зашифровать: $C = E_{KU_b}(M)$

3. Для получателя В не должен вызывать вычислительных трудностей процесс дешифрования полученного шифрованного текста с помощью личного ключа с целью восстановления оригинального сообщения: $M = D_{KR_b}(C)$.

4. Для противника должно быть невозможным с точки зрения вычислительных возможностей восстановление личного ключа KR_b из имеющегося открытого ключа KU_b .

5. Для противника должно быть невозможным с точки зрения вычислительных возможностей восстановление оригинального сообщения M из имеющихся открытого ключа KU_b и зашифрованного текста C .

К этим требованиям можно добавить еще одно, которое, хотя и представляется, в общем, полезным, не является необходимым для всех приложений, реализующих криптосистемы с открытым ключом.

6. Функции шифрования и дешифрования могут применяться в любом порядке:

Перечисленные требования в своей совокупности весьма сложны для выполнения, что, поэтому только один такой алгоритм получил широкое признание - RSA.

Чтобы понять это, эти требования в некотором более удобном виде. Эти требования сводятся к необходимости нахождения некоторой односторонней функции с лазейкой. *Односторонней функцией* называется функция, отображающая свои аргументы в некоторый диапазон значений так, что каждое значение функции имеет уникальное обратное значение, при этом значения функции вычислить легко, а обратные - практически невозможно:

$Y = f(X)$ - вычисляется легко;

$X = f^{-1}(Y)$ - практически не поддается вычислению.

(Не следует путать понятие односторонней функции с понятием односторонней функции хэширования - последняя предполагает в качестве аргумента произвольно большое поле данных и переводит его в некоторое фиксированное множество выводимых данных. Такие функции используются для аутентификации).

В общем случае термин "легко вычисляемый" означает, что проблема решается за полиномиальное время, рассматриваемое как функция длины вводимого значения. Так, если длина вводимого значения равна n битов, то время, требуемое для вычисления функции пропорционально n^a , где a является фиксированной константой. Такие алгоритмы называются алгоритмами, принадлежащими классу P . Термин «практически невычисляемый» обозначает более размытое понятие. В общем случае можно сказать, что функция является практически невычисляемой, если усилия по ее

вычислению возрастают быстрее, чем полиномиальная функция от длины вводимого значения. Например, если вводимое значение имеет длину p битов и время, требуемое для вычисления функции, пропорционально 2^n , то такая функция считается практически невычислимой. К сожалению, для каждого конкретного алгоритма очень непросто выяснить, отражает ли этот алгоритм указанную степень сложности. К тому же в определении обычного понятия вычислительной сложности алгоритма рассматриваются оценки сложности либо в наихудшем случае, либо в среднем. Для криптографии эти оценки бесполезны, криптография требует практической невычислимости обратной функции почти для любого вводимого значения, а не для наихудшего или среднего случая.

Вернемся к определению односторонней функции с лазейкой - такая функция предполагается легко вычислимой в одном направлении и практически невычислимой в другом в отсутствии дополнительной информации. При наличии дополнительной информацией обратная функция может быть вычислена за полиномиальное время. Подводя итог, можно сказать так: односторонние функции с лазейкой являются такими обратимыми функциями f_k , для которых:

$Y = f_k(X)$ - вычисляется легко, если известны K и X

$X = f_k^{-1}(Y)$ - вычисляется легко, если известны K и Y

$X = f_k^{-1}(Y)$ - практически не поддается вычислению, если Y известно, а K — нет.

Таким образом, для разработки практически применимой схемы шифрования с открытым ключом требуется найти подходящую одностороннюю функцию с лазейкой.

Криптоанализ схем шифрования с открытым ключом.

Как и в случае симметричного шифрования, схема шифрования с открытым ключом уязвима с точки зрения анализа с перебором всех ключей. И контрмеры здесь те же - использование длинных ключей. Однако в данном случае имеются и другие варианты защиты. Криптосистемы с открытым ключом зависят от некоторой обратимой математической функции со специальными свойствами. Сложность вычисления такого рода функций может зависеть не линейно от числа битов в ключе, а расти более быстро. Поэтому длина ключа должна быть достаточно большой для того, чтобы сделать анализ с перебором всех ключей практически невыполнимым, но достаточно малой для того, чтобы на практике

можно было использовать операции шифрования и дешифрования. Предлагаемые для использования на практике длины ключей, конечно же, обеспечивают практическую неэффективность анализа с перебором всех ключей, но при этом скорость шифрования/дешифрования оказывается слишком медленной для того, чтобы соответствующие алгоритмы можно было рекомендовать для универсального применения. Поэтому, как уже упоминалось выше, шифрование с открытым ключом в настоящее время ограничивается областями управления ключами и приложениями цифровой подписи.

Другой формой атаки является попытка найти способ вычисления личного ключа по известному открытому ключу. На сегодняшний день нет математического доказательства невозможности такой формы атаки ни для одного алгоритма шифрования с открытым ключом. С этой точки зрения любой конкретный алгоритм данного типа, включая широко распространенный алгоритм RSA, оказывается не внушающим доверия. А история криптографии показывает, что проблема, которая кажется неразрешимой, может оказаться вполне разрешимой, если посмотреть на нее с некоторой другой, совершенно новой точки зрения.

Наконец, существует форма атаки, применимая только к системам с открытым ключом. Эта форма, по существу, является формой анализа с вероятным текстом сообщения. Предположим, например, что должно быть отправлено сообщение, состоящее исключительно из 56-битового ключа DES. Противник может зашифровать все возможные ключи, используя открытый ключ, что позволит ему дешифровать подобное сообщение с помощью простого сравнения образцов с передаваемым зашифрованным текстом. В данном случае не имеет значения, насколько велика длина ключа схемы шифрования с открытым ключом - анализ сводится к простому перебору 56-битовых ключей. Возможности такого рода анализа можно воспрепятствовать присоединением к таким простым сообщениям случайных битов.

Алгоритм RSA.

Схема, разработанная Райвестом, Шамиром и Адлеманом, основана на выражениях со степенями. Открытый текст шифруется блоками, каждый из которых содержит двоичное значение, меньшее некоторого заданного числа n . Это значит, что длина блока должна

быть меньше или равна $\log_2(n)$. На практике длина блока выбирается равной 2^k битам, где $2^k < n \leq 2^{k+1}$. Шифрование и дешифрование для блока открытого текста M и блока шифрованного текста C можно представить в виде следующих формул:

$$C = M^e \bmod n,$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n.$$

Как отправитель, так и получатель должны знать значение n . Но только отправитель знает значение e , и только получателю известно значение d . Таким образом, данная схема является алгоритмом шифрования с открытым ключом $KU = \{e, n\}$ и личным ключом $KR = \{d, n\}$. Чтобы этот алгоритм мог использоваться для шифрования с открытым ключом, должны быть выполнены следующие требования.

1. Должны существовать такие значения e , d и n , что $M^{ed} = M \bmod n$ для всех $M < n$.
2. Должны относительно легко вычисляться M^e и C^d для всех значений $M < n$.
3. Должно быть практически невозможно определить d по имеющимся e и n .

Рассмотрим первое требование, а остальные рассмотрим позже. Необходимо найти соотношение вида: $M^{ed} = M \bmod n$.

Здесь используют следствие теоремы Эйлера п. 2.1.3 (см. уравнение (2.7)): для таких любых двух простых чисел p и q и таких любых двух целых чисел n и m , что $n = pq$ и $0 < m < n$, и произвольного целого числа k выполняются следующие соотношения: $m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$, где $\varphi(n)$ является функцией Эйлера, значение которой равно числу положительных целых чисел, меньших n и взаимно простых с n . Как показано в п.2.1.3, в случае простых p и q имеем: $\varphi(pq) = (p-1)(q-1)$. Поэтому требуемое отношение получается при условии: $ed = k\varphi(n) + 1$.

Это эквивалентно следующим соотношениям:

$ed \equiv 1 \bmod \varphi(n)$, $d \equiv e^{-1} \bmod \varphi(n)$, т.е. e и d являются взаимно обратными по модулю $\varphi(n)$. Обратите внимание, что в соответствии с правилами арифметики в классах вычетов это может иметь место только тогда, когда d (а, следовательно, и e) является взаимно простым с $\varphi(n)$. В эквивалентной записи $\text{НОД}(\varphi(n), d) = 1$.

Теперь у нас есть все, чтобы представить схему RSA. Компонентами схемы являются:

p и q - два простых числа (секретные, выбираются);

$n = pq$ - (открытое, вычисляется),

такое e , что $\text{НОД}(\varphi(n), e) = 1$, $1 < e < \varphi(n)$. (открытое, выбирается);

$d = e^{-1} \bmod \varphi(n)$ - (секретное, вычисляется).

Личный ключ складывается из $\{d, n\}$, а открытый — из $\{e, n\}$.

Предположим, что пользователь А опубликовал свой открытый ключ и теперь пользователь В собирается переслать ему сообщение М. Тогда пользователь В вычисляет $C = M^e \bmod n$ и пересылает С. Получив этот зашифрованный текст, пользователь А дешифрует его, вычисляя $M = C^d \bmod n$.

При выборе размера n были обнаружены ряд ограничений. Чтобы избежать выбора значений n , которые могут быть разложены на множители с меньшими усилиями, должны быть ограничения на p и q :

1. Значения p и q должны различаться по длине всего на несколько разрядов. Например, и p , и q должны попадать в диапазон от 10^{76} до 10^{100} ;

2. Как $(p - 1)$, так и $(q - 1)$ должны содержать в своих разложениях достаточно большой простой множитель;

3. $\text{НОД}(p - 1, q - 1)$ должен быть достаточно малым.

Кроме того, было показано, что если $e < n$ и $d < n^{1/2}$, то d можно определить достаточно легко.

3.4.3. Аутентификация

Основные типы нарушения защиты [19]:

1. Раскрытие содержимого. Открытие содержимого сообщения любому лицу или процессу, не владеющему соответствующим криптографическим ключом.

2. Анализ потока данных. Раскрытие структуры потока обмена данными участвующих в таком обмене сторон. В случае ориентированного на установление логических соединений приложения может быть определена частота и длительность соединений. И в среде, ориентированной на установление логических соединений, и при отсутствии таковых может быть определено число и длина сообщений, пересылаемых участвующими в обмене сторонами.

3. Имитация. Внедрение в поток сообщений от ложного источника. Здесь подразумевается и создание сообщений

противником, выдаваемых им за сообщения от уполномоченного объекта, и обманные подтверждения получения или неполучения сообщения лицом, не являющимся истинным адресатом сообщения.

4. Модификация содержимого. Изменение содержимого сообщения, включая вставку, удаление, реорганизацию или любую другую модификацию сообщения.

5. Модификация последовательности сообщений. Любая модификация последовательности сообщений, формирующих поток обмена данными, включая вставку, удаление или изменение порядка следования сообщений.

6. Модификация временных характеристик. Задержка или воспроизведение сообщений. В случае ориентированного на установление логических соединений приложения весь сеанс или некоторая последовательность сообщений может быть воспроизведением некоторого ранее осуществленного реального сеанса или некоторой последовательности ранее переданных сообщений с определенными задержками во времени или повторениями. В приложении без установления соединений можно задержать или воспроизвести отдельное сообщение (например, дейтаграмму).

7. Отречение. Отрицание получения сообщения адресатом или отрицание факта передачи сообщения источником.

Меры, принимаемые в связи с первыми двумя типами атаки, относятся к конфиденциальности (п.3.4.1). Меры, принимаемые в связи с нарушениями, указанными в пунктах 3-6 приведенного выше списка, относятся к вопросам аутентификации сообщений. Механизмы решения проблем, возникающих в связи с атаками, представленными в п. 7, относятся к проблеме использования цифровых подписей, но, вообще, средства цифровой подписи учитывают многие вопросы, вытекающие из рассмотрения пунктов 3-6.

Рассмотрим аутентификацию. В аутентификации сообщений и средствах цифровой подписи могут быть выделены два основных уровня. На низшем уровне должна выполняться некоторая функция, порождающая аутентификатор (удостоверение) - значение, используемое для аутентификации сообщения. Результат выполнения этой функции низшего уровня затем используется как примитив в протоколе аутентификации высшего уровня, дающем получателю сообщения возможность проверить достоверность сообщения.

Какие же это функции? Такие функции можно разделить на три класса [19]:

- Шифрование сообщения. В качестве аутентификатора используется шифрованный текст всего сообщения.

- Код аутентичности сообщения (Message Authentication Code - MAC). В качестве аутентификатора выступает значение фиксированной длины, генерируемое некоторой открытой функцией сообщения и секретным ключом.

- Функция хэширования. В качестве аутентификатора используется значение, генерируемое некоторой открытой функцией, противопоставляющей любому сообщению произвольной длины значение фиксированной длины, называемое значением хэш-функции.

Рассмотрим их вкратце.

Шифрование сообщения само по себе в некоторой мере может выполнять функции аутентификации сообщения.

Альтернативная техника аутентификации предполагает присоединение к сообщению созданного с использованием секретного ключа небольшого блока данных фиксированного размера, обычно называемого криптографической контрольной суммой, или кодом аутентичности сообщения (MAC - Message Authentication Code). При этом предполагается, что две участвующие в обмене данных стороны, скажем А и В, используют общий секретный ключ К. Чтобы послать сообщение М адресату В, отправитель А вычисляет код аутентичности сообщения как функцию сообщения и ключа: $MAC = C_K(M)$. Сообщение с добавленным к нему значением MAC пересылается адресату. Получатель выполняет аналогичные вычисления с полученным сообщением, используя тот же секретный ключ, чтобы вычислить новое значение MAC.

Вычисленное значение MAC сравнивается с полученным вместе с сообщением. Функция вычисления MAC подобна по своим действиям шифрованию. Разница лишь в том, что для алгоритма вычисления MAC не требуется свойство обратимости, как для алгоритма шифрования, чтобы можно было дешифровать сообщение. Оказывается, что такие математические свойства функции аутентификации делают ее менее уязвимой ко взлому по сравнению с функцией шифрования.

Вариацией идеи использования кодов аутентичности сообщений является односторонняя функция хэширования. Как и в

случае кодов аутентичности сообщений, функция хэширования получает на вход сообщение M произвольной длины, а на выход выдает хэш-код $H(M)$ фиксированного размера, иногда называемый профилем сообщения. Хэш-код является функцией всех битов сообщения и обеспечивает контроль ошибок: изменение любого числа битов в сообщении выливается в изменение хэш-кода. Целью использования функции хэширования является получение «дактилоскопической» характеристики файла, сообщения или вообще любого блока данных. Чтобы оказаться полезной для аутентификации сообщений, функция хэширования H должна иметь следующие свойства:

1. Быть применимой к блоку данных любой длины.
2. Давать на выходе значение фиксированной длины.
3. Значение $H(x)$ должно вычисляться относительно легко для любого заданного x , а алгоритм вычисления должен быть практичным с точки зрения как аппаратной, так и программной реализации.
4. Для любого данного кода h должно быть практически невозможно вычислить x , для которого $H(x) = h$. Такое свойство иногда называют односторонностью.
5. Для любого данного блока x должно быть практически невозможно вычислить $y \neq x$, для которого $H(x) = H(y)$. Такое свойство иногда называют слабой сопротивляемостью коллизиям.
6. Должно быть практически невозможно вычислить любую пару различных значений x и y , для которых $H(x) = H(y)$. Такое свойство иногда называют сильной сопротивляемостью коллизиям.

Первые три из указанных здесь свойств описывают требования, обеспечивающие возможность практического применения функции хэширования для аутентификации сообщений.

Четвертое свойство обеспечивает односторонность: легко получить код на основе имеющегося сообщения, но практически невозможно воссоздать сообщение, имея только соответствующий код. Это свойство важно тогда, когда алгоритм аутентификации предполагает использование секретного значения. Само секретное значение непосредственно не пересылается, но если функция хэширования не является односторонней, то противник может определить секретное значение достаточно легко: при возможности наблюдать или перехватывать поток данных он получит в распоряжение сообщение M и хэш-код $C = H(S_{AB}||M)$. Затем он

рассмотрит функцию, обратную функции хэширования, и получит $S_{AB} \parallel M = H^{-1}(C)$. Теперь, когда противник имеет и M , и $S_{AB} \parallel M$, восстановить значение S_{AB} не составит для него никакого труда.

Пятое свойство гарантирует то, что не удастся найти другое сообщение, дающее в результате хэширования то же самое значение, что и данное сообщение. Это предотвращает возможность фальсификации сообщения в том случае, когда выполняется шифрование хэш-кода.

Шестое свойство определяет стойкость функции хэширования к конкретному классу атак, известных под названием атак, построенных на парадоксе задачи о днях рождения.

3.4.4. Электронные цифровые подписи

Важнейшей областью применения криптографии с открытым ключом являются цифровые подписи.

Основные требования к цифровой подписи [19]:

- Подпись должна быть двоичным кодом, который зависит от подписываемого сообщения;
- Подпись должна использовать некоторую информацию, уникальную для отправителя, чтобы предотвратить возможность как фальсификации, так и отрицания авторства.
- Цифровую подпись должно быть относительно просто произвести.
- Цифровую подпись должно быть относительно просто распознать и проверить.
- С точки зрения вычислений должно быть нереально фальсифицировать цифровую подпись ни с помощью создания нового сообщения для имеющейся цифровой подписи, ни с помощью создания фальшивой цифровой подписи для имеющегося сообщения.
- Экземпляр цифровой подписи должно быть удобно хранить в запоминающем устройстве

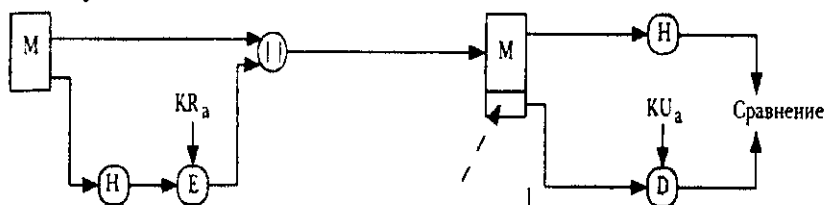
Национальный институт стандартов и технологии (NIST) опубликовал федеральный стандарт обработки информации FIPS PUB 186, известный также как DSS (Digital Signature Standard стандарт цифровой подписи). Стандарт DSS основан на алгоритме хэширования SHA (Secure Hash Algorithm — защищенный алгоритм хэширования) и представляет новую технологию использования цифровой подписи - алгоритм DSA (Digital Signature Algorithm -

алгоритм цифровой подписи). Стандарт DSS был предложен в 1991 г., а его исправленная версия — в 1993 г. в ответ на возникшие сомнения в безопасности соответствующей схемы. В 1996 году в него были внесены незначительные изменения.

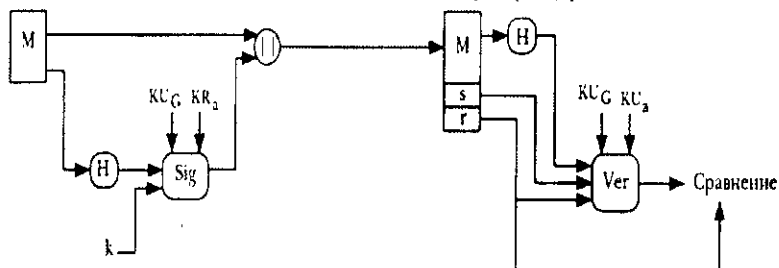
Подход DSS.

В стандарте DSS используется алгоритм, призванный обеспечить только функцию цифровой подписи. В отличие от RSA данный алгоритм не может служить для шифрования или обмена ключами.

На рис. 3.38 сравниваются схемы генерирования цифровых подписей с использованием DSS и RSA. При подходе на основе RSA сообщение, которое должно быть подписано, поступает на вход функции хэширования, которая выдает защищенный хэш-код фиксированной длины. Этот хэш-код шифруется затем личным ключом отправителя, в результате чего и получается подпись. После этого передаются и сообщение, и его подпись. Получатель принимает сообщение и вычисляет хэш-код. Кроме того, он дешифрует подпись, используя открытый ключ отправителя. Если вычисленный хэш-код соответствует дешифрованной подписи, подпись считается подлинной. Поскольку только отправитель знает свой личный ключ, подлинную подпись может поставить только он.



(а) Подход RSA $E_{KR_a}[H(M)]$



(б) Подход DSS

Рис. 3.38. Два подхода к использованию цифровых подписей

Подход DSS также основан на функции хэширования. Хэш-код подается на вход функции создания подписи вместе со случайным числом k , специально генерируемым для данной подписи. Функция создания подписи зависит также от личного ключа отправителя KR_a и ряда параметров, известных группе общающихся сторон. Можно считать, что это множество составляет глобальный открытый ключ KU_G . В результате получается подпись, складывающаяся из двух компонентов, обозначаемых s и r .

В пункте назначения генерируется хэш-код поступившего сообщения. Этот код и подпись подаются на вход функции верификации. Функция верификации зависит также от глобального открытого ключа и от открытого ключа отправителя KU_a , соответствующего личному ключу отправителя. Если подпись является подлинной, то на выходе функции верификации получается значение, совпадающее с компонентом r подписи. Функция создания подписи такова, что только отправитель, зная свой личный ключ, может создать правильную подпись. Криптостойкость цифровой подписи – в вычислении дискретных логарифмов.

Алгоритм цифровой подписи.

Алгоритм цифровой подписи создан с учетом трудностей вычисления дискретных логарифмов [19].

В алгоритме три параметра, являющиеся открытыми. Выбирается 160-битовое простое число q , а затем выбирается такое простое число p длиной между 512 и 1024 битами, что q делит $(p - 1)$. Далее выбирается число $g = h^{(p-1)/q} \bmod p$, где h является целым числом между 1 и $(p - 1)$ с тем ограничением, что g должен быть больше 1.

Имея эти числа, каждый пользователь выбирает личный ключ (x) и генерирует открытый ключ (y). Личный ключ (x) должен быть числом от 1 до $(q - 1)$ и должен выбираться случайным или псевдослучайным образом. Открытый ключ вычисляется на основе личного ключа по формуле $y = g^x \bmod p$. Вычислить (y) по имеющемуся значению x относительно просто. А вот вычислить x по имеющемуся значению y – достаточно сложно, так как потребуется вычислить дискретный логарифм y по основанию g и по модулю p .

Для создания цифровой подписи пользователь вычисляет два параметра: r и s , являющиеся функциями компонентов открытого ключа (p, q, g), личного ключа пользователя (x), хэш-кода сообщения ($H(M)$) и некоторого целого числа k , которое выбирается случайным или псевдослучайным образом (оно уникально для каждой подписи).

4. ПОСТРОЕНИЕ И ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Построение систем защиты информации в информационных системах

4.1.1. Концепция и этапы создания защищенных информационных систем

При разработке и построении системы защиты информации в информационных системах необходимо придерживаться определенных методологических принципов проведения исследований, проектирования, производства, эксплуатации и развития таких систем. Системы защиты информации (СЗИ) относятся к классу сложных систем и для их построения могут использоваться основные принципы построения сложных систем с учетом специфики решаемых задач [5]:

- ◆ параллельная разработка ИС и СЗИ;
- ◆ системный подход к построению защищенных ИС;
- ◆ многоуровневая структура СЗИ;
- ◆ иерархическая система управления СЗИ;
- ◆ блочная архитектура защищенных ИС;
- ◆ возможность развития СЗИ;
- ◆ дружественный интерфейс защищенных ИС с пользователями и обслуживающим персоналом.

Первый из приведенных принципов построения СЗИ требует проведения одновременной *параллельной разработки ИС и механизмов защиты*. Только в этом случае возможно эффективно обеспечить реализацию всех остальных принципов. Причем в процессе разработки защищенных ИС должен соблюдаться разумный компромисс между созданием встроенных неразделимых механизмов защиты и блочных унифицированных средств и процедур защиты. Только на этапе разработки ИС можно полностью учесть взаимное влияние блоков и устройств собственно ИС и механизмов защиты, добиться системности защиты оптимальным образом.

Принцип системности является одним из основных концептуальных и методологических принципов построения защищенных ИС. Он предполагает:

- ♦ анализ всех возможных угроз безопасности информации;
- ♦ обеспечение защиты на всех жизненных циклах ИС;
- ♦ защиту информации во всех звеньях ИС;
- ♦ комплексное использование механизмов защиты.

Потенциальные угрозы выявляются в процессе создания и исследования модели угроз. В результате исследований должны быть получены данные о возможных угрозах безопасности информации, о степени их опасности и вероятности реализации. При построении СЗИ учитываются потенциальные угрозы, реализация которых может привести к существенному ущербу и вероятность таких событий не является очень близкой к нулю.

Защита ресурсов ИС должна осуществляться на этапах разработки, производства, эксплуатации и модернизации, а также по всей технологической цепочке ввода, обработки, передачи, хранения и выдачи информации. Реализация этих принципов позволяет обеспечить создание СЗИ, в которой отсутствуют слабые звенья как на различных жизненных циклах ИС, так и в любых элементах и режимах работы ИС.

Механизмы защиты, которые используются при построении защищенных систем, должны быть взаимосвязаны по месту, времени и характеру действия. Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых. Любая, даже простая СЗИ является комплексной.

Система защиты информации должна иметь несколько уровней, перекрывающих друг друга, т. е. такие системы целесообразно строить по принципу построения матрешек.

Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни защиты (рис. 4.1).



Рис. 4.1. Многоуровневая СЗИ

Например, для отдельного объекта ИС можно выделить 6 уровней (рубежей) защиты:

1. Охрана по периметру территории объекта;
2. Охрана по периметру здания;
3. Охрана помещения;
4. Защита аппаратных средств;
5. Защита программных средств;
6. Защита информации.

Системы защиты информации ИС всегда должны иметь *централизованное управление*. В распределенных ИС управление защитой может осуществляться по иерархическому принципу. Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках предприятия, организации, корпорации, министерства. Для осуществления централизованного управления в СЗИ должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа, изготовления атрибутов идентификации и другие.

Одним из важных принципов построения защищенных ИС является использование *блочной архитектуры*. Применение данного принципа позволяет получить целый ряд преимуществ:

- ♦ упрощается разработка, отладка, контроль и верификация устройств (программ, алгоритмов);
- ♦ допускается параллельность разработки блоков;
- ♦ используются унифицированные стандартные блоки;
- ♦ упрощается модернизация систем;
- ♦ удобство и простота эксплуатации.

Основываясь на принципе блочной архитектуры защищенной ИС, можно представить структуру идеальной защищенной системы. В такой системе имеется минимальное ядро защиты, отвечающее нижней границе защищенности систем определенного класса (например, ПЭВМ). Если в системе необходимо обеспечить более высокий уровень защиты, то это достигается за счет согласованного подключения аппаратных блоков или инсталляции дополнительных программных средств.

В случае необходимости могут быть использованы более совершенные блоки ИС, чтобы не допустить снижения эффективности применения системы по прямому назначению. Это объясняется потреблением части ресурсов ИС вводимыми блоками защиты.

Стандартные входные и выходные интерфейсы блоков позволяют упростить процесс модернизации СЗИ, альтернативно использовать аппаратные или программные блоки. Здесь просматривается аналогия с семиуровневой моделью OSI.

При разработке сложной ИС, например, вычислительной сети, необходимо предусматривать *возможность ее развития* в двух направлениях: увеличения числа пользователей и наращивания возможностей сети по мере совершенствования информационных технологий.

С этой целью при разработке ИС предусматривается определенный запас ресурсов по сравнению с потребностями на момент разработки. Наибольший запас производительности необходимо предусмотреть для наиболее консервативной части сложных систем - каналов связи. Часть резерва ресурсов ИС может быть востребована при развитии СЗИ. На практике резерв ресурсов, предусмотренный на этапе разработки, исчерпывается уже на момент полного ввода в эксплуатацию сложных систем. Поэтому при разработке ИС предусматривается возможность модернизации системы. В этом смысле сложные системы должны быть развивающимися или открытыми. Термин открытости в этой трактовке относится и к защищенным ИС. Причем механизмы защиты, постоянно совершенствуясь, вызывают необходимость наращивания ресурсов ИС. Новые возможности, режимы ИС, а также появление новых угроз в свою очередь стимулируют развитие новых механизмов защиты. Важное место в процессе создания открытых систем играют международные стандарты в области взаимодействия устройств, подсистем. Они позволяют использовать подсистемы различных типов, имеющих стандартные интерфейсы взаимодействия.

Система защиты информации ИС должна быть:

1. Дружественной по отношению к пользователям и обслуживающему персоналу;
2. Максимально автоматизирована и не должна требовать от пользователя выполнять значительный объем действий, связанных с СЗИ;
3. Не должна создавать ограничений в выполнении пользователем своих функциональных обязанностей.

В СЗИ необходимо предусмотреть меры снятия защиты с отказавших устройств для восстановления их работоспособности. Система защиты информации должна создаваться совместно с

создаваемой информационной системой. При построении системы защиты могут использоваться существующие средства защиты, или же они разрабатываются специально для конкретной ИС. В зависимости от особенностей информационной системы, условий ее эксплуатации и требований к защите информации процесс создания СЗИ может не содержать отдельных этапов, или содержание их может несколько отличаться от общепринятых норм при разработке сложных аппаратно-программных систем. Но обычно разработка таких систем включает следующие этапы:

- ◆ разработка технического задания;
- ◆ эскизное проектирование;
- ◆ техническое проектирование;
- ◆ рабочее проектирование;
- ◆ производство опытного образца.

Одним из основных этапов разработки СЗИ является этап разработки технического задания. Именно на этом этапе решаются практически все специфические задачи, характерные именно для разработки СЗИ.

Процесс разработки систем, заканчивающийся выработкой технического задания, называют научно-исследовательской разработкой, а остальную часть работы по созданию сложной системы называют опытно-конструкторской разработкой. Опытно-конструкторская разработка аппаратно-программных средств ведется с применением систем автоматизации проектирования, алгоритмы проектирования хорошо изучены и отработаны. Поэтому особый интерес представляет рассмотрение процесса научно - исследовательского проектирования.

4.1.2. Техническое задание на проектирование защищенной информационной системы

Целью этого этапа является разработка технического задания на проектирование СЗИ [5]. Техническое задание содержит основные технические требования к разрабатываемой СЗИ, а также согласованные взаимные обязательства заказчика и исполнителя разработки. Технические требования определяют значения основных технических характеристик, выполняемые функции, режимы работы, взаимодействие с внешними системами и т. д.

Аппаратные средства оцениваются следующими характеристиками: быстродействие, производительность, емкость

запоминающих устройств, разрядность, стоимость, характеристики надежности и др. Программные средства характеризуются требуемым объемом оперативной и внешней памяти, системой программирования, в которой разработаны эти средства, совместимостью с ОС и другими программными средствами, временем выполнения, стоимостью и т. д.

Получение значений этих характеристик, а также состава выполняемых функций и режимов работы средств защиты, порядка их использования и взаимодействия с внешними системами составляют основное содержание этапа научно-исследовательской разработки. Для проведения исследований на этом этапе заказчик может привлекать исполнителя или научно-исследовательское учреждение, либо организует совместную их работу.

Научно-исследовательская разработка начинается с анализа угроз безопасности информации, анализа защищаемой ИС и анализа конфиденциальности и важности информации в ИС (рис. 4.2).

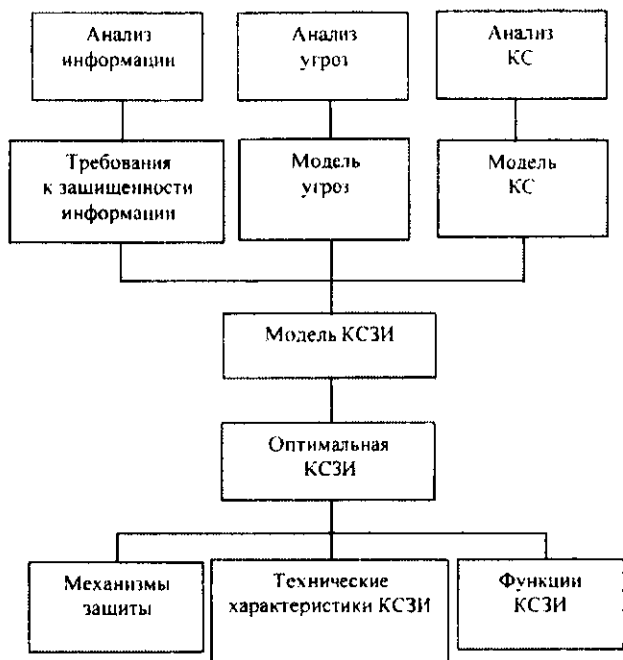


Рис. 4.2. Последовательность и содержание научно-исследовательской разработки СЗИ

Прежде всего производится анализ конфиденциальности и важности информации, которая должна обрабатываться, храниться и передаваться в ИС. На основе анализа делается вывод о целесообразности создания СЗИ. Если информация не является конфиденциальной и легко может быть восстановлена, то создавать СЗИ нет необходимости. Не имеет смысла также создавать СЗИ в ИС, если потеря целостности и конфиденциальности информации связана с незначительными потерями.

В этих случаях достаточно использовать штатные средства ИС и, возможно, страхование от утраты информации.

При анализе информации определяются потоки конфиденциальной информации, элементы ИС, в которых она обрабатывается и хранится. На этом этапе рассматриваются также вопросы разграничения доступа к информации отдельных пользователей и целых сегментов ИС. На основе анализа информации определяются требования к ее защищенности. Требования задаются путем присвоения определенного грифа конфиденциальности, установления правил разграничения доступа.

Очень важная исходная информация для построения СЗИ получается в результате анализа защищаемой ИС. Так как СЗИ является подсистемой ИС, то взаимодействие системы защиты с ИС можно определить как внутреннее, а взаимодействие с внешней средой - как внешнее (рис. 4.3).

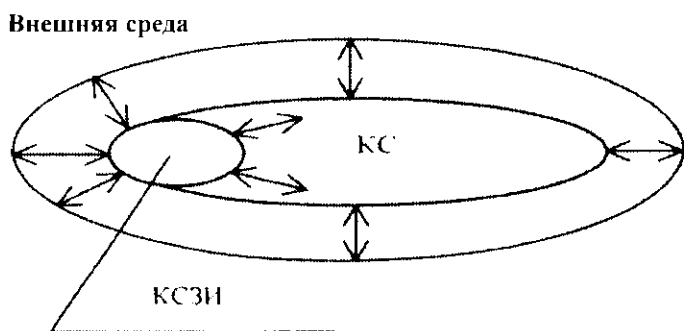


Рис. 4.3. Схема взаимодействия СЗИ

Внутренние условия взаимодействия определяются архитектурой ИС. При построении СЗИ учитываются:

- ♦ географическое положение ИС;

- ♦ тип ИС (распределенная или сосредоточенная);
- ♦ структуры ИС (техническая, программная, информационная и т. д.);

- ♦ производительность и надежность элементов ИС;
- ♦ типы используемых аппаратных и программных средств и режимы их работы;

- ♦ угрозы безопасности информации, которые порождаются внутри ИС (отказы аппаратных и программных средств, алгоритмические ошибки и т. п.).

Учитываются следующие внешние условия:

- ♦ взаимодействие с внешними системами;
- ♦ случайные и преднамеренные угрозы.

Анализ угроз безопасности является одним из обязательных условий построения СЗИ. По результатам проведенного анализа строится модель угроз безопасности информации в ИС. Модель угроз безопасности информации в ИС содержит систематизированные данные о случайных и преднамеренных угрозах безопасности информации в конкретной ИС. Систематизация данных модели предполагает наличие сведений обо всех возможных угрозах, их опасности, временных рамках действия, вероятности реализации. Часто модель угроз рассматривается как композиция модели злоумышленника и модели случайных угроз. Модели представляются в виде таблиц, графов или на вербальном уровне. При построении модели злоумышленника используются два подхода:

1. Модель ориентируется только на высококвалифицированного злоумышленника-профессионала, оснащенного всем необходимым и имеющего легальный доступ на всех рубежах защиты;

2. Модель учитывает квалификацию злоумышленника, его оснащенность (возможности) и официальный статус в ИС.

Первый подход проще реализуется и позволяет определить верхнюю границу преднамеренных угроз безопасности информации.

Второй подход отличается гибкостью и позволяет учитывать особенности ИС в полной мере. Градация злоумышленников по их квалификации может быть различной. Например, может быть выделено три класса злоумышленников:

1. Высококвалифицированный злоумышленник-профессионал;
2. Квалифицированный злоумышленник-непрофессионал;
3. Неквалифицированный злоумышленник-непрофессионал.

Класс злоумышленника, его оснащенность и статус на объекте ИС определяют возможности злоумышленника по несанкционированному доступу к ресурсам ИС.

Угрозы, связанные с непреднамеренными действиями, хорошо изучены, и большая часть их может быть формализована. Сюда следует отнести угрозы безопасности, которые связаны с конечной надежностью технических систем. Угрозы, порождаемые стихией или человеком, формализовать сложнее. Но с другой стороны, по ним накоплен большой объем статистических данных. На основании этих данных можно прогнозировать проявление угроз этого класса.

Модель злоумышленника и модель случайных угроз позволяют получить полный спектр угроз и их характеристик. В совокупности с исходными данными, полученными в результате анализа информации, особенностей архитектуры проектируемой КС, модели угроз безопасности информации позволяют получить исходные данные для построения модели СЗИ.

4.1.3. Моделирование, выбор показателей эффективности и критериев оптимальности защищенной информационной системы

Оценка эффективности функционирования СЗИ представляет собой сложную научно-техническую задачу. СЗИ оценивается в процессе разработки ИС, в период эксплуатации и при создании (модернизации) СЗИ для уже существующих ИС. При разработке сложных систем распространенным методом проектирования является синтез с последующим анализом. Система синтезируется путем согласованного объединения блоков, устройств, подсистем и анализируется (оценивается) эффективность полученного решения. Из множества синтезированных систем выбирается лучшая по результатам анализа, который осуществляется с помощью моделирования [5].

Моделирование СЗИ заключается в построении образа (модели) системы, с определенной точностью воспроизводящего процессы, происходящие в реальной системе [1,2]. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Для оценки систем используются аналитические и имитационные модели. В *аналитических моделях* функционирование исследуемой системы записывается в виде математических или

логических соотношений. Для этих целей используется мощный математический аппарат: алгебра, функциональный анализ, разностные уравнения, теория вероятностей, математическая статистика, теория множеств, теория массового обслуживания и т. д.

При *имитационном моделировании* моделируемая система представляется в виде некоторого аналога реальной системы. В процессе имитационного моделирования на ЭВМ реализуются алгоритмы изменения основных характеристик реальной системы в соответствии с эквивалентными реальным процессам математическими и логическими зависимостями.

Модели делятся также на детерминированные и стохастические. Модели, которые оперируют со случайными величинами, называются *стохастическими*. Так как на процессы защиты информации основное влияние оказывают случайные факторы, то модели систем защиты являются стохастическими.

Моделирование СЗИ является сложной задачей, потому что такие системы относятся к классу сложных организационно-технических систем, которым присущи следующие особенности [1,2]:

- ♦ сложность формального представления процессов функционирования таких систем, главным образом, из-за сложности формализации действий человека;

- ♦ многообразие архитектур сложной системы, которое обуславливается многообразием структур ее подсистем и множественностью путей объединения подсистем в единую систему;

- ♦ большое число взаимосвязанных между собой элементов и подсистем;

- ♦ сложность функций, выполняемых системой;

- ♦ функционирование систем в условиях неполной определенности и случайности процессов, оказывающих воздействие на систему;

- ♦ наличие множества критериев оценки эффективности функционирования сложной системы;

- ♦ существование интегрированных признаков, присущих системе в целом, но не свойственных каждому элементу в отдельности (например, система с резервированием является надежной, при ненадежных элементах);

- ♦ наличие управления, часто имеющего сложную иерархическую структуру;

- ♦ разветвленность и высокая интенсивность информационных потоков.

Для преодоления этих сложностей применяются:

1. Специальные методы неформального моделирования.
2. Декомпозиция общей задачи на ряд частных задач.
3. Макромоделирование.

Рассмотрим эти методы:

1. Специальные методы неформального моделирования.

Специальные методы неформального моделирования основаны на применении неформальной теории систем. Основными составными частями неформальной теории систем являются [5]:

- ♦ структурирование архитектуры и процессов функционирования сложных систем;
- ♦ неформальные методы оценивания;
- ♦ неформальные методы поиска оптимальных решений.

Структурирование является развитием формального описания систем, распространенного на организационно-технические системы.

Примером структурированного процесса является конвейерное производство. В основе такого производства лежат два принципа:

- ♦ строгая регламентация технологического процесса производства;
- ♦ специализация исполнителей и оборудования.

Предполагается, что конструкция производимой продукции отвечает следующим требованиям:

- ♦ изделие состоит из конструктивных иерархических элементов (блоков, узлов, схем, деталей и т.п.);
- ♦ максимальная простота, унифицированность и стандартность конструктивных решений и технологических операций.

В настоящее время процесс производства технических средств ИС достаточно полно структурирован. Структурное программирование также вписывается в рамки структурированных процессов. На основе обобщения принципов и методов структурного программирования могут быть сформулированы условия структурированного описания изучаемых систем и процессов их функционирования [5]:

1. Полнота отображения основных элементов и их взаимосвязей;
2. Адекватность;
3. Простота внутренней организации элементов описания и взаимосвязей элементов между собой;

4.Стандартность и унифицированность внутренней структуры элементов и структуры взаимосвязей между ними;

5.Модульность;

6.Гибкость, под которой понимается возможность расширения и изменения структуры одних компонентов модели без существенных изменений других компонентов;

7.Доступность изучения и использования модели любому специалисту средней квалификации соответствующего профиля.

В процессе проектирования систем необходимо получить их характеристики. Некоторые характеристики могут быть получены путем измерения. Другие получаются с использованием аналитических соотношений, а также в процессе обработки статистических данных. Однако существуют характеристики сложных систем, которые не могут быть получены приведенными методами. К таким характеристикам СЗИ относятся вероятности реализации некоторых угроз, отдельные характеристики эффективности систем защиты и другие.

Указанные характеристики могут быть получены единственно доступными методами - методами *неформального оценивания*. Сущность методов заключается в привлечении для получения некоторых характеристик специалистов-экспертов в соответствующих областях знаний.

Наибольшее распространение из неформальных методов оценивания получили методы экспертных оценок. Метод экспертных оценок представляет собой алгоритм подбора специалистов - экспертов, задания правил получения независимых оценок каждым экспертом и последующей статистической обработки полученных результатов. Методы экспертных оценок используются давно, хорошо отработаны. В некоторых случаях они являются единственно возможными методами оценивания характеристик систем.

Неформальные методы поиска оптимальных решений могут быть распределены по двум группам:

- ♦ методы неформального сведения сложной задачи к формальному описанию и решение задачи формальными методами;

- ♦ неформальный поиск оптимального решения.

Для моделирования систем защиты информации целесообразно использовать следующие теории и методы, позволяющие свести решение задачи к формальным алгоритмам:

- ♦ теория нечетких множеств;

- ♦ теория конфликтов;

- ♦ теория графов;
- ♦ формально-эвристические методы;
- ♦ эволюционное моделирование.

Методы *теории нечетких множеств* [4] позволяют получать аналитические выражения для количественных оценок нечетких условий принадлежности элементов к тому или иному множеству. Теория нечетких множеств хорошо согласуется с условиями моделирования систем защиты, так как многие исходные данные моделирования (например, характеристики угроз и отдельных механизмов защиты) не являются строго определенными.

Теория конфликтов является относительно новым направлением исследования сложных человеко-машинных систем. Конфликт между злоумышленником и системой защиты, разворачивающийся на фоне случайных угроз, является классическим для применения теории конфликта. Две противоборствующие стороны преследуют строго противоположные цели. Конфликт развивается в условиях неоднозначности и слабой предсказуемости процессов, способности сторон оперативно изменять цели. Теория конфликтов является развитием теории игр. Теория игр позволяет:

- ♦ структурировать задачу, представить ее в обозримом виде, найти области количественных оценок, упорядочений, предпочтений, выявить доминирующие стратегии, если они существуют;
- ♦ до конца решить задачи, которые описываются стохастическими моделями.

Теория игр позволяет найти решение, оптимальное или рациональное в среднем. Она исходит из принципа минимизации среднего риска. Такой подход не вполне адекватно отражает поведение сторон в реальных конфликтах, каждый из которых является уникальным. В теории конфликтов предпринята попытка преодоления этих недостатков теории игр. Теория конфликтов позволяет решать ряд практических задач исследования сложных систем. Однако она еще не получила широкого распространения и открыта для дальнейшего развития.

Из *теории графов* для исследования систем защиты информации в наибольшей степени применим аппарат сетей Петри. Управление условиями в узлах сети Петри позволяет моделировать процессы преодоления защиты злоумышленником. Аппарат сетей Петри позволяет формализовать процесс исследования эффективности СИ.

К *формально-эвристическим методам* отнесены методы поиска оптимальных решений не на основе строгих математических, логических соотношений, а основываясь на опыте человека, имеющихся знаниях и интуиции. Получаемые решения могут быть далеки от оптимальных, но они всегда будут лучше решений, получаемых без эвристических методов.

Наибольшее распространение из эвристических методов получили лабиринтные и концептуальные методы.

В соответствии с лабиринтной моделью задача представляется человеку в виде лабиринта возможных путей решения. Предполагается, что человек обладает способностью быстрого отсеивания бесперспективных путей движения по лабиринту. В результате среди оставшихся путей с большой вероятностью находится путь, ведущий к решению поставленной задачи.

Концептуальный метод предполагает выполнение действий с концептами. Под концептами понимаются обобщенные элементы и связи между ними. Концепты получаются человеком, возможно и неосознанно, в процессе построения структурированной модели. В соответствии с концептуальным методом набор концепт универсален и ему соответствуют имеющиеся у человека механизмы вычисления, трансформации и формирования отношений. Человек проводит мысленный эксперимент со структурированной моделью и порождает ограниченный участок лабиринта, в котором уже несложно найти решение.

Эволюционное моделирование представляет собой разновидность имитационного моделирования. Особенность его заключается в том, что в процессе моделирования совершенствуется алгоритм моделирования.

Сущность неформальных методов непосредственного поиска оптимальных решений состоит в том, что человек участвует не только в построении модели, но и в процессе ее реализации.

2. Декомпозиция общей задачи оценки эффективности функционирования СЗИ.

Сложность выполняемых функций, значительная доля нечетко определенных исходных данных, большое количество механизмов защиты, сложность их взаимных связей и многие другие факторы делают практически неразрешимой проблему оценки эффективности системы в целом с помощью одного какого-либо метода моделирования.

Для решения этой проблемы применяется метод декомпозиции (разделения) общей задачи оценки эффективности на ряд частных задач. Так, задача оценки эффективности СЗИ может разбиваться на частные задачи:

- ♦ оценку эффективности защиты от сбоев и отказов аппаратных и программных средств;
- ♦ оценку эффективности защиты от НСДИ;
- ♦ оценку эффективности защиты от ПЭМИН и т. д.

При оценке эффективности защиты от отказов, приводящих к уничтожению информации, используется, например, такая величина, как вероятность безотказной работы $P(t)$ системы за время t .

Этот показатель вычисляется по формуле:

$$P(t) = 1 - P_{\text{отк}}(t), \quad (4.1)$$

где $P_{\text{отк}}(t)$ - вероятность отказа системы за время t .

Величина $P_{\text{отк}}(t)$, в свою очередь, определяется в соответствии с известным выражением:

$$P_{\text{отк}}(t) = e^{-\lambda t}, \quad (4.2)$$

где λ - интенсивность отказов системы.

Таким образом, частная задача оценки влияния отказов на безопасность информации может быть довольно просто решена известными формальными методами.

Довольно просто решается частная задача оценки эффективности метода шифрования при условии, что атака на шифр возможна только путем перебора ключей, и известен метод шифрования.

Среднее время взлома шифра при этих условиях определяется по формуле:

$$T = \frac{s_t}{2}, \quad (4.3)$$

где T - среднее время взлома шифра;

Λ - число символов, которые могут быть использованы при выборе ключа (мощность алфавита шифрования);

S - длина ключа, выраженная в количестве символов;

t - время проверки одного ключа.

Время t зависит от производительности, используемой для атаки на шифр ИС и сложности алгоритма шифрования. При расчете криптостойкости обычно считается, что злоумышленник имеет в

своем распоряжении ИС наивысшей производительности, уже существующей или перспективной.

В свою очередь частные задачи могут быть декомпозированы на подзадачи.

Главная сложность метода декомпозиции при оценке систем заключается в учете взаимосвязи и взаимного влияния частных задач оценивания и оптимизации. Это влияние учитывается как при решении задачи декомпозиции, так и в процессе получения интегральных оценок. Например, при решении задачи защиты информации от электромагнитных излучений используется экранирование металлическими экранами, а для повышения надежности функционирования системы необходимо резервирование блоков, в том числе и блоков, обеспечивающих бесперебойное питание. Решение этих двух частных задач взаимосвязано, например, при создании СЗИ на летательных аппаратах, где существуют строгие ограничения на вес. При декомпозиции задачи оптимизации комплексной системы защиты приходится всякий раз учитывать общий лимит веса оборудования.

3. Макромоделирование.

При оценке сложных систем используется также макромоделирование. Такое моделирование осуществляется для общей оценки системы. Задача при этом упрощается за счет использования при построении модели только основных характеристик. К макромоделированию прибегают в основном для получения предварительных оценок систем.

В качестве макромодели можно рассматривать модель СЗИ, представленной на рис. 4.3. Если в СЗИ используется k уровней защиты, то в зависимости от выбранной модели злоумышленника ему необходимо преодолеть $k-m$ уровней защиты, где m - номер наивысшего уровня защиты, который злоумышленник беспрепятственно преодолевает в соответствии со своим официальным статусом. Если злоумышленник не имеет никакого официального статуса на объекте ИС, то ему, в общем случае, необходимо преодолеть все k уровней защиты, чтобы получить доступ к информации. Для такого злоумышленника вероятность получения несанкционированного доступа к информации $P_{\text{несд}}$ может быть рассчитана по формуле:

$$P_{\text{несд}} = \prod^k P_i \quad (4.4)$$

где P - вероятность преодоления злоумышленником i -го уровня защиты.

На макроуровне можно, например, исследовать требуемое число уровней защиты, их эффективность по отношению к предполагаемой модели нарушителя с учетом особенностей ИС и финансовых возможностей проектирования и построения СЗИ.

Выбор показателей эффективности и критериев оптимальности СЗИ.

Эффективность систем оценивается с помощью показателей эффективности. Иногда используется термин - показатель качества. Показателями качества, как правило, характеризуют степень совершенства какого-либо товара, устройства, машины. В отношении сложных человеко-машинных систем предпочтительнее использование термина показатель эффективности функционирования, который характеризует степень соответствия оцениваемой системы своему назначению.

Показатели эффективности системы, как правило, представляют собой некоторое множество функций y_k от характеристик системы x_n :

$$y_k = f(x_1, x_2, \dots, x_n), k=1, \dots, K, n=1, \dots, N, \quad (4.5)$$

где K - мощность множества показателей эффективности системы;

N - мощность множества характеристик системы.

Характеристиками системы $x_1, x_2, \dots, x_n$ называются первичные данные, отражающие свойства и особенности системы. Используются количественные и качественные характеристики. Количественные характеристики систем имеют числовое выражение. Их называют также параметрами. К *количественным* характеристикам относят разрядность устройства, быстродействие процессора и памяти, длину пароля, длину ключа шифрования и т. п. *Качественные* характеристики определяют наличие (отсутствие) определенных режимов, защитных механизмов или сравнительную степень свойств систем («хорошо», «удовлетворительно», «лучше», «хуже»).

Примером показателя эффективности является криптостойкость шифра, которая выражается временем или стоимостью взлома шифра. Этот показатель для шифра DES, например, зависит от одной характеристики - разрядности ключа. Для методов замены криптостойкость зависит от количества используемых алфавитов замены, а для методов перестановок - от

размерности таблицы и количества используемых маршрутов Гамильтона.

Для того чтобы оценить эффективность системы защиты информации или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на использовании показателей эффективности, называют критерием эффективности. Для получения критерия эффективности при использовании некоторого множества k показателей используют ряд подходов [5].

1. Выбирается один *главный показатель*, и оптимальной считается система, для которой этот показатель достигает экстремума. При условии, что остальные показатели удовлетворяют системе ограничений, заданных в виде неравенств. Например, оптимальной может считаться система, удовлетворяющая следующему критерию эффективности:

$$P_{из} = P_{из}^{max} \quad (4.6)$$

при $C' < C_{доп}$, $G < G_{доп}$,

где $P_{из}$ - вероятность преодоления злоумышленником системы защиты за определенное время;

C и G - стоимостные и весовые показатели, соответственно, которые не должны превышать допустимых значений.

2. Методы, основанные на *ранжировании показателей* по важности. При сравнении систем одноименные показатели эффективности сопоставляются в порядке убывания их важности по определенным алгоритмам.

Примерами таких методов могут служить лексикографический метод и метод последовательных уступок.

Лексикографический метод применим, если степень различия показателей по важности велика. Две системы сравниваются сначала по наиболее важному показателю. Оптимальной считается такая система, у которой лучше этот показатель. При равенстве самых важных показателей сравниваются показатели, занимающие по рангу вторую позицию. При равенстве и этих показателей сравнение продолжается до получения предпочтения в i -м показателе.

Метод последовательных уступок предполагает оптимизацию системы по наиболее важному показателю Y_1 .

Определяется допустимая величина изменения показателя Y_1 , которая называется уступкой. Измененная величина показателя: $Y_1^I = Y_1 \pm \Delta_1$ (Δ_1 - величина уступки) фиксируется. Определяется 330

оптимальная величина показателя Y_2 , при фиксированном значении Y_1^1 , выбирается уступка Δ_2 и процесс повторяется до получения Y_{k-1}

3. *Мультипликативные и аддитивные методы* получения критериев эффективности основываются на объединении всех или части показателей с помощью операций умножения или сложения в обобщенные показатели (Z_Y, Z_C). Показатели, используемые в обобщенных показателях, называют *частными* (y, y).

Если в произведение (сумму) включается часть показателей, то остальные частные показатели включаются в ограничения. Показатели, образующие произведение (сумму), могут иметь весовые коэффициенты k (k). В общем виде эти методы можно представить следующим образом:

$$Z_Y = \text{extr} \prod k y ; \quad Z_C = \text{extr} \sum k_j y_j \quad (4.7)$$

4. Оценка эффективности СЗИ может осуществляться также *методом Парето*. Сущность метода заключается в следующем. При использовании n показателей эффективности системе соответствует точка в n -мерном пространстве. В n -мерном пространстве строится область парето-оптимальных решений. В этой области располагаются несравнимые решения, для которых улучшение какого-либо показателя невозможно без ухудшения других показателей эффективности. Выбор наилучшего решения из числа парето-оптимальных может осуществляться по различным правилам.

4.1.4. Математическая постановка задачи разработки защищенной информационной системы

После выбора показателей эффективности и критерия эффективности может быть осуществлена математическая постановка задачи разработки СЗИ. На этом этапе уже известны:

- ♦ $F = \{f_1, f_2, \dots, f_n\}$ - функции, которые должна выполнять СЗИ;
- ♦ $M = \{m_1, m_2, \dots, m_k\}$ - возможные механизмы защиты;
- ♦ $U = \{u_1, u_2, \dots, u_p\}$ - способы управления СЗИ.
- ♦ $Y = \{y_1, y_2, \dots, y_v\}$ - показатели эффективности СЗИ.

Показатели эффективности зависят от выполняемых функций (F), механизмов защиты (M), и способов управления (U) СЗИ: $Y = \Phi(F, M, U)$.

Критерий эффективности получается с использованием показателей эффективности: $K = E(Y)$.

Тогда математическая постановка задачи разработки СЗИ в общем случае может быть представлена в следующем виде:

найти $\text{extr} S(F, M^*, U^*)$, при $M^* \in M$, $U^* \in U$, которым соответствуют $Y^* \in Y_d$, где Y_d - множество допустимых значений показателей эффективности СЗИ.

То есть, требуется создать или выбрать такие механизмы защиты информации и способы управления системой защиты, при которых обеспечивается выполнение всего множества требуемых функций и достигается максимум или минимум выбранного критерия, а также выполняются ограничения на некоторые показатели эффективности.

Такая постановка применима не только для решения общей, но и частных задач оценки эффективности системы защиты информации.

4.1.5. Оценка эффективности и создание организационной структуры системы защиты информации

Оценка эффективности СЗИ.

Эффективность СЗИ оценивается как на этапе разработки, так и в процессе эксплуатации. В оценке эффективности СЗИ, в зависимости от используемых показателей и способов их получения, можно выделить три подхода [5]:

- ◆ классический;
- ◆ официальный;
- ◆ экспериментальный.

Классический подход.

Под классическим подходом к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной КС. Такой подход используется при разработке и модернизации СЗИ. Однако возможности классических методов комплексного оценивания эффективности применительно к СЗИ ограничены в силу ряда причин: высокая степень

неопределенности исходных данных, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев оптимальности создают значительные трудности для применения классических методов оценки эффективности.

Официальный подход.

Большую практическую значимость имеет подход к определению эффективности СЗИ, который условно можно назвать официальным. Политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. В этих документах необходимо определить требования к защищенности информации различных категорий конфиденциальности и важности.

Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь в ИС, чтобы она соответствовала определенному классу защиты. Используя такие документы, можно оценить эффективность СЗИ. В этом случае критерием эффективности СЗИ является ее класс защищенности.

Несомненным достоинством таких классификаторов (стандартов) является простота использования. Основным недостатком официального подхода к определению эффективности систем защиты является то, что не определяется эффективность конкретного механизма защиты, а констатируется лишь факт его наличия или отсутствия. Этот недостаток в какой-то мере компенсируется заданием в некоторых документах достаточно подробных требований к этим механизмам защиты.

Во всех развитых странах разработаны свои стандарты защищенности компьютерных систем критического применения. Так, в министерстве обороны США используется стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria) [5], который известен как Оранжевая книга.

Согласно Оранжевой книге для оценки информационных систем рассматриваются четыре группы безопасности: А, В, С, D. В некоторых случаях группы безопасности делятся дополнительно на классы безопасности.

Группа А (гарантированная или проверяемая защита) обеспечивает гарантированный уровень безопасности. Методы защиты, реализованные в системе, могут быть проверены формальными методами. В этой группе имеется только один класс - А1.

Группа В (полномочная или полная защита) представляет полную защиту КС. В этой группе выделены классы безопасности В1, В2 и В3.

Класс В1 (защита через грифы или метки) обеспечивается использованием в КС грифов секретности, определяющих доступ пользователей к частям системы.

Класс В2 (структурированная защита) достигается разделением информации на защищенные и незащищенные блоки и контролем доступа к ним пользователей.

Класс В3 (области или домены безопасности) предусматривает разделение КС на подсистемы с различным уровнем безопасности и контролем доступа к ним пользователей.

Группа С (избирательная защита) представляет избирательную защиту подсистем с контролем доступа к ним пользователей. В этой группе выделены классы безопасности С1 и С2.

Класс С1 (избирательная защита информации) предусматривает разделение в КС пользователей и данных. Этот класс обеспечивает самый низкий уровень защиты ИС.

Класс С2 (защита через управляемый или контролируемый доступ) обеспечивается раздельным доступом пользователей к данным.

Группу D (минимальной безопасности) составляют ИС, проверенные на безопасность, но которые не могут быть отнесены к классам А, В или С.

Организация защиты информации в вычислительных сетях министерства обороны США осуществляется в соответствии с требованиями руководства «The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines». Этот документ получил название Красная книга (как и предыдущий - по цвету обложки).

Подобные стандарты защищенности ИС приняты и в других развитых странах. Так, в 1991 году Франция, Германия, Нидерланды и Великобритания приняли согласованные «Европейские критерии», в которых рассмотрено 7 классов безопасности от Е0 до Е6.

В Российской Федерации аналогичный стандарт разработан в 1992 году Государственной технической комиссией (ГТК) при Президенте РФ (ныне ФСТЭК России). Этим стандартом является руководящий документ ГТК «Концепция защиты средств

вычислительной техники и автоматизированных систем от НСД к информации» [6.7].

Устанавливается семь классов защищенности средств вычислительной техники (СВТ) от НСД к информации (таблица 4.1). Самый низкий класс - седьмой, самый высокий - первый.

Таблица 4.1

Показатели защищенности по классам СВТ

Наименование показателя	Класс защищенности						
	6	5	4	3	2	1	
1. Дискреционный принцип контроля доступа	+	+	+	+	+	+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=	=
3. Очистка памяти	-	+	+	+	+	+	=
4. Изоляция модулей	-	-	+	=	+	+	=
5. Маркировка документов	-	-	+	-	+	+	=
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	+	+	=
7. Сопоставление пользователя с устройством	-	-	+	=	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=	=
9. Гарантия проектирования	-	+	+	+	+	+	+
10. Регистрация	-	+	+	+	=	=	=
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=	=
12. Надежное восстановление	-	-	-	+	=	=	=
13. Целостность КСЗ	-	+	+	+	=	=	=
14. Контроль модификации	-	-	-	-	+	+	=
15. Контроль дистрибуции	-	-	-	-	+	+	=
16. Гарантии архитектуры	-	-	-	-	-	+	+
17. Тестирование	+	+	+	+	+	+	=
18. Руководство пользователя	+	=	=	=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	+	=
20. Текстовая документация	+	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+	+

Обозначения: «-» - нет требований к данному классу; «+» - новые или дополнительные требования; «=» - требования совпадают с требованиями к СВТ предыдущего класса; КСЗ - комплекс средств защиты.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- ♦ первая группа содержит только один седьмой класс;

- ♦ вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

- ♦ третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

- ♦ четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

Кроме требований к защищенности отдельных элементов СВТ, в Руководящем документе приведены требования к защищенности автоматизированных систем (АС) [6,7]. В отличие от СВТ автоматизированные системы являются функционально ориентированными. При создании АС учитываются особенности пользовательской информации, технология обработки, хранения и передачи информации, конкретные модели угроз.

Устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Третья группа классифицирует АС, с которыми работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А. Во вторую группу сведены АС, пользователи которых имеют одинаковые права доступа ко всей информации АС. Группа содержит два класса - 2Б и 2А. Первую группу составляют многопользовательские АС, в которых пользователи имеют разные права доступа к информации. Группа включает пять классов- 1Д, 1Г, 1В, 1Б, 1А.

Требования ко всем девяти классам защищенности АС сведены в таблицу. 4.2.

Для примера целесообразно рассмотреть подробно требования к одному из представительных классов защищенности, а именно - к классу 1В.

В подсистеме управления доступом автоматизированной системы должны осуществляться:

- ♦ идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

- ♦ идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;
- ♦ идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- ♦ контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- ♦ управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета должна обеспечивать:

- ♦ регистрацию входа/выхода субъектов доступа в систему/из системы, либо регистрацию загрузки и инициализации операционной системы и ее программного останова;
- ♦ регистрацию выдачи печатных (графических) документов на «твердую» копию;
- ♦ регистрацию запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- ♦ регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;

Таблица 4.2

Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	ЗБ	З	2Б	2	ИД	И	ИБ	ИБ	1
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+

Продолжение табл. 4.2

к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)				+	+	+	+	+	+
выдачи печатных (графических) выходных документов				+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
доступа программ субъектов, доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
изменения полномочий субъектов доступа							+	+	+
создаваемых защищаемых объектов доступа				+			+	+	+
2.2. Учет носителей информации				+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей				+		+	+	+	+
2.4. Сигнализация попыток нарушения защиты							+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам									+

доступа (группам субъектов) на разных ключах								
3.3. Использование аттестованных (сертифицированных) криптографических средств			+				+	+
4. Подсистема обеспечения целостности								
4.1. Обеспечение целостности программных средств и обрабатываемой информации			+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации			+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС			+			+	+	+
4.4. Периодическое тестирование СЗИ НСД			+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД			+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты			+			+	+	+

Обозначения: «+» - есть требования к данному классу: СЗИ НСД - система защиты информации от несанкционированного доступа.

♦ регистрацию изменений полномочий субъектов доступа и статуса объектов доступа;

♦ автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

♦ учет всех защищаемых носителей информации с помощью их любой маркировки;

♦ очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется путем записи последовательности 1 и 0 в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

♦ сигнализацию попыток нарушения защиты.

Подсистема обеспечения целостности предусматривает:

- ♦ обеспечение целостности программных средств СЗИ НСД, а также неизменность программной среды. Целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

- ♦ охрану СВТ (устройств и носителей информации), что предполагает охрану территории и здания, где размещается АС, с помощью технических средств и специального персонала, строгий пропускной режим, специальное оборудование помещений АС;

- ♦ наличие администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

- ♦ периодическое тестирование всех функций СЗИ НСД с помощью специальных программ не реже одного раза в год;

- ♦ наличие средств восстановления СЗИ НСД (ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности);

- ♦ использование сертифицированных средств защиты.

Представленный перечень является тем минимумом требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Стандарт требований TCSEC соответствует информационным системам с применением ЭВМ общего пользования (main frame) и мини ЭВМ. Для персональных ЭВМ (ПЭВМ) и локальных сетей ПЭВМ требования безопасности должны быть несколько иными. Такие требования изложены [5] в стандарте The Trusted Network Interpretation of Department of Defence Trusted Computer System Evaluation Guidelines, получившем название Красная книга. Неофициальные названия стандартов США Оранжевая книга и Красная книга связаны с соответствующим цветом обложек этих документов.

Экспериментальный подход

Под экспериментальным подходом понимается организация процесса определения эффективности существующих КСЗИ путем попыток преодоления защитных механизмов системы специалистами,

выступающими в роли злоумышленников. Такие исследования проводятся следующим образом. В качестве условного злоумышленника выбирается один или несколько специалистов в области информационной борьбы наивысшей квалификации. Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению слабых звеньев в системе защиты. При этом могут моделироваться действия злоумышленников, соответствующие различным моделям поведения нарушителей: от неквалифицированного злоумышленника, не имеющего официального статуса в исследуемой КС, до высококвалифицированного сотрудника службы безопасности.

Служба безопасности до момента преодоления защиты «злоумышленниками» должна ввести в СЗИ новые механизмы защиты (изменить старые), чтобы избежать «взлома» системы защиты.

Такой подход к оценке эффективности позволяет получать объективные данные о возможностях существующих СЗИ, но требует высокой квалификации исполнителей и больших материальных и временных затрат. Для проведения экспериментов необходимо иметь самое современное оборудование (средства инженерно-технической разведки, аппаратно-программные и испытательные комплексы (стенды) и т. п.)

Создание организационной структуры СЗИ

Одной из основных составляющих СЗИ является организационная структура, которая создается для выполнения организационных мер защиты, эксплуатации технических, программных и криптографических средств защиты, а также для контроля за выполнением установленных правил эксплуатации ИС обслуживающим персоналом и пользователями. Такие структуры входят в состав службы безопасности ведомств, корпораций, фирм, организаций. Они могут иметь различный количественный состав и внутреннюю структуру. Это может быть отдел, группа или отдельное должностное лицо. Непосредственной эксплуатацией средств защиты и выполнением организационных мероприятий занимаются органы защиты информации, размещаемые на объектах ИС. Их называют объектовыми органами защиты информации или органами обеспечения безопасности информации (ОБИ). Если объекты ИС располагаются на одной территории с другими объектами ведомства, корпорации, фирмы, то часть функций, таких как охрана,

разведывательная и контрразведывательная и некоторые другие выполняются соответствующими отделами службы безопасности. Подразделение (должностное лицо) ОБИ может входить организационно и в состав вычислительных центров или отделов автоматизации. При этом службы безопасности сохраняют за собой функции контроля и методического обеспечения функционирования СЗИ. Количественный состав и его структура органа ОБИ определяется после завершения разработки СЗИ.

При создании органа ОБИ используются данные, полученные в результате разработки СЗИ:

- ♦ официальный статус ИС и информации, обрабатываемой в системе;
- ♦ перечень организационных мероприятий защиты и их характеристики;
- ♦ степень автоматизации СЗИ;
- ♦ особенности технической структуры и режимы функционирования ИС.

Органы ОБИ создаются в соответствии с законодательством РФ, регулирующим взаимоотношения граждан и юридических лиц в сфере информационных технологий. В зависимости от владельца, конфиденциальности и важности обрабатываемой в ИС информации определяется юридический статус самой ИС и органа ОБИ. В соответствии со статусом органа ОБИ определяются его юридические права и обязанности, определяется порядок взаимодействия с государственными органами, осуществляющими обеспечение безопасности информации в государстве.

При создании органов ОБИ руководствуются также требованиями подзаконных актов (Постановлений Правительства, решений ФСТЭК и ФСБ, ГОСТ и других), а также руководящими документами ведомств.

В результате разработки СЗИ определяется перечень организационных мероприятий защиты информации, которые представляют собой действия, выполняемые сотрудниками служб безопасности, органов ОБИ, обслуживающим персоналом и пользователями, в интересах обеспечения безопасности информации. Все организационные мероприятия защиты можно разделить на два класса:

1. защитные мероприятия, непосредственно направленные на обеспечение безопасности информации;

2. эксплуатационные мероприятия, связанные с организацией эксплуатации сложных систем.

Подавляющее большинство защитных, организационных мероприятий связано с обслуживанием технических, программных и криптографических средств защиты. Примерами таких мероприятий являются: использование паролей и материальных идентификаторов, контроль доступа к информационным ресурсам путем выполнения определенных действий при получении сигнала о нарушении правил разграничения доступа и анализа журнала контроля, дублирование и восстановление информации и др.

Некоторые функции системы защиты могут быть реализованы только за счет организационных мероприятий, например, доступ в помещение с информационными ресурсами может осуществлять контролер. Защита от пожара реализуется путем вызова пожарной команды, эвакуации информационных ресурсов, использования средств тушения пожара.

Часто организационные мероприятия дополняют технические, программные и криптографические средства, образуя еще один уровень защиты. Так зеркальное дублирование, которое выполняется без вмешательства человека, может быть дополнено периодическим дублированием информации на съемные магнитные носители. Автоматизированный контроль вскрытия дверей, корпусов, крышек и других элементов защиты внутреннего монтажа устройств от несанкционированной модификации может быть дополнен опечатыванием этих элементов (использованием специальных защитных знаков) и контролем целостности печатей (защитных знаков) должностными лицами.

Под эксплуатационными организационными мероприятиями понимается комплекс мероприятий, связанных с необходимостью технической эксплуатации системы защиты информации, как подсистемы сложной человеко-машинной системы. Задачи, решаемые в процессе технической эксплуатации ИС, приведены в п.4.2.2.

Имея полный перечень организационных мероприятий защиты и зная их характеристики, можно определить в общих чертах организационно-штатную структуру подразделения ОБИ. Организационно-штатная структура подразделения ОБИ уточняется в процессе анализа степени автоматизации системы защиты, а также режимов функционирования ИС. При этом решается вопрос о распределении обязанностей по эксплуатации средств СЗИ между

обслуживающим персоналом и должностными лицами подразделения ОБИ. Так рабочая станция дежурного оператора СЗИ может обслуживаться специалистами подразделения технического обслуживания, так как такое рабочее место по технической структуре, как правило, не отличается от рабочих мест других пользователей. В то же время устройства криптозащиты с учетом особенностей конструкции и повышенных требований по ограничению доступа к ним, как правило, обслуживаются специалистами подразделения ОБИ.

Особенности технической структуры СЗИ и ИС, а также режимы их функционирования влияют на количество рабочих мест операторов СЗИ и режим работы операторов. При высокой степени автоматизации выполнения функций защиты число операторов может быть минимальным. При круглосуточном режиме работы число операторов СЗИ соответственно увеличивается.

В небольших организациях, использующих защищенные ИС, функции обеспечения защиты информации и технической эксплуатации могут выполняться одним должностным лицом, например, администратором ЛВС.

В процессе создания подразделений ОБИ выполняют следующий комплекс мероприятий:

1. определяются организационно-штатная структура, права и обязанности должностных лиц;
2. должностные лица обучаются практической работе с СЗИ;
3. разрабатывается необходимая документация;
4. оборудуются рабочие места должностных лиц;
5. определяется система управления КСЗИ.

Организационно-штатная структура определяет перечень должностей, подчиненность подразделения и должностных лиц подразделения. Каждому должностному лицу определяются его права и обязанности в соответствии с занимаемой должностью.

Эффективность функционирования СЗИ во многом определяется уровнем руководства всем процессом ОБИ. Орган управления СЗИ готовит предложения руководству организации при формировании и корректировке политики безопасности, определяет права и обязанности должностных лиц, планирует и обеспечивает выполнение технического обслуживания, осуществляет методическое руководство подчиненными структурами, организует контроль и анализ эффективности СЗИ, осуществляет подбор, расстановку и обучение специалистов.

При отборе специалистов для работы в подразделении ОБИ, кроме деловых качеств, необходимо учитывать и морально-психологические данные кандидатов. Каждый специалист должен приобрести знания и навыки в эксплуатации механизмов защиты. Специалисты подразделений обслуживания и пользователи должны быть обучены работе в защищенных ИС. Перед получением допуска все обязательно проходят тестирование.

В процессе создания организационной структуры СЗИ используются следующие документы: законы, постановления Правительства, решения ФСТЭК, ГОСТ, ведомственные директивы, инструкции и методические материалы. Кроме того, используется документация, полученная с установленными средствами защиты. В процессе эксплуатации СЗИ документы разрабатываются и ведутся силами подразделений ОБИ.

Рабочие места должностных лиц подразделения ОБИ оборудуются средствами, полученными от разработчиков. Это пульта управления, мониторы, средства дистанционного контроля и т. п. Кроме того, на рабочих местах должны быть средства связи, инструкции, эксплуатационная документация, а также средства пожаротушения.

4.2. Организация функционирования защищенной информационной системы

4.2.1. Применение системы защиты информации

Организация доступа к ресурсам КС.

Функционирование СЗИ зависит не только от характеристик созданной системы, но и от эффективности ее использования на этапе эксплуатации КС. Основными задачами этапа эксплуатации являются максимальное использование возможностей СЗИ, заложенных в систему при построении, и совершенствование ее защитных функций в соответствии с изменяющимися условиями.

Процесс эксплуатации СЗИ можно разделить на применение системы по прямому назначению, что предполагает выполнение всего комплекса мероприятий, непосредственно связанных с защитой информации в ИС, и техническую эксплуатацию (рис.4.4). Применение по назначению предусматривает организацию доступа к ресурсам ИС и обеспечение их целостности.

Под *организацией доступа к ресурсам* понимается весь комплекс мер, который выполняется в процессе эксплуатации ИС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.

Организация доступа к ресурсам предполагает:

- ♦ разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам ИС в соответствии с функциональными обязанностями должностных лиц;
- ♦ организацию работы с конфиденциальными информационными ресурсами на объекте;
- ♦ защиту от технических средств разведки;
- ♦ охрану объекта;
- ♦ эксплуатацию системы разграничения доступа.



Рис. 4.4. Содержание процесса эксплуатации СЗИ

Права должностных лиц по доступу к ресурсам ИС устанавливаются руководством организации, в интересах которой используется ИС. Каждому должностному лицу определяются для использования технические ресурсы (рабочая станция, сервер, аппаратура передачи данных и т.д.), разрешенные режимы и время работы. Руководством устанавливается уровень компетенции должностных лиц по манипулированию информацией. Лицо,

ответственное за ОБИ в ИС, на основании решения руководителя о разграничении доступа должностных лиц обеспечивает ввод соответствующих полномочий доступа в систему разграничения доступа.

Руководство совместно со службой безопасности определяет порядок работы с конфиденциальными информационными ресурсами, не используемыми непосредственно в ИС, хотя бы и временно. К таким ресурсам относятся конфиденциальная печатная продукция, в том числе и полученная с помощью ИС, а также машинные носители информации, находящиеся вне устройств ИС. Учетом, хранением и выдачей таких ресурсов занимаются должностные лица из службы безопасности, либо другие должностные лица по совместительству.

Службой безопасности выполняется весь комплекс мероприятий противодействия техническим средствам разведки. Контролируется применение пассивных средств защиты от ПЭМИ и наводок. Активные средства защиты от угроз этого класса используются в соответствии с графиком работы объекта. Периодически осуществляются проверки помещений на отсутствие в них закладных устройств аудио- и видеоразведки, а также обеспечивается защищенность линий связи от прослушивания.

Охрана объекта ИС обеспечивает разграничение непосредственного доступа людей на контролируемую территорию, в здания и помещения. Подразделение охраны (охранник) может находиться на объекте, а может охранять несколько объектов. В последнем случае на объекте находятся только технические средства охраны и сигнализации. В соответствии с принятой политикой безопасности руководство совместно со службой безопасности определяют структуру системы охраны. Количественный состав и режим работы подразделения охраны определяется важностью и конфиденциальностью информации ИС, а также используемыми техническими средствами охраны и сигнализации.

Система разграничения доступа (СРД) является одной из главных составляющих комплексной системы защиты информации. В этой системе можно выделить следующие компоненты:

- ◆ средства аутентификации субъекта доступа;
- ◆ средства разграничения доступа к техническим устройствам компьютерной системы;
- ◆ средства разграничения доступа к программам и данным;
- ◆ средства блокировки неправомерных действий;

- ♦ средства регистрации событий;
- ♦ дежурный оператор системы разграничения доступа.

Эффективность функционирования системы разграничения доступа во многом определяется надежностью механизмов аутентификации. Особое значение имеет аутентификация при взаимодействии удаленных процессов, которая всегда осуществляется с применением методов криптографии. При эксплуатации механизмов аутентификации основными задачами являются: генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в ИС. При компрометации атрибутов доступа (пароля, персонального кода и т. п.) необходимо срочное их исключение из списка разрешенных. Эти действия должны выполняться дежурным оператором системы разграничения доступа.

В больших распределенных ИС проблема генерации и доставки атрибутов идентификации и ключей шифрования не является тривиальной задачей. Так, например, распределение секретных ключей шифрования должно осуществляться вне защищаемой компьютерной системы. Значения идентификаторов пользователя не должны храниться и передаваться в системе в открытом виде. На время ввода и сравнения идентификаторов необходимо применять особые меры защиты от подсматривания набора пароля и воздействия вредительских программ типа клавиатурных шпионов и программ-имитаторов СРД.

Средства разграничения доступа к техническим средствам препятствуют несанкционированным действиям злоумышленника, таким как включение технического средства, загрузка операционной системы, ввод-вывод информации, использование нештатных устройств и т. д. Разграничение доступа осуществляется оператором СРД путем использования технических и программных средств. Так оператор СРД может контролировать использование ключей от замков подачи питания непосредственно на техническое средство или на все устройства, находящиеся в отдельном помещении, дистанционно управлять блокировкой подачи питания на устройство или блокировкой загрузки ОС. На аппаратном или программном уровне оператор может изменять техническую структуру средств, которые может использовать конкретный пользователь.

Средства разграничения доступа к программам и данным используются наиболее интенсивно и во многом определяют

характеристики СРД. Эти средства являются аппаратно-программными. Они настраиваются должностными лицами подразделения, обеспечивающего безопасность информации, и изменяются при изменении полномочий пользователя или при изменении программной и информационной структуры. Доступ к файлам регулируется диспетчером доступа. Доступ к записям и отдельным полям записей в файлах баз данных регулируется также с помощью систем управления базами данных.

Эффективность СРД можно повысить за счет шифрования файлов, хранящихся на внешних запоминающих устройствах, а также за счет полного стирания файлов при их уничтожении и стирания временных файлов. Даже если злоумышленник получит доступ к машинному носителю путем, например, несанкционированного копирования, то получить доступ к информации он не сможет без ключа шифрования.

В распределенных ИС доступ между подсистемами, например удаленными ЛВС, регулируется с помощью межсетевых экранов. Межсетевой экран необходимо использовать для управления обменом между защищенной и незащищенной компьютерными системами. При этом регулируется доступ как из незащищенной ИС в защищенную, так и доступ из защищенной системы в незащищенную. Компьютер, реализующий функции межсетевого экрана, целесообразно размещать на рабочем месте оператора СЗИ.

Средства блокировки неправомерных действий субъектов доступа являются неотъемлемой компонентой СРД. Если атрибуты субъекта доступа или алгоритм его действий не являются разрешенными для данного субъекта, то дальнейшая работа в ИС такого нарушителя прекращается до вмешательства оператора СЗИ. Средства блокировки исключают или в значительной степени затрудняют автоматический подбор атрибутов доступа.

Средства регистрации событий также являются обязательной компонентой СРД. Журналы регистрации событий располагаются на ВЗУ. В таких журналах записываются данные о входе пользователей в систему и о выходе из нее, о всех попытках выполнения несанкционированных действий, о доступе к определенным ресурсам и т. п. Настройка журнала на фиксацию определенных событий и периодический анализ его содержимого осуществляется дежурным оператором и вышестоящими должностными лицами из подразделения ОБИ. Процесс настройки и анализа журнала целесообразно автоматизировать программным путем.

Непосредственное управление СРД осуществляет дежурный оператор СЗИ, который, как правило, выполняет и функции дежурного администратора ИС. Он загружает ОС, обеспечивает требуемую конфигурацию и режимы работы ИС, вводит в СРД полномочия и атрибуты пользователей, осуществляет контроль и управляет доступом пользователей к ресурсам ИС.

Обеспечение целостности и доступности информации в ИС

На этапе эксплуатации ИС целостность и доступность информации в системе обеспечивается путем:

- ♦ дублирования информации;
- ♦ повышения отказоустойчивости ИС;
- ♦ противодействия перегрузкам и «зависаниям» системы;
- ♦ использования строго определенного множества программ;
- ♦ контроля целостности информации в ИС;
- ♦ особой регламентации процессов технического обслуживания и проведения доработок;
- ♦ выполнения комплекса антивирусных мероприятий.

Одним из главных условий обеспечения целостности и доступности информации в ИС является ее дублирование. Стратегия дублирования выбирается с учетом важности информации, требований к непрерывности работы ИС, трудоемкости восстановления данных. Дублирование информации обеспечивается дежурным администратором ИС.

Целостность и доступность информации поддерживается также путем резервирования аппаратных средств, блокировок ошибочных действий людей, использования надежных элементов ИС и отказоустойчивых систем. Устраняются также преднамеренные угрозы перегрузки элементов систем. Для этого используются механизмы измерения интенсивности поступления заявок на выполнение (передачу) и механизмы ограничения или полного блокирования передачи таких заявок. Должна быть предусмотрена также возможность определения причин резкого увеличения потока заявок на выполнение программ или передачу информации.

В сложных системах практически невозможно избежать ситуаций, приводящих к «зависаниям» систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят заикливания программ, непредусмотренные остановки и другие ситуации, выход из которых возможен лишь путем прерывания вычислительного процесса и

последующего его восстановления. На этапе эксплуатации ведется статистика и осуществляется анализ таких ситуаций. «Зависания» своевременно обнаруживаются, и вычислительный процесс восстанавливается. При восстановлении, как правило, необходимо повторить выполнение прерванной программы с начала или с контрольной точки, если используется механизм контрольных точек. Такой механизм используется при выполнении сложных вычислительных программ, требующих значительного времени для их реализации.

В защищенной ИС должно использоваться только разрешенное программное обеспечение. Перечень официально разрешенных к использованию программ, а также периодичность и способы контроля их целостности должны быть определены перед началом эксплуатации ИС.

В защищенных ИС, сданных в эксплуатацию, как правило, нет необходимости использовать трансляторы и компиляторы, программы-отладчики, средства трассировки программ и тому подобные программные средства. Работы по созданию и модернизации программного обеспечения должны производиться в автономных ИС или, как исключение, в сегментах защищенной ИС, при условии использования надежных аппаратно-программных средств, исключающих возможность проведения мониторинга и несанкционированного внедрения исполняемых файлов в защищаемой ИС.

Простейшим методом контроля целостности программ является метод контрольных сумм. Для исключения возможности внесения изменений в контролируемый файл с последующей коррекцией контрольной суммы необходимо хранить контрольную сумму в зашифрованном виде или использовать секретный алгоритм вычисления контрольной суммы.

Однако наиболее приемлемым методом контроля целостности информации является использование хэш-функции. Значение хэш-функции практически невозможно подделать без знания ключа. Поэтому следует хранить в зашифрованном виде или в памяти, недоступной злоумышленнику, только ключ хэширования (стартовый вектор хэширования).

Контроль состава программного обеспечения и целостности (неизменности) программ осуществляется при плановых проверках комиссиями и должностными лицами, а также дежурным оператором СЗИ по определенному плану, неизвестному пользователям. Для

осуществления контроля используются специальные программные средства. В вычислительных сетях такая «ревизия» программного обеспечения может осуществляться дистанционно с рабочего места оператора СЗИ.

Особое внимание руководства и должностных лиц подразделения ОБИ должно быть сосредоточено на обеспечении целостности структур ИС и конфиденциальности информации, защите от хищения и несанкционированного копирования информационных ресурсов во время проведения технического обслуживания, восстановления работоспособности, ликвидации аварий, а также в период модернизации ИС. Так как на время проведения таких специальных работ отключаются (или находятся в неработоспособном состоянии) многие технические и программные средства защиты, то их отсутствие компенсируется системой организационных мероприятий:

- ◆ подготовка ИС к выполнению работ;
- ◆ допуск специалистов к выполнению работ;
- ◆ организация работ на объекте;
- ◆ завершение работ.

Перед проведением работ, по возможности, должны предприниматься следующие шаги:

◆ отключить фрагмент ИС, на котором необходимо выполнять работы, от функционирующей ИС;

- ◆ снять носители информации с устройств;
- ◆ осуществить стирание информации в памяти ИС;
- ◆ подготовить помещение для работы специалистов.

Перед проведением специальных работ необходимо всеми доступными способами изолировать ту часть ИС, на которой предполагается выполнять работы, от функционирующей части ИС. Для этого могут быть использованы аппаратные и программные блокировки и физические отключения цепей.

Все съемные носители с конфиденциальной информацией должны быть сняты с устройств и храниться в заземленных металлических шкафах в специальном помещении. Информация на несъемных носителях стирается путем трехкратной записи, например, двоичной последовательности чередующихся 1 и 0. На объекте необходимо определить порядок действий в случае невозможности стереть информацию до проведения специальных работ, например, при отказе накопителя на магнитных дисках. В этом случае восстановление работоспособности должно выполняться под

непосредственным контролем должностного лица из подразделения ОБИ. При восстановлении функции записи на носитель первой же операцией осуществляется стирание конфиденциальной информации. Если восстановление работоспособности накопителя с несъемным носителем информации невозможно, то устройство подлежит утилизации, включая физическое разрушение носителя.

При оборудовании помещения для проведения специальных работ осуществляется подготовка рабочих мест и обеспечивается изоляция рабочих мест от остальной части ИС. На рабочих местах должны использоваться сертифицированные и проверенные на отсутствие закладок приборы (если они не поставлялись в комплекте ИС). Меры по обеспечению изолированности рабочих мест от остальной ИС имеют целью исключить доступ сотрудников, выполняющих специальные работы, к элементам функционирующей ИС.

Допуск специалистов осуществляется на рабочие места в определенное время и после выполнения всех подготовительных операций.

При прибытии специалистов из других организаций, например, для проведения доработок, кроме обычной проверки лиц, допускаемых на объект, должны проверяться на отсутствие закладок приборы, устройства, которые доставлены для выполнения работ.

В процессе выполнения специальных работ необходимо исключить использование не проверенных аппаратных и программных средств, отклонения от установленной документацией технологии проведения работ, доступ к носителям с конфиденциальной информацией и к функционирующим в рабочих режимах элементам ИС.

Специальные работы завершаются контролем работоспособности ИС и отсутствия закладок. Проверка на отсутствие аппаратных закладок осуществляется путем осмотра устройств и тестирования их во всех режимах. Отсутствие программных закладок проверяется по контрольным суммам, а также путем тестирования. Результаты доработок принимаются комиссией и оформляются актом, в котором должны быть отражены результаты проверки работоспособности и отсутствия закладок. После проверок осуществляется восстановление информации и задействуются все механизмы защиты.

Для защиты ИС от компьютерных вирусов необходимо руководствоваться рекомендациями:

использовать программные продукты, полученные законным официальным путем;

дублировать информацию;

регулярно использовать антивирусные средства;

особую осторожность проявлять при использовании новых съемных носителей информации и новых файлов;

при работе в распределенных системах целесообразно новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели ЭВМ.

В автономных ИС непосредственную ответственность за выполнение комплекса антивирусных мероприятий целесообразно возложить на пользователя ИС. В ЛВС такая работа организуется должностными лицами подразделения ОБИ. Исполняемые файлы, в том числе саморазархивирующиеся и содержащие макрокоманды, должны вводиться в ЛВС под контролем дежурного оператора СЗИ и подвергаться проверке на отсутствие вирусов.

Успех эксплуатации СЗИ в большой степени зависит от уровня организации управления процессом эксплуатации. Иерархическая система управления позволяет организовать реализацию политики безопасности информации на этапе эксплуатации ИС. При организации системы управления следует придерживаться следующих принципов:

- ♦ уровень компетенции руководителя должен соответствовать его статусу в системе управления;

- ♦ строгая регламентация действий должностных лиц;

- ♦ документирование алгоритмов обеспечения защиты информации;

- ♦ непрерывность управления;

- ♦ адаптивность системы управления.

- ♦ контроль над реализацией политики безопасности.

Каждое должностное лицо из руководства организации, службы безопасности или подразделения ОБИ должны иметь знания и навыки работы с СЗИ в объеме, достаточном для выполнения своих функциональных обязанностей. Причем должностные лица должны располагать минимально возможными сведениями о конкретных механизмах защиты и о защищаемой информации. Это достигается за счет очень строгой регламентации их деятельности. Документирование всех алгоритмов эксплуатации СЗИ позволяет, при необходимости, легко заменять должностных лиц, а также осуществлять контроль над их деятельностью. Реализация этого

принципа позволит избежать «незаменимости» отдельных сотрудников и наладить эффективный контроль деятельности должностных лиц. Непрерывность управления СЗИ достигается за счет организации дежурства операторов СЗИ. Система управления должна быть гибкой и оперативно адаптироваться к изменяющимся условиям функционирования.

4.2.2. Техническая эксплуатация защищенной информационной системы

Техническая эксплуатация сложной системы включает в себя комплекс мероприятий, обеспечивающий эффективное использование системы по назначению. Комплексная СЗИ является подсистемой ИС и ее техническая эксплуатация организуется в соответствии с общим подходом обеспечения эффективности применения ИС.

Подробное изложение задач технической эксплуатации ИС – это достаточно объемный материал, поэтому приведем лишь общую характеристику задач, решаемых в процессе технической эксплуатации СЗИ. К этим задачам относятся:

- ◆ организационные задачи;
- ◆ поддержание работоспособности СЗИ;
- ◆ обеспечение технической эксплуатации.

К организационным задачам относятся:

- ◆ планирование технической эксплуатации;
- ◆ организация дежурства;
- ◆ работа с кадрами;
- ◆ работа с документами.

Планирование технической эксплуатации осуществляется на длительные сроки (полгода, год и более). Используется также среднесрочное (квартал, месяц) и краткосрочное планирование (неделя, сутки). На длительные сроки планируются полугодовое техническое обслуживание и работа комиссий, поставки оборудования, запасных изделий и приборов, ремонты устройств и т. п. Среднесрочное планирование и краткосрочное применяются при организации технического обслуживания, проведении доработок, организации дежурства и др.

Для непрерывного выполнения организационных мер защиты, и эксплуатации всех механизмов защиты организуется дежурство. Режим дежурства зависит от режима использования ИС. Дежурный

оператор СЗИ может выполнять по совместительству и функции общего администрирования в компьютерной сети. Рабочее место оператора СЗИ, как правило, располагается в непосредственной близости от наиболее важных компонентов ИС (серверов, межсетевых экранов и т. п.) и оборудуется всеми необходимыми средствами оперативного управления СЗИ.

Работа с обслуживающим персоналом и пользователями сводится к подбору кадров, их обучению, воспитанию, к созданию условий для высокоэффективного труда.

В процессе технической эксплуатации используется четыре типа документов:

1. Законы.
2. Ведомственные руководящие документы.
3. Документация предприятий-изготовителей.
4. Документация, разрабатываемая в процессе эксплуатации.

В законах отражены общие вопросы эксплуатации СЗИ. В ведомствах (министерствах, объединениях, корпорациях, государственных учреждениях) разрабатывают инструкции, директивы, государственные стандарты, методические рекомендации и т. п.

Предприятия-изготовители поставляют эксплуатационно-техническую документацию: технические описания, инструкции по эксплуатации, формуляры (паспорта) и др.

В организациях, эксплуатирующих ИС, разрабатывают и ведут планирующую и учетно-отчетную документацию.

Одной из центральных задач технической эксплуатации является поддержание работоспособности систем. Работоспособность поддерживается в основном за счет проведения технического обслуживания, постоянного контроля работоспособности и ее восстановления в случае отказа. Работоспособность средств защиты информации контролируется постоянно с помощью аппаратно-программных средств встроенного контроля и периодически должностными лицами службы безопасности и комиссиями. Сроки проведения контроля и объем работ определяются в руководящих документах.

Успех технической эксплуатации зависит и от качества обеспечения, которое включает:

- ♦ материально-техническое обеспечение;
- ♦ метрологическое обеспечение;
- ♦ транспортировка и хранение;

♦ обеспечение безопасности эксплуатации.

Материально-техническое обеспечение позволяет удовлетворить потребность в расходных материалах, запасных изделиях и приборах, инструментах и других материальных средствах, необходимых для эксплуатации СЗИ.

Транспортировка и хранение устройств защищенной ИС должны предусматривать защиту от несанкционированного доступа к устройствам в пути и в хранилищах. Для обеспечения необходимых условий транспортировки и хранения выполняются мероприятия подготовки устройств согласно требованиям эксплуатационно-технической документации.

Метрологическое обеспечение позволяет поддерживать измерительные приборы в исправном состоянии.

В процессе эксплуатации важно обеспечивать безопасность обслуживающего персонала и пользователей прежде всего от угрозы поражения электрическим током, а также от возможных пожаров.

В целом от уровня технической эксплуатации во многом зависит эффективность использования СЗИ.

СПИСОК ЛИТЕРАТУРЫ

1. Бусленко Н.П. Моделирование сложных систем / Н.П. Бусленко. М.: Наука, 1978. 400 с.
2. Волкова В.Н. Основы теории систем и системного анализа / В.Н. Волкова, А.А. Денисов. СПб.: СПбГТУ, 1997. 510 с.
3. Острейковский В.А. Теория систем / В.А.Острейковский. М.: Высшая школа, 1997. 240 с.
4. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л.А. Заде. М.: Мир, 1976. 168 с.
5. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос, ИБОЮЛ Н.А.Егоров, 2001. 264 с.
6. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.:Jet Info, 1997.
7. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.:Jet Info, 1997.
8. Российская Федерация. Законы. «Об информации, информационных технологиях и о защите информации»: Федер. Закон:[принят Гос.Думой 8 июля 2006 г.; одобрен Советом Федерации 14 июля 2006 г.] [Электронный ресурс]. Режим доступа: <http://www.rg.ru/gazeta/rg/2006/07/29.html>.
9. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-99. Введ. 2000-01-01. М.: Изд-во стандартов, 1999. 11 с.
10. Доктрина информационной безопасности Российской Федерации: [утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895] [Электронный ресурс].- Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/min_bezop/doctr.shm.
11. Терминология в области защиты информации: справочник. М.: ВНИИ «Стандарт», 1993. 110 с.
12. Хорев А.А. Техническая защита информации: учебное

пособие для студентов вузов. В 3-х томах / Т. 1. Технические каналы утечки информации. М.: НППЦ «Аналитика», 2008. 436 с.: ил.

13. Петраков А.В., Лагутин В.С. Защита абоненского телетрафика: учебное пособие. 3-е изд., испр. и доп. М.: Радио и связь, 2004. 504 с.

14. Шеннон К. Математическая теория связи. Работы по теории информации и кибернетике. М.: ИИЛ, 1963. 830 с.

15. Шрейдер Ю.А. О семантических аспектах теории информации. Информация и кибернетика. М.: Сов. Радио, 1967. 324 с.

16. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. Москва, 1992.

17. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.

18. Щеглов А.Ю. Защита информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.: ил.

19. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. М.: Издательский дом «Вильямс», 2001. 672 с.

СВЕДЕНИЯ О МФГС

На неформальном саммите СНГ 8 мая 2005 г. была подписана Декларация о гуманитарном сотрудничестве, которая предусматривала создание Межгосударственного фонда гуманитарного сотрудничества государств-участников СНГ.

На заседании Совета глав правительств СНГ 25 мая 2006 г. в Душанбе семью государствами – Республикой Армения, Республикой Беларусь, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Узбекистаном, -- был подписан Договор о создании Межгосударственного фонда гуманитарного сотрудничества государств-участников СНГ (МФГС). В июне 2008 г. к Договору о Фонде присоединилась Азербайджанская Республика.

МФГС является межгосударственной некоммерческой организацией. Высший орган Фонда – Правление, членами которого являются полномочные представители государств-участников Фонда.

Место нахождения Исполнительной дирекции Фонда – г. Москва.

Цель Фонда -- создание благоприятных возможностей для развития гуманитарного сотрудничества как на пространстве государств-участников Договора о Фонде, так и на уровне каждой из стран Содружества.

Миссия МФГС как специализированной организации в области гуманитарного сотрудничества на пространстве СНГ – способствовать развитию общего гуманитарного пространства и межкультурного диалога в Содружестве посредством образования, науки, культуры, массовых коммуникаций, информации, архивного дела, спорта, туризма и работы с молодежью.

Стратегическим направлением деятельности МФГС является проведение межгосударственных мероприятий, способствующих

развитию межкультурного диалога на пространстве Содружества.

В деятельности МФГС приоритетное внимание уделяется разработке и осуществлению на регулярной основе во всех государствах-участниках МФГС крупных многоцелевых проектов, реализации мероприятий, отвечающих тематике гуманитарных годов в СНГ, а также стимулирующих развитие продуктивных контактов в научно-образовательной и творческой общественной среде.

МФГС руководствуется принципами разнообразия, равноправия, учета интересов каждого из участников стран Содружества, которые строятся на основе междисциплинарного подхода. Эти принципы тесно связаны с такими ценностями как справедливость, солидарность, терпимость, равенство, уважение прав человека.

МФГС работает в тесном взаимодействии с Советом по гуманитарному сотрудничеству государств-участников СНГ (СГС), с которым он согласует план своей работы.

**Межгосударственный фонд гуманитарного сотрудничества
государств-участников СНГ (МФГС)**

Адрес: 119049, Россия, г.Москва 1-ый Спасоналивковский пер., д.4

Телефон: +7 (495) 411-61-28; Факс: +7 (499) 238-06-76

<http://www.mfgs-sng.org>

Учебное пособие

**Баскаков Игорь Владимирович, Евсеев Владимир Леонович,
Пролетарский Андрей Викторович, Суоров Александр Михайлович**

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Редактор *А.К. Ковальчук*
Технический редактор *В.В. Яроц*
Компьютерная верстка *О.И. Трифонова*



Межотраслевой институт повышения квалификации кадров по новым
направлениям развития техники и технологии
МГТУ им. Н.Э.Баумана

Бумага офсетная. Гарнитура "Times New Roman".
Формат 60×90/16. Объем 22,63 п.л.
Тираж 500 экз. Заказ № 358

Отпечатано в типографии МГТУ им. Н.Э.Баумана
105005, Москва, 2-ая Бауманская ул., д.5
baumanprint@gmail.com
Тел.: 8 (499) 267-32-83