МВД России
Санкт-Петербургский университет

ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ

Курс лекций

Санкт-Петербург
2020

План 2020, поз. 17

УДК 004
ББК 32.97
К 88

Куватов В. И., Чудаков О. Е., Родин В. Н.

К 88 Программно-аппаратная защита информации: курс лекций. — Санкт-Петербург: Изд-во СПб ун-та МВД России. — 192 с.

ISBN 978-5-91837-307-1

Курс лекций соответствует программе учебной дисциплины «Программно-аппаратная защита информации». В содержании рассмотрены методы и средства программно-аппаратной защиты информации, особенности их применения для обеспечения информационной безопасности компьютеров, компьютерных систем и сетей. Дается классификация средств и систем программно-аппаратной защиты информации. Анализируются угрозы, источники угроз, уязвимые компоненты средств вычислительной техники и автоматизированных систем.

Предназначен для обучающихся в образовательных организациях системы МВД России.

УДК 004
ББК 32.97

Рецензенты:
Думачёв В. Н., кандидат физико-математических наук, доцент
(Воронежский институт МВД России);
Локтионов О. В., кандидат технических наук
начальник Центра информационных технологий,
связи и защиты информации ГУ МВД
по г. Санкт-Петербургу и Ленинградской области

ISBN 978-5-91837-307-1

СОДЕРЖАНИЕ

Список сокращений и обозначений

АС — автоматизированные системы
АСУ — автоматизированные системы управления
ЗУ — запоминающие устройства
ИС — информационные системы
КС — компьютерные системы
НСД — несанкционированный доступ
ОС — операционная система
ПАЗИ — программно-аппаратная защита информации
ПАСЗИ — программно-аппаратные средства защиты информации
ПК — персональный компьютер
СВТ — средства вычислительной техники
СЗИ — средства защиты информации
СЗКИ — система защиты кофиденциальной информации
СПД — система передачи данных
СУБД — системы управления базами данных
ТО МВД России — территориальные органы МВД России
ЦП — центральный процессор

Введение

Задачи обеспечения информационной безопасности, по мере перехода различных государственных и коммерческих структур на компьютерные методы хранения, обработки и передачи данных становятся все более важными, а в некоторых сферах (оборона, правоохранительная деятельность, дипломатические отношения, экономика и пр.) — критически важными. Надежное обеспечение информационной безопасности может быть достигнуто только при комплексном подходе, включающем все средства, способы и методы защиты информации. В частности, система защиты информации немыслима без программно-аппаратных методов и средств защиты информации.

Данное издание посвящено вопросам программно-аппаратной защиты информации в средствах вычислительной техники, автоматизированных системах и сетях передачи данных. Курс лекций разработан в соответствии с:

— Федеральными государственным образовательным стандартом высшего образования, основной образовательной и рабочими учебными программами по специальности: 10.05.05 — Безопасность информационных технологий в правоохранительной сфере;

— требованиями Приказа Министерства образования и науки России от 19 декабря 2013 г. № 1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования — программам бакалавриата, программам специалитета, программам магистратуры».

Курс лекций содержит:

— перечень угроз, каналов утечки и уязвимостей программно-аппаратных средств защиты информации (ПАСЗИ);

— формализованные требования к ПАЗИ;

— классификацию ПАСЗИ;

— методы аутентификации, идентификации и разграничения доступа субъектов к объектам ПАЗИ;

— средства и методы защиты информации в компьютерных сетях;

— разрушающие программные воздействия (включая компьютерные вирусы) и защиту от них;

— новые средства и системы ПАЗИ;

— основы экспертного оценивания программ и данных.

Предназначен для обучающихся в образовательных организациях системы МВД России по специальности 10.05.05 — Безопасность информационных технологий в правоохранительной сфере.

Лекция 1. Предмет и задачи программно-аппаратной защиты информации

Вопросы лекции:

1.1 Место программно-аппаратной защиты информации в системе информационной безопасности.

1.2 Объект и предмет программно-аппаратной защиты информации.

1.3 Назначение и состав системы программно-аппаратной защиты информации.

1.4. Эшелонированная оборона.

Система информационной безопасности представляет собой взаимоувязанное множество методов и средств защиты информации, различающихся по природе и задачам, для решения которых они предназначены. Одной из важнейших составных частей этого множества является подмножество методов и средств программно-аппаратной защиты информации (ПАЗИ).

Особенность ПАЗИ заключается в том, что с некоторыми ее методами и средствами сталкивается практически каждый пользователь компьютера. Это имена и пароли, которые мы вводим при включении своего персонального компьютера, антивирусные средства, которые мы используем для защиты от компьютерных вирусов, средства удаления файлов, средства восстановления ошибочно удаленных файлов и т. д.

Другая особенность заключается в исключительно большом разнообразии методов и средств ПАЗИ, в появлении все новых и потери интереса к старым методам и средствам в ходе научно-технического прогресса. Эта особенность обуславливает целесообразность изучения базовых принципов программно-аппаратной защиты с практическим освоением только наиболее перспективных программно-аппаратных методов и средств.

1.1. Место программно-аппаратной защиты информации в системе информационной безопасности

В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» говорится о трех направлениях защиты информации: правовом, организационном и техническом. Специалисты по защите информации придерживаются более детальной классификации. Они считают, что система защиты информации представляет собой взаимоувязанное подмножество правовых, организационных, морально-этических, страхо-

вых, технических, физических, криптографических, стеганографических и программно-аппаратных методов и средств обеспечения информационной безопасности (рис. 1.1). Некоторые специалисты выделяют психологические методы.

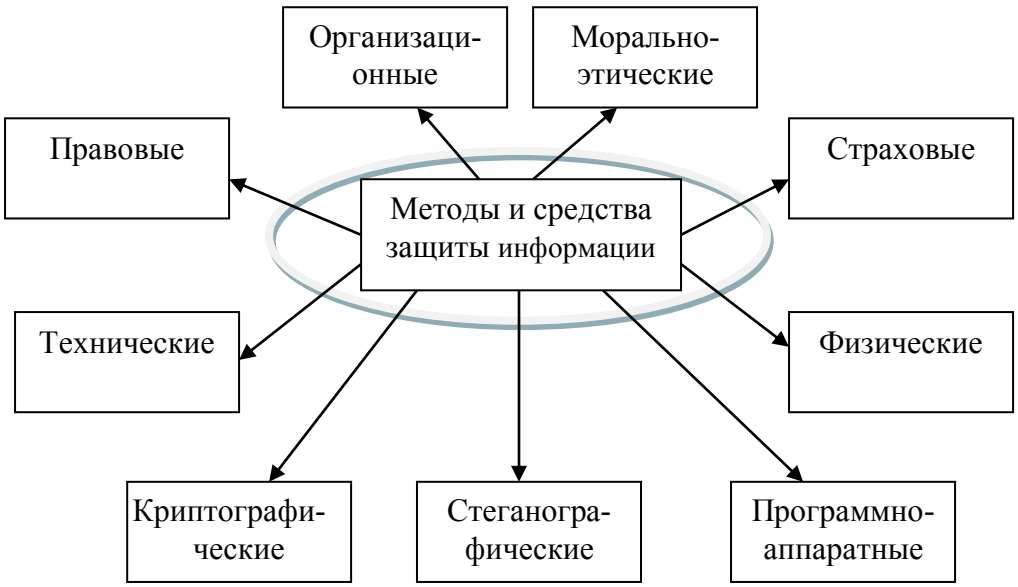

Рис. 1.1. Методы и средства обеспечения информационной безопасности

Все перечисленные методы и средства делятся на два класса: формальные и неформальные.

Формальные методы реализуются техническими устройствами или компьютерными программами, функционирующими по встроенным в них алгоритмам. К формальным методам относятся: технические, криптографические, стеганографические, программно-аппаратные методы и средства.

Неформальные методы реализуются (проводятся) людьми или правилами (законами, актами, нормами и т. д.), регламентирующими деятельность людей или функционирование программно-аппаратных средств. К неформальным методам относятся: правовые (нормативно-правовые), морально-этические нормы, организационные меры и страховые методы. Страховые методы представляют собой достаточно новое направление и пока не описаны в учебниках по информационной безопасности.

Физические методы являются как формальными, поскольку они предполагают технические устройства, препятствующие доступу злоумышленников на охраняемую территорию, так и неформальными,

поскольку они предполагают наличие людей, выполняющих определенные функции по контролю охраняемой территории.

Одним из важнейших видов формальных методов и средств защиты информации являются программно-аппаратные методы и средства. Программно-аппаратные методы и средства предназначены для защиты информации, хранящейся и обрабатываемой в компьютерах и КС, передаваемой по каналам связи компьютерных сетей.

Для этих же целей могут применяться криптографические и стеганографические методы и средства. Граница между программно-аппаратной, криптографической и стеганографической защитой информации с точки зрения целей размыта. Поэтому ряд специалистов относит криптографию к программно-аппаратным методам и средствам. Некоторые специалисты к программно-аппаратным методам и средствам относят также и стеганографию.

Мы будем исходить из того, что программно-аппаратные, криптографические и стеганографические средства принципиально различаются по методам, положенным в их основу. Поэтому будем считать программно-аппаратную, криптографическую и стеганографическую защиту разными видами обеспечения безопасности информации.

1.2. Объект и предмет программно-аппаратной защиты информации

Объект программно-аппаратной защиты. Программно-аппаратная защита информации, как и каждая научная дисциплина, имеет свой объект и предмет. В руководящих документах по информационной безопасности Федеральной службы по техническому и экспортному контролю (ФСТЭК, ранее государственная техническая комиссия — ГТК) указаны два *различающихся между собой класса объектов* программно-аппаратной защиты информации: средства вычислительной техники (СВТ) и автоматизированные системы (АС).

Под СВТ понимают совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. К СВТ относят автономные компьютеры, устройства ввода/вывода данных, встроенные и автономные устройства хранения данных, ОС ЭВМ, системы управления базами данных (СУБД), прикладное программное обеспечение и пр.

Под АС понимают полнофункциональные системы, предназначенные для обработки данных или для управления. При этом различают два вида автоматизированных систем управления: АСУ органи-

зационного типа (предприятием, организацией, министерством и пр.) и АСУ технологическими процессами (производственной линией, станком и пр.). Структура объекта ПАЗИ приведена на рис. 1.2.

Рис. 1.2. Структура объекта программно-аппаратной защиты информации

Специалисты в области информационной безопасности часто понятие «автоматизированная система» отождествляют с понятиями «компьютерная система» или «информационная система». Мы также будем отождествлять эти понятия там, где различия между ними не носят принципиального характера.

Материальной основой хранения и передачи информации в КС являются электронные и электромеханические устройства ввода/вывода, системы передачи данных и машинные носители информации. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в КС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней иерархии, преобразуется (обрабатывается) центральными процессорами (ЦП) 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 носите-

лей информации использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты.

Большинство типов машинных носителей информации являются съемными, т. е. могут сниматься с устройств и использоваться (бумага) или храниться (ленты, диски, бумага) отдельно от устройств. Таким образом, для защиты информации в КС необходимо защищать устройства ввода/вывода, устройства передачи данных и машинные носители от несанкционированных (неразрешенных) воздействий на них.

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

При решении проблемы защиты информации в КС необходимо учитывать также противоречивость человеческого фактора. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию. Понятие «объект защиты» или «объект» часто трактуется в более широком смысле, чем это показано на рис. 1.2. Для сосредоточенных КС 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.

Первичными понятиями программно-аппаратной защиты информации являются понятия «информационная безопасность», «безопасность информации в компьютерных системах» и «защищенные компьютерные системы». Поясним эти понятия.

Информационная безопасность — состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечивается их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз.

Безопасность информации в КС — это такое состояние всех компонент КС, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

Защищенные КС — это системы, в которых обеспечивается безопасность информации.

В современных условиях информационная безопасность является одним из наиболее важных направлений обеспечения безопасности личности, общества и государства. Безопасность информации достигается проведением руководством государства, ведомства, организации адекватной политики информационной безопасности. Политика информационной безопасности разрабатывается и принимается как официальный руководящий документ органами управления государством, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В руководящих документах по информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

До использования компьютерных сетей основная часть обработки и обмена данными была централизована, информация и управление ей были сосредоточены в одном месте. Компьютерные сети логически и физически рассредоточили данные, а также вычислительную мощность и службы обмена сообщениями по всей организации. Поэтому службы безопасности, защищающие данные, средства, также должны быть рассредоточены.

Предмет ПАЗИ. Предметом ПАЗИ в КС является информация. Информация имеет ряд особенностей:

— она нематериальна, не имеет массы и энергии;

— информация хранится и передается с помощью материальных носителей (мозг человека, звуковые и электромагнитные волны, машинные носители и т. п.);

— любой материальный объект содержит информацию о самом себе или о другом объекте.

Информации присуще множество свойств, которые можно поделить на общие и специфические свойства. Наиболее важными общими свойствами информации являются ее количество, ценность и полезность.

Количество информации. Количество информации в сообщении оценивается в битах по формуле Шеннона:

$$I = -\sum_{i=1}^{n} P_i log_2(P_i),$$

где: n — количество символов сообщения, P_i — вероятность возникновения в сообщении i-го символа. В случае равновероятных исходов (все вероятности P_i равны между собой) формула Шеннона преобразуется в формулу Хартли

$$I = log_2(n).$$

Ценность информации. Информация добывается с целью получения прибыли или преимуществ перед конкурентами, противоборствующими сторонами. Следовательно, информация имеет ценность. Ценная информация покупается и продается, и ее правомочно рассматривать как товар.

Ценность информации определяется степенью ее полезности для владельца (пользователя). Информация может быть ценной для ее владельца, но не иметь цены для других. Например, сведения о состоянии здоровья обычного гражданина являются ценной информацией для него. Но эта информация, скорее всего, не заинтересует постороннего человека, и не будет иметь для него цены.

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

$$C(t) = C_0 e^{-2.3t/\tau},$$

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

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.

Полезность информации. Цена информации, связана с ее полезностью для конкретных людей, организаций, государств. Полезность информации, помимо прочего, зависит от способности человека ее воспринять. Одна и та же информация может быть бесполезной

в двух случаях: когда она уже известна или когда человек не способен ее воспринять.

Информация может быть получена тремя путями:

— проведением научных исследований;

— покупкой информации;

— противоправным добыванием информации.

Специфическими свойствами информации, определяющими ее безопасность, являются конфиденциальность, целостность и доступность. Поясним эти свойства.

Конфиденциальность. Законом «Об информации, информационных технологиях и о защите информации» гарантируется право собственника 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, коммерческую, служебную и т. п. тайну.

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».

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. Для обозначения ценности конфиденциальной коммерческой информации используются три категории: «коммерческая тайна — строго конфиденциально», «коммерческая тайна — конфиденциально» и «коммерческая тайна». Используется и другой подход к градации ценности коммерческой информации: «строго конфиденциально — строгий учет», «строго конфиденциально». Существуют соответствующие градации и других видов тайн.

Целостность информации означает, что она не изменялась в ходе ее передачи или хранения. Понятие целостности тесно коррелирует с понятием истинности (достоверности). Истинной или достоверной является та информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках. Ин-

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

Доступность информации означает возможность создавать, уничтожать, изменять, читать ее тем должностным лицам, которым это положено в соответствии с политикой безопасности, принятой в организации.

1.3. Назначение и состав системы программно-аппаратной защиты информации

Программно-аппаратная защита информации предназначена для защиты информации, обрабатываемой (хранящейся) на средствах вычислительной техники и в автоматизированных системах. Толкование понятий СВТ и АС приведено нами ранее.

В соответствии с современными взглядами ПАЗИ включает в свой состав: систему идентификации, аутентификации и авторизации, систему разграничения и контроля доступа, систему регистрации событий безопасности, межсетевые экраны, систему обнаружения и предотвращения вторжений (IDS), сканеры безопасности, систему обеспечения целостности информации, виртуальные частные сети, систему защиты программ от исследования, систему защиты программ от компьютерных вирусов, специализированные многофункциональные системы программно-аппаратной защиты — UTM и DLP-системы, систему защиты от привилегированных пользователей (PIM,PUM, PAM систему), и SIEM систему (рис. 1.3). Кроме того, в состав системы защиты информации входят: средства доверенной загрузки, средства контроля съемных носителей, средства гарантированного удаления информации, средства восстановления ошибочно удаленной информации.

Рис. 1.3. Состав системы программно-аппаратной защиты информации

На рис. 1.3 отсутствуют средства криптографической и стеганографической защиты, которые, как отмечено ранее, некоторые специалисты также включают в состав программно-аппаратных средств. Кроме того, на этом рисунке в состав программно-аппаратной защиты включены относительно новые классы систем — централизованные системы мониторинга информационной безопасности (Security information and event management — SIEM) и системы защиты информации от привилегированных пользователей (PIM, PUM, PAM системы).

SIEM — это объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информационной безопасностью и SEM (Security event management) — управление событиями безопасности. Как видно из названия SIEM «сама по себе» не способна что-то предотвращать или защищать. Она предназначена для анализа информации, поступающей от других систем, таких как DLP, IDS, UTM, антивирусов, раз-

личных аппаратных средств (маршрутизаторы и т. д.) и дальнейшего выявления отклонения от норм по каким-то критериям. Эти системы позволяют централизованно собирать и анализировать поток событий, поступающих со всех имеемых на объекте средств защиты. В настоящее время (2020) SIEM системы имеются у 23 % крупных российских компаний. Процесс их внедрения в России идет достаточно активно. Пока для системы защиты информации от привилегированных пользователей (прежде всего от системных администраторов) нет установившихся российских терминов. Поэтому эти системы часто так и называют — PAM, PIM, PUM системы. PAM расшифровывается как Privileged Access Management, PIM — Privileged Identify Management, а PUM — Privileged User Management. Самый ранний сертификат ФСТЭК для системы защиты информации от привилегированных пользователей был получен в 2014 году.

Поясним еще два термина, показанные на рис. 1.3: DLP и UTM.

DLP (Data Leak Prevention) — система предотвращения утечек из ИС. Обеспечивает предотвращение утечек конфиденциальной информации за периметр организации, выявление угроз информации, контроль деятельности персонала и т. п.

UTM (Unified Threat Management) — система, обеспечивающая мощную комплексную защиту организации от внешних сетевых угроз. Объединяет межсетевой экран, VPN, систему предотвращения вторжений, защиту от вирусов, от программ-шпионов, от спама. По желанию в состав UTM системы можно включать и другие программные средства.

Классификация систем и средств, входящих в состав программно-аппаратной защиты, приведенная на рис. 1.3, выполнена по функциональному признаку. По месту нахождения некоторые из этих систем и средств являются автономными, входят в состав ОС, комплексируются в специализированные (добавочные) программно-аппаратные системы защиты компьютерной информации — UTM системы, в DLP-системы.

Системы и средства можно классифицировать по иерархическому принципу: на нижнем уровне иерархии находятся средства защиты, ориентированные на решение одной задачи: средства контроля съемных носителей, средства гарантированного удаления информации, средства восстановления ошибочно удаленной информации, межсетевые экраны, системы обнаружения и предупреждения вторжений,

виртуальные частные сети, сканеры безопасности и пр. На втором уровне иерархии находятся многофункциональные системы, такие как DLP и UTM-системы, ОС компьютеров и компьютерных сетей. Эти многофункциональные системы включают в свой состав некоторые или все средства нижнего уровня. На верхнем уровне иерархии находится программно-аппаратная система защиты информации, которая включает себя системы второго уровня.

На рис. 1.4 показан процент наиболее распространенных систем и средств ПАЗИ, развернутых в российских компаниях.

Из рисунка следует, что межсетевой экран стоит у 88 % участников опроса. VPN шлюз используют 59 % компаний. Данная защита востребована у компаний топливно-энергетического комплекса (60 % компаний) и в финансовом секторе (56 % компаний). Система обнаружения вторжений имеется у 40 % компаний, причем она имеется у половины компаний здравоохранения и информационных технологий. VPN шлюз с поддержкой ГОСТ имеется у 31 % компаний и UTM решение — у 20 %. Заметим, что в качестве респондентов выступали только крупные российские компании.

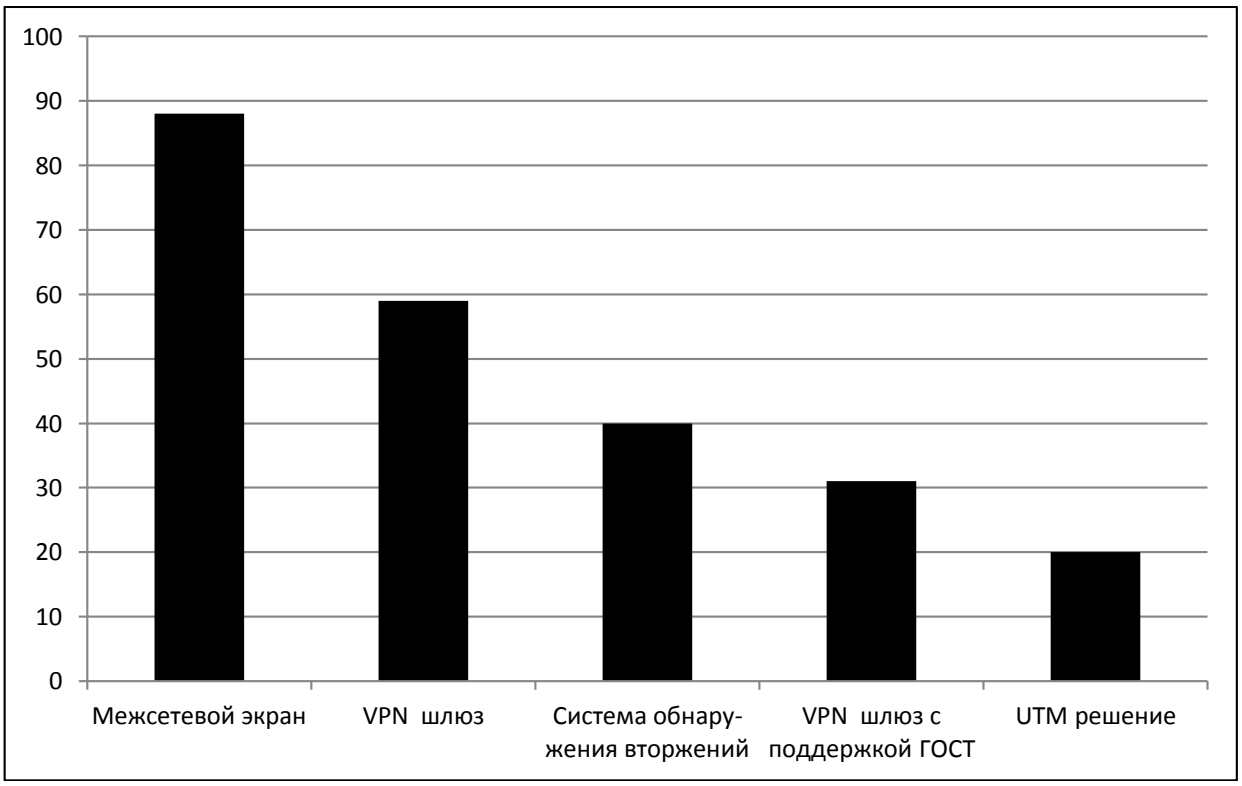

Рис. 1.4. Процент СЗИ, развернутых в российских компаниях (2020)

1.4. Эшелонированная оборона

В теории ПАЗИ часто используют термин эшелонированная оборона (defense in depth) или многоуровневая защита — что одно и то же. Эшелонированная оборона представляет собой иерархически организованный набор уровней защиты КС. На каждом уровне устанавливаются свои средства и применяются свои методы защиты информации. Правильный выбор средств и методов, их правильная настройка позволяют создать «хорошую» систему защиты информации. Один из вариантов эшелонированной обороны представлен на рис. 1.5.

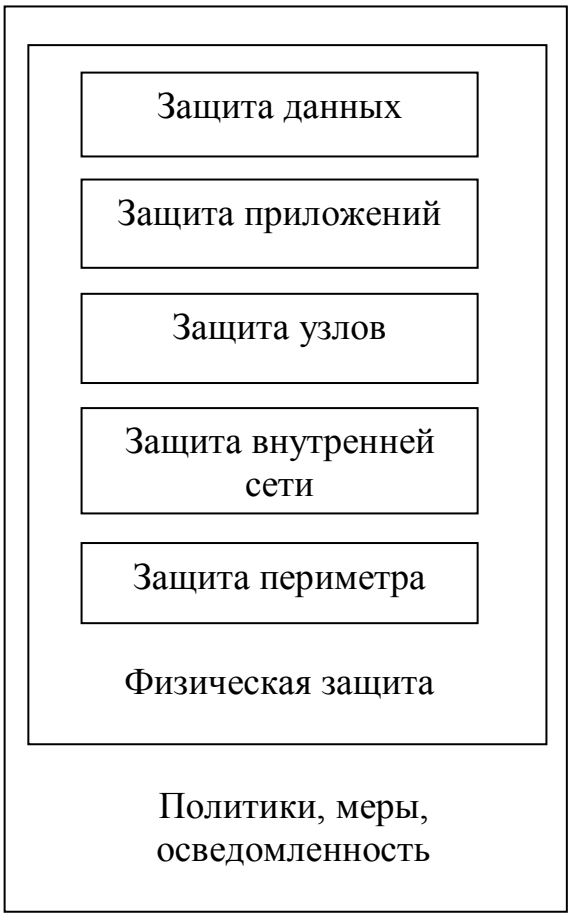

Рис. 1.5. Модель многоуровневой защиты

Поясним этот рисунок.

Политика безопасности описывает все аспекты работы системы с точки зрения информационной безопасности. Уровень политики безопасности является базовым. Он подразумевает наличие документированных организационных мер защиты и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и т. п. (см., например, стандарт ISO/IEC 17799).

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы: защита помещений, видеонаблюдение, контроль доступа.

Уровень защиты периметра включает меры безопасности в точках входа в защищаемую сеть. Именно начиная с этого уровня, применяются программно-аппаратные средства защиты. Классические средства защиты периметра — это межсетевой экран, система обнаружения вторжений, средства антивирусной защиты для шлюзов безопасности.

Уровень защиты внутренней сети ведает обеспечением безопасности внутреннего трафика и сетевой инфраструктуры. Это виртуальные локальные сети, протоколы IPSec и т. д. На этом уровне могут быть использованы те же средства, что и средства защиты периметра, например, межсетевые экраны.

Уровень защиты узлов защищает от атак на отдельные узлы сети. На этом уровне первоочередное внимание уделяется защите ОС: настройкам, повышающим безопасность конфигурации (отключению неиспользуемых потенциально опасных служб), организации установки исправлений и обновлений, идентификации и аутентификации пользователей. Важную роль на этом уровне играет антивирусная защита.

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения: почтовые и web-серверы, серверы баз данных и пр. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты на этом уровне используются настройки безопасности самих приложений, установка обновлений, антивирусная защита.

Уровень защиты данных определяет порядок защиты обрабатываемых и хранящихся данных от НСД и других угроз. Это может быть шифрование данных при хранении и передаче, разграничение доступа к данным средствами файловой системы.

В ходе идентификации рисков определяется, что является целью нарушителя, на каком уровне или на каких уровнях защиты ему лучше противостоять. В соответствии с этим выбираются и контрмеры. При этом учитывается, что защита от угрозы на нескольких уровнях снижает вероятность ее реализации, а значит и уровень риска, но удорожает систему защиты.

Действительно, пусть для защиты от i-й угрозы предполагается использовать средства защиты на двух уровнях. Пусть средство, устанавливаемое на j-м уровне, стоит C_{ij}, и защищает от этой угрозы с вероятностью P_{ij}. Тогда вероятность защиты от i-й угрозы будет $P_i = 1 - (1 - P_{i1})(1 - P_{i2})$, а стоимость $C_i = C_{i1} + C_{i2}$.

Концепция эшелонированной обороны в настоящее время является общепринятой, поэтому производители средств защиты информации реализуют ее выпуском целых линеек защитных средств, которые функционируют совместно и управляются, как правило, единым устройством управления.

Контрольные вопросы:

1. Определите место ПАЗИ в системе информационной безопасности.
2. Что является объектом и предметом ПАЗИ?
3. Назовите назначение и состав системы ПАЗИ.
4. Что включает в себя модель многоуровневой защиты?

Лекция 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации

Вопросы лекции:

2.1. Угрозы информации и источники угроз.

2.2. Уязвимые компоненты компьютеров, компьютерных систем и сетей.

2.3. Виды и статистика нарушений информационной безопасности компьютерных систем и сетей.

Описанию программно-аппаратных средств защиты информации, показанных на рис. 1.3, посвящен настоящий курс лекций. Однако, чтобы лучше понимать от чего защищают эти средства, начнем с анализа основных угроз, каналов утечки и уязвимостей средств вычислительной техники и автоматизированных систем.

2.1. Угрозы информации и источники угроз

Ранее мы привели некоторые термины из области информационной безопасности. В частности, мы привели понятие информационной безопасности как состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечивается их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз. С позиций данного определения угроза информации есть совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества, государства (Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности»). Под угрозой информации в СВТ и АС понимается возможность возникновения на какомлибо этапе ее жизненного цикла такого события, следствием которого могут быть негативные воздействия на информацию. Способность СВТ (АС) выполнять свои функции при воздействии на нее случайных или умышленных угроз называется безопасностью СВТ (АС).

Угроза информации может быть, а может и не быть реализована. Реализация угрозы называется атакой. Атаки могут быть направлены на автономный персональный компьютер, автономное автоматизиро-

ванное рабочее место[1] (АРМ) или сеть АРМ, объединенных в локальную вычислительную сеть (ЛВС).

Атаки преследуют цели нарушения конфиденциальности, целостности и доступности информации. Напомним, что под конфиденциальностью понимается невозможность случайного или преднамеренного доступа к информации нелегальным пользователем, под целостностью — невозможность случайного или преднамеренного изменения информации нелегальным пользователем, под доступностью — невозможность в отказе от доступа к информации легальному пользователю.

Рассмотрим еще некоторые термины, введенные ГОСТами (Национальный стандарт РФ. ГОСТ Р. 50922-2006. «Защита информации. Основные термины и определения». Утвержден Приказом Росстандарта РФ от 27.12.2006 г. № 373-ст; Национальный стандарт РФ. ГОСТ Р. 512754-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Утвержден Приказом Росстандарта РФ от 27.12.2006 г. № 374-ст) и руководящими документами ФСТЭК (Руководящий документ ФСТЭК «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением Председателя ГосТехКомиссии от 30.03.1992 г.).

Фактор, воздействующий на защищаемую информацию, это явление, действие или процесс, результатом которого могут быть утечка (нарушение конфиденциальности), искажение, уничтожение (нарушение целостности) защищаемой информации, блокирование доступа (нарушение доступности) к ней.

Источник угрозы безопасности информации — субъект (физическое лицо, либо материальный объект или физическое явление), являющееся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость (брешь) информационной системы — свойство ИС, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

---

[1] Согласно ГОСТ 34.003-90 («Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения») автоматизированное рабочее место (АРМ) — это программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. Основным элементом автоматизированного рабочего места являются персональный компьютер (в том числе монитор, принтер и другие внешние устройства) с установленным на нем программным обеспечением.

Основными источниками угроз информационным ресурсам являются:

— различные виды разведок иностранных государств, криминальных структур и конкурентов;

— собственный недобросовестный персонал;

— стихийные бедствия и другие форс-мажорные обстоятельства.

Планируя мероприятия по защите информации, следует представлять от кого необходимо защищаться, кто является потенциальным нарушителем — источником угроз. В общем случае это: хакеры, шпионы, террористы, охотники за промышленными секретами, организованные преступные сообщества, вандалы, собственные сотрудники. Защищаться необходимо не от всех собственных сотрудников, а от уволенных и обиженных: системных администраторов, сотрудников службы безопасности, «продвинутых» пользователей. В таблице 2.1 отображена структура источников угроз информационной безопасности.

Таблица 2.1

Структура источников угроз информационной безопасности информации (2020)

Вид угрозы	**Значимость угрозы (в %)**
Конкуренты, криминальные структуры, хакеры	17 %
Случайные люди	1 %
Собственные сотрудники из них: – уволенные или уволившиеся сотрудники; – сотрудники, состоящие в штате	82 % – 34 % 42 %

Как следует из данной таблицы, 82 % источников угроз — внутренние нарушители и лишь порядка 17 % — внешние. Причем из 82 % внутренних источников угроз порядка 34 % это уволенные или уволившиеся сотрудники и 48 % — сотрудники, состоящие в штате. Как видим, основные угрозы нарушению информационной безопасности исходят от сотрудников организации. В связи с этим определенный интерес представляет вопрос о том, какие события предшествуют угрозам информационной безопасности со стороны сотрудников. Статистические данные показывают, что внутреннему нарушению информационной безопасности предшествуют события, связанные: с увольнением (47 %), не повышением в должности (20 %), конфликтом (20 %), другими событиями (13 %).

Нарушители классифицируются также по уровню возможностей, предоставляемых им штатными средствами СВТ и АС. По этому признаку выделяют четыре уровня нарушителей.

Первый (самый низкий) уровень — нарушитель может запускать задачи из фиксированного набора, реализующие заранее предусмотренные функции по обработке информации. *Второй* уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации. *Третий* уровень определяется возможностью управления функционированием АС, т. е. воздействием на базовое программное обеспечение системы, на состав и конфигурацию ее оборудования. *Четвертый* уровень определяется возможностью осуществлять проектирование, реализацию и ремонт технических средств АС вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке данных. В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС, в том числе и о системе ее защиты.

Классификация угроз информации

Этапы выявления и анализа угроз играют исключительно важную роль при создании и модернизации систем информационной безопасности СВТ и АС, так как на их основе формируется требования к этим системам и политика безопасности. Классификация угроз информационной безопасности СВТ и АС приведена в таблице 2.2.

Таблица 2.2

Классификация угроз безопасности информации

<table>
<tr><th>Классификационный признак</th><th colspan="4">Классификация угроз по данному признаку</th></tr>
<tr><td>По положению источника</td><td colspan="2">Внешние</td><td colspan="2">Внутренние</td></tr>
<tr><td>По природе возникновения</td><td>Внешние случайные</td><td>Внешние преднамеренные</td><td>Внутренние преднамеренные</td><td>Внутренние случайные</td></tr>
<tr><td>По виду источника</td><td colspan="2">Природа</td><td>Нарушитель</td><td>Персонал</td></tr>
<tr><td>По способу воздействия угрозы</td><td colspan="2">Несанкционированный доступ к информации нарушителем или персоналом</td><td colspan="2">Перехват информации по техническим каналам утечки нарушителем или персоналом</td></tr>
<tr><td>По объекту воздействия</td><td>Воздействует на внешние каналы из сети «Интернет»</td><td>Воздействует на АРМ персонала из ЛВС</td><td>Кража печатных материалов или магнитных носителей</td><td></td></tr>
<tr><td>По результату воздействия</td><td>Нарушение конфиденциальности</td><td>Нарушение целостности</td><td>Нарушение доступности</td><td></td></tr>
</table>

Поясним эту таблицу.

По положению источника угроз. Внутренние угрозы, источник которых расположен в пределах территориального расположения основ-

ных элементов КС (в пределах предприятия). Внешние угрозы, источник которых расположен вне территориального расположения основных элементов КС, т. е. вне предприятия. Например, в условиях рыночной экономики, когда существует реальная конкуренция между организациями, у них возникает интерес к деятельности соперничающих фирм. Целью этого интереса является добывание информации, относящейся к коммерческой тайне: о замыслах, финансовом состоянии, клиентах, ценах и т. д. Получение такой информации и ее использование конкурентами может причинить существенный ущерб фирме.

По природе возникновения внешние и внутренние угрозы могут быть как преднамеренными угрозами (заранее планируются кем-то), так и случайными угрозами (не планируются заранее, возникают неожиданно).

По виду источника угроз: **у**грозы могут исходить от природной среды, от нарушителя, от персонала или от программно-аппаратных средств. Например, преднамеренные угрозы представляют собой либо нарушителя (внешнего нарушителя безопасности информации), либо завербованный персонал предприятия (внутренний нарушитель безопасности информации).

Случайные угрозы представляют собой либо природную среду (стихийное бедствие, пожар), либо персонал, который по своей халатности может совершить ошибку, повлекшую за собой нарушение безопасности информации, либо программно-аппаратные средства, в процессе эксплуатации которых может произойти отказ в следствие их старения или неправильного использования, либо в результате ошибок, допущенных в ходе их разработки.

Преднамеренные угрозы безопасности информации в лице нарушителя или завербованного персонала осуществляются, как правило, через перехват информации по техническим каналам утечки информации или через несанкционированный доступ.

Следовательно, *по способу воздействия* на защищаемую информацию угрозы делятся на угрозы перехвата информации по техническим каналам утечки информации и угрозы несанкционированного доступа к информации. Поскольку угрозы перехвата информации по техническим каналам утечки информации рассматриваются в техническом направлении защиты информации, остановимся только на угрозах несанкционированного доступа к информации.

Несанкционированный доступ — доступ к информации, нарушающий правила разграничения доступа с использованием штат-

ных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники и автоматизированных систем.

НСД может осуществляться:

1. На уровне сети «Интернет», где объектом воздействия являются внешние каналы связи, для которых возможен:

— перехват передаваемых данных с целью их хищения, модификации, разрушения или переадресации;

— несанкционированное отправление данных от имени другого пользователя;

— отрицание пользователями подлинности данных, а также фактов отправления или получения информации.

Для защиты информации от угрозы НСД на уровне сети «Интернет» в настоящее время применяются в основном криптографические и стеганографические средства защиты информации.

2. На уровне ЛВС, где объектом воздействия являются АРМ сотрудников, для которых возможно:

— хищение, искажение, подлог и разрушение информации;

— внедрение программных закладок и компьютерных вирусов;

— нарушение работоспособности программно-аппаратных средств компьютера.

2.2. Уязвимые компоненты компьютеров, компьютерных систем и сетей

Уязвимые компоненты аппаратной части средств вычислительной техники и автоматизированных систем

Угрозы реализуются через уязвимые компоненты СВТ и АС. Под уязвимыми компонентами понимаются любые компоненты СВТ и АС, обладающие недостатками, которые могут привести к нарушению безопасности хранения, передачи и обработки информации. Обобщенные уязвимые компоненты с соответствующими им видами угроз представлены на рис. 2.1. На этом рисунке двойными стрелками показаны информационные потоки между уязвимыми элементами, а одинарными — виды угроз, актуальные для уязвимых компонентов.

Рис. 2.1. Уязвимые компоненты компьютерной системы и виды угроз

Как следует из рис. 2.1, к уязвимым компонентам СВТ и АС относятся:

— персональный компьютер с установленным на нем программным обеспечением;

— монитор;

— принтер, ксерокс;

— различные внешние запоминающие устройства;

— аппаратура связи и коммутации.

Уязвимости, характерные для каждого из этих компонент, отображены в прямоугольниках во внешней части рис. 2.1 мелким шрифтом. Уязвимости, характерные для линий связи между внешними устройствами и центральной частью компьютера: перехват потока данных и регистрация излучений — отображены крупным шрифтом внутри рисунка.

Уязвимости операционных систем

Одним из наиболее уязвимых компонентов КС, является программное обеспечение ПК, так как с его помощью возможен доступ к любым компьютерным ресурсам. Рассмотрим классификацию программного обеспечения ПК по областям их использования, для чего выделим три класса программных продуктов: пакеты прикладных программ, системное ПО, инструментальное ПО (рис. 2.2).

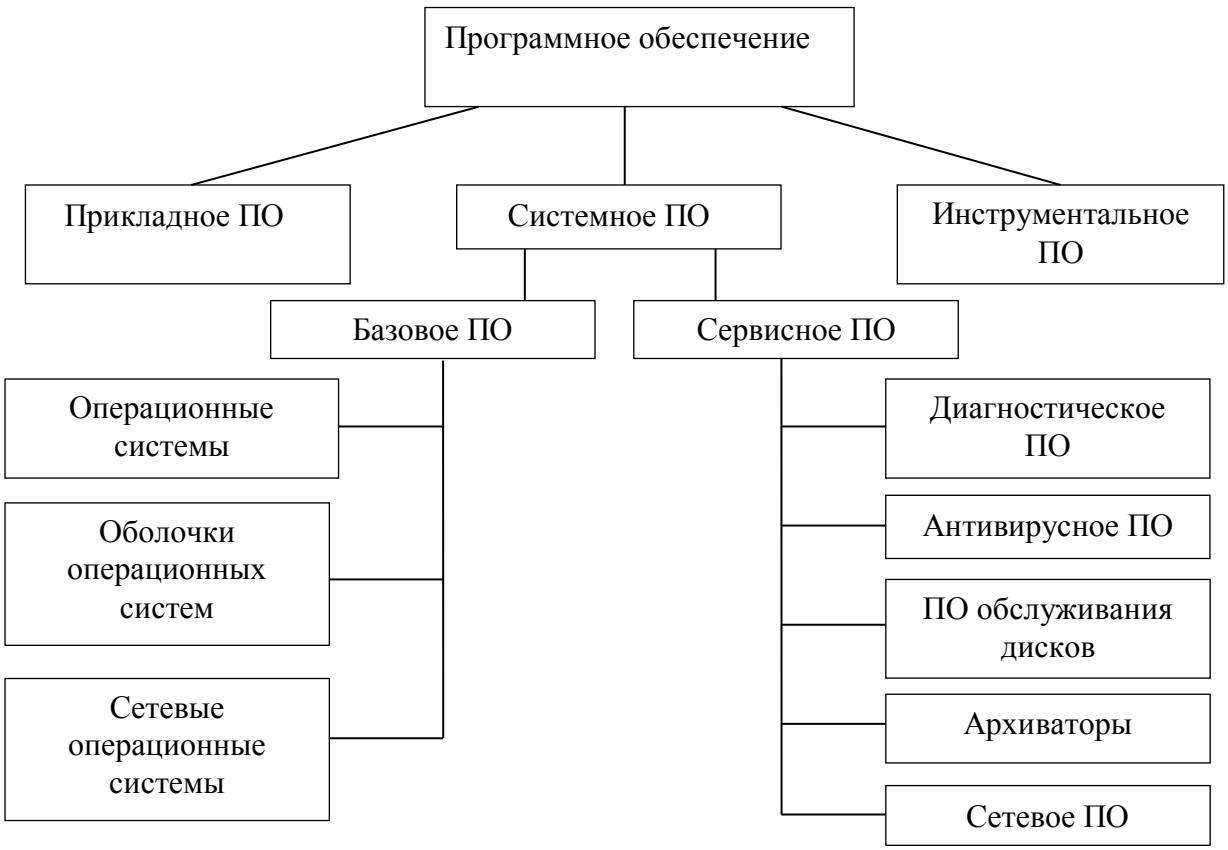

Рис. 2.2. Классификация программного обеспечения

Область применения системного программного обеспечения — аппаратная часть КС и сетей, пакетов прикладных программ — функциональные задачи различных предметных областей (MS Word — работа с текстовыми документами, MS Excel — табличные вычисления, 1С Бухгалтерия — бухгалтерский учет и пр.), Инструментального программного обеспечения — технология разработки программ.

Одним из самых уязвимых элементов программного обеспечения является ОС, являющаяся частью системного программного обеспечения. Операционная система — это комплекс программ, обеспечивающий управление ресурсами ЭВМ (вычислительной системы) и процессами, использующими эти ресурсы при вычислениях.

Уязвимость ОС связана с тем, что они содержат много «дыр» (ошибок, допущенных в ходе их разработки) или «потайных ходов» (преднамеренных уязвимостей). Ошибки, допущенные в ходе разработки есть следствие исключительной сложности ОС. Так в 2005 году в ОС различных версий Windows было выявлено 812 «дыр» (исследования US-CERT). Специалисты из McAfee отмечают, что из 124 «дыр», обнаруженных в Windows XP Professional, 29 так и осталось не устраненными, что дало компании основание присвоить Windows статус критически опасной ОС.

Классический пример потайного входа по взлому системы парольной защиты привел в свое время один из создателей языка программирования *C* и ОС *UNIX* Кен Томпсон в своей лекции по случаю вручения ему премии Тьюринга[1]. В компилятор языка *C* был вставлен код, распознававший, когда на его вход поступала программа, содержащая приглашение зарегистрироваться (логин). Компилятор добавлял в эту программу код, распознававший пароль, выбранный самим Томпсоном. Так Томпсон получал возможность успешно проходить процедуру регистрации и идентификации, не зная легальных паролей пользователей.

В 2020 году специалистами по информационной безопасности НПО «Эшелон» было обследовано 76 программных продуктов как отечественного, так и импортного производства. В 26 продуктах из 76 обследованных (34 %) была выявлена 81 уязвимость. Наиболее уязвимым видом программного обеспечения стало прикладное программное обеспечение со встроенными средствами защиты информации.

Анализируя эти и другие данные, специалисты по безопасности КС и сетей пришли к выводу о том, что:

1. Современные универсальные ОС, в частности ОС семейства Windows, несмотря на все многообразие встроенных в них механизмов защиты, не могут рассматриваться как сколько-нибудь защищенные. Практически в любой момент времени их эксплуатации, ОС содержат критичную уязвимость, что создает большую угрозу атаки на защищаемые ресурсы. То же самое относится и к большинству прикладных программ.

2. Для реализации защищенной обработки информации необходимы дополнительные средства защиты компьютерной информации, задачей которых является защита от атак на уязвимости, связанные

[1] Б. Анин. Защита компьютерной информации. — СПб.: БХВ, 2000. — 368 с.

с наличием ошибок программирования в системном программном обеспечении и в прикладных программах.

3. Несовершенство ОС и прикладных программ — едва ли не главная причина колоссального ущерба, нанесенного мировой экономике компьютерными злоумышленниками.

Большинство хакерских атак становится возможным из-за наличия уязвимостей в существующих ОС и прикладном ПО. В сети Интернет появляется все больше вредоносного кода, который использует эти уязвимости для проникновения в компьютеры, выполнения запрограммированных действий и дальнейшего своего распространения. Для подтверждения справедливости данного утверждения приведем некоторую статистику.

2.3. Виды и статистика нарушений информационной безопасности компьютерных систем и сетей

Виды и статистика нарушений безопасности информации в мире

Согласно отчетам Института компьютерной безопасности США (Computer Security Institute — CSI — www.gocsi.com) по анализу более 500 крупных корпораций и государственных организаций за несколько лет:

— 90 % респондентов зафиксировали различные атаки на свои информационные ресурсы;

— 80 % — понесли немалый финансовый урон вследствие этих нарушений, но только 44 % из них смогли подсчитать его.

Официально зарегистрированный объем потерь вследствие нарушений компьютерной безопасности для опрошенных организаций возрос со 100 миллионов долларов в 1997 году, до 456 миллионов в 2002 году. При этом на первом месте оказалась кража конфиденциальной информации (171 млн дол.), на втором — финансовые мошенничества (116 млн дол.), на третьем — убытки от компьютерных вирусов (50 млн дол.). Далее идут такие компьютерные преступления, как саботаж, злоупотребления, отказ в обслуживании и атаки внешних злоумышленников (табл. 2.3).

Таблица 2.3

Статистика потерь от различных видов нарушений информационной безопасности (в млн долларов США)

Тип атаки	1998	1999	2000	2001	2002
Кража информации	33,6	42,5	66,7	151,1	170,8
Финансовые мошенничества	11,2	42,5	56	93	115,8
Несанкционированный доступ со стороны сотрудников	50,6	3,6	22,6	6,1	4,5
Вирусы	7,9	5,3	29,2	45,3	50
Саботаж	2,1	4,4	27,1	5,2	15,1
Злоупотребления сотрудников	3,7	7,6	28	35	50,1
Отказ в обслуживании	2,8	3,3	8,2	4,3	18,4
Атаки внешних злоумышленников	1,6	2,9	7,1	19,1	13.1
Мошенничества с устройствами телекоммуникации	17,3	0,8	4	9	0,4

Относительно статистика по динамике кибератак за 2011–2013 годы приведена в таблице 2.4.

Таблица 2.4

Динамика кибератак в 2011–2013 годах

Динамика кибератак	Годы		
	2011	2012	2013
Вирусы, черви, шпионы и др вредоносное ПО	76 %	72 %	71 %
Спам атаки	73 %	69 %	67 %
Фишинговые атаки	27 %	26 %	26 %
Сетевые/хакерские атаки	27 %	27 %	19 %
Корпоративный шпионаж			17 %
Кражамобильных устройств		15 %	17 %
Dos и DDoS атаки	17 %	17 %	18 %
Кража крупного оборудования			10 %
Целевые (таргетированные) атаки	13 %	10 %	8 %
Преступное вредительство, включая поджоги	4 %	5 %	5 %
Другое	4 %	5 %	5 %

Статистика нарушений информационной безопасности в России

Согласно исследованиям российской компании GROUP-IB, основными мишенями кибератак в России остаются государственный и финансовый сектор, прежде всего небольшие региональные банки, а мо-

тив нападения — промышленный шпионаж или кража денег. Сами атаки стали более изощренными и практически всегда происходят с использованием методов социального инжиниринга. Например, сотрудники одного из банков получили на рабочую почту рассылку о вакансиях в Центробанке. Многие не удержались и открыли зараженное письмо, вирус начал распространяться по внутренней сети банка.

Начиная с 2013 года, сразу несколько разных групп русскоговорящих хакеров регулярно атакуют наши банки, платежные системы. И очень успешно. Наиболее яркий пример — деятельность группы Anunak (также известной как Carbanak). Она успешно атаковала более 50 российских банков и пять платежных систем. Общая сумма хищений, к которым причастны эти мошенники, составляет более 1 млрд рублей.

Большая часть хищений приходится на вторую половину 2014 года. Часть группы была разоблачена. Остальные продолжают действовать под другими названиями. По данным управления «К» Бюро специальных технических мероприятий МВД России в 2013 году было выявлено около 8000 компьютерных преступлений. Треть этих преступлений оказались мошенничеством и кражами. А в 2014 году количество компьютерных преступлений, связанных с мошенничеством и кражами увеличилось на 41 %.

Более 10000 преступлений в сфере телекоммуникаций и компьютерной информации были зафиксированы в России в первой половине 2015 года. Это на 67 % больше, чем за аналогичный период прошлого года.

Еще одна хакерская группа — Buhtrap успешно похитила у 13 банков 1,8 млрд рублей. Средняя сумма хищения составила 143 млн рублей. Обобщенный алгоритм подготовки и реализации несанкционированного доступа, используемый группой Buhtrap (на примере НСД к банковским системам) состоит из следующих этапов:

1. Нарушитель отправляет письма с вредоносным вложением от имени, например, Центрального банка России или потенциального клиента.

2. После открытия сотрудником атакуемого банка вредоносных вложений на его компьютер устанавливаются средства удаленного доступа, которые обеспечивают начальный доступ к сети финансового учреждения.

3. Далее атакующий начинает проводить внутренний аудит сети банка, постепенно собирая информацию о внутренних серверах, администраторах, операторах банковских систем.

4. На рабочие места операторов банковских систем устанавливаются программы слежения, записывающие видеороботы с этими системами, которые создают снимки с экранов и передают всю информацию атакующим, что дает им возможность правильно повторять действия настоящих операторов систем.

5. В отдельных случаях злоумышленники добираются до сетей управления банкоматами и получают контроль над некоторыми из них. Как итог, у хакеров есть возможность по команде выдавать всю имеющуюся наличность из этих банкоматов.

Представленный алгоритм предполагает поэтапное совершенствование воздействий на атакуемую КС. Безопасность — это цепочка и для эффективной атаки важно определить ее слабое звено. Такое звено может быть обнаружено во всем, что связано с компьютерной безопасностью: в политике безопасности, в средствах защиты, в реализациях программного и аппаратного обеспечения, в управлении системой. Могут использоваться также дефекты, которые на первый взгляд не имеют непосредственного отношения к обеспечению безопасности, например, дефекты прикладного программного обеспечения.

В 2015 году в России была проведена первая в мире успешная атака на брокера, вызвавшая большой резонанс среди участников финансового рынка. Использовался Троян Corkow (также известный как Metel). Этот Троян предоставляет удаленный доступ к системе, что позволяет злоумышленнику запускать программы, управлять клавиатурой и мышкой параллельно с оператором системы. В результате несанкционированного доступа к терминалу торговой системы было выставлено пять заявок на покупку 437 млн долларов и две на продажу 97 млн долларов. Это принесло ущерб банку в 300 млн рублей.

В результате еще одного инцидента через банкоматы за один день было похищено около 500 млн рублей. Пострадало полтора десятка крупных банков — участников одной из российских расчетных систем, которая позволяет снимать средства с карт Visa и MasterCard по выгодным тарифам.

В 2017 году лидером среди преступных сообществ оказалась группировка Cobalt. Известно примерно полсотни ее успешных атак на разные российские банки. Добыча — от нескольких миллионов до полумиллиарда рублей за одну атаку.

Как и во всех описанных выше случаях, хакеры использовали вредоносные программы, которые хорошо известны антивирусным компаниям. Но обнаружить их работу вовремя стандартными сред-

ствами защиты очень сложно. Эти программы предоставляют удаленный доступ к нужным системам внутри защищенных сетей и открывают преступникам все возможности, доступные сотрудникам финансовых учреждений.

Распространение мобильных технологий все больше привлекает преступников, которые используют вирусы и трояны для кражи денег с банковских счетов. Число зарегистрированных случаев создания, использования и распространения вредоносных программ за короткое время выросло вдвое.

По данным МВД количество киберпреступлений в России с 2013 по 2018 годы возросло в шесть раз. Это вызвано все большей доступностью программных средств, с помощью которых даже слабо подготовленные пользователи могут совершать сложные преступления.

По мнению руководства бюро специальных технических мероприятий, (БСТМ) современные сервисы, площадки для общения и размещения рекламы, где существует возможность переводов денежных средств, притягивают злоумышленников и потенциальных жертв. Ситуация в сфере безопасности переводов электронных платежей, которая сложилась в стране, подрывает к ним доверие плательщиков и ставит под угрозу бизнес в Интернет-пространстве.

Также участились случаи незаконного использования ОС на мобильных устройствах для получения конфиденциальной информации о пользователе. С этой целью распространяются программы вредоносного характера, специально созданные, чтобы получать данные о банковских счетах пользователя. МВД России также раскрыло преступную деятельность по удаленному контролю мобильных устройств граждан злоумышленниками.

Современные возможности и функции устройств иногда идут во вред их владельцам. Огромная часть мобильных гаджетов привязана к учетной записи, а свои данные пользователи загружают в облачные сервисы. Завладев информацией с учетной записи, преступник получает огромный массив данных — от переписки и списка контактов, до сведений о перемещениях и личных фотографиях, и у правонарушителя появляется возможность заблокировать мобильное устройство в любую минуту. С этой информацией для него не составляет особого труда узнать пароли банковских карт и получить к ним доступ.

Американская компания Symantec оценила ущерб от киберпреступности в России за 2012 год в размере 1 млрд долларов, а в 2013 году — в размере 1,48 млрд. В мире в целом ущерб составил в 2012 году

110 млрд долларов, а в 2013 году — 113 млрд долларов. Таким образом, количество компьютерных преступлений в России составляет 1,3 % от общемирового количества, в то время как численность населения России составляет 1,9 % от числа жителей Земли. При этом большинство жителей Африки и значительная часть жителей Азии не имеет компьютеров, и, соответственно — возможности совершать компьютерные преступления.

По данным исследования 2014 года Cost of Cyber Crime Study, проведенного компанией Pomenon Instituute при поддержке HP Enterprise Security, средний ущерб российских организаций от киберпреступлений в 2014 году достиг 3,3 млн долларов, а средний ущерб организаций США — 12,7 млн долларов, что на 96 % больше аналогичного показателя 5 лет назад. Среднее время устранения последствий кибератаки возросло на 33 %, а ущерб от одной атаки превысил 1,6 млн долларов. Дороже всего компаниям обходится распознавание атак и восстановление информации после них — 49 % годовых издержек.

По данным лаборатории Касперского в мире ежедневно появляется до 70000 вредоносных программ. Часто они используют новые методы заражения, скрывая свое присутствие в системе, стремясь действовать в обход защиты. В 2015 году у 96 % российских компаний фиксировались инциденты в области IT безопасности. Чаще всего инциденты приводили к потере данных о платежах (13 %), клиентских баз (12 %) и информации о сотрудниках (12 %).

По информации Управления «К» БСТМ МВД России число компьютерных преступлений ежегодно, как минимум, удваивается. За последние десять лет количество компьютерных преступлений увеличилось в 22,3 раза и продолжает увеличиваться в среднем в 3,5 раза в год. При этом успешно расследуется около 49 % зарегистрированных компьютерных преступлений. Обвинительные приговоры выносятся в 25,5 % случаев.

Однако реальную картину эти цифры не отражают, по оценке криминологов латентность компьютерных преступлений составляет от 80 % до 90 %. То есть на самом деле количество преступлений в сфере высоких технологий (в том числе и компьютерных преступлений) больше в 4–10 раз. Это происходит потому, что многие банки и крупные компании в имиджевых целях скрывают совершенные в отношении них преступления, а средние и мелкие компании вообще не имеют в штате службы информационной или компьютерной без-

опасности и не в состоянии обнаружить и зафиксировать факт совершенного в отношении них преступления.

Не только банки подвергаются атакам хакеров. С помощью вредоносных писем злоумышленники пытались инфицировать, например, системы научно-производственного центра «Вигстар», занимающегося производством оборудования для российских вооруженных сил и спецслужб. Были атакованы предприятия стратегического назначения стран СНГ в ходе шпионской кампании Roaming Tiger. Командно контрольная инфраструктура указывала на китайское происхождение Roaming Tiger.

Известна история с мошенниками, создавшими поддельные сайты таких компаний, как «ГАЗ», «Газпромнефть», «Транснефть», АФК «Система» и многих других. Эти мошеннические ресурсы наносят не только репутационный, но и прямой финансовый ущерб владельцам брендов.

Есть немало и других киберугроз для финансовых и промышленных учреждений, предприятий[1].

Виды компьютерных преступлений в отношении граждан

Выше мы рассмотрели виды компьютерных преступлений, совершаемых в отношении банков и других юридических лиц. Здесь приведем наиболее распространенные виды компьютерных преступлений в отношении граждан.

Фишинг. Fishing в переводе с английского языка означает рыбалку. В области киберпреступлений этот термин означает «ловлю» логинов и паролей пользователей. В 2015–2016 годах уже упоминавшаяся выше компания Group-IB фиксировала ежемесячно около 100000 фишинговых атак.

Схема фишинга очень проста, не требует использования вредоносных программ и позволяет хакерам зарабатывать миллионы рублей. Приведем эту схему.

1. Мошенники покупают или достают иными способами списки уязвимых сайтов самой разной тематики. Таких сайтов на просторах Интернета очень много.

2. Обладая даже ограниченным доступом к такому сайту, они могут изменять его. И часть посетителей, зашедших на «поломанный» сайт в результате поискового запроса в системах Google, Yandex,

[1] Овчинский В. С. Криминология цифрового мира: учебник. — М.: Инфра-М, 2018. — 352 с.

Bing, Rambler, Mail.ru и пр., перенаправляется на фишинговый (мошеннический) сайт.

3. Фишинговый сайт замаскирован под акцию по розыгрышу призов. Он информирует жертву, что та выиграла денежный приз и может получить деньги. Для этого ее просят указать данные банковской карты.

4. Если жертва соглашается, то на следующем шаге ее просят указать текущий баланс карты. На сайтах большинства банков есть услуга перевода с карты на карту. Чтобы перевести деньги, необходимо указать данные карты отправителя, получателя, сумму перевода и СМС-код подтверждения. Как только жертва указывает нужные данные о своей карте, программа на сервере хакеров автоматически пытается сделать перевод того самого текущего баланса жертвы с ее карты на карту мошенников.

5. Жертва должна подтвердить денежный перевод со своей карты с помощью СМС-кода. В этот момент на фишинговом сайте жертве показывают окно, информирующее, что для получения выигрыша нужно ввести СМС-код, полученный на мобильный телефон. Если жертва вводит код в поле фишингового сайта, злоумышленники используют его для мошеннического денежного перевода.

Банковские трояны для Android-устройств. Этот вид вредоносных программ представляет наибольшую угрозу для счетов физических лиц. Дело в том, что более 80 % смартфонов в мире работает на платформе Android. Поэтому большинство вирусов для смартфонов пишутся под нее. Банковские трояны, написанные под Android, умеют похищать деньги автоматически. Они собирают данные карт, и уже не важно, клиентом какого банка является владелец телефона. Зараженный трояном смартфон фактически шпионит за своим владельцем: передает хакерам историю звонков и СМС, доступ к любым файлам на телефоне и к информации в «облачном» хранилище, следит за геолокацией (определением реального географического местоположения электронного устройства, например, сотового телефона или компьютера, подключенного к Интернету).

Жертва сама загружает и запускает вредоносную программу, иногда следуя инструкциям по установке. Чтобы заставить жертву выполнить эти манипуляции, злоумышленник распространяет такие программы под видом легальных, например, пиратской версии навигатора, средств просмотра фото- или видеофайлов, обновлений ОС, расширений и т. п.

С мобильного устройства можно получить абсолютно все данные для совершения мошенничества: остаток на банковском счете; номер банковской карты, срок действия и CVV (Card Validaton Value); СМС-коды для подтверждения платежей; сведения, подключен ли интернет-банк; коды восстановления пароля для доступа в интернет-банк.

Ежедневно в России совершается около 70 успешных хищений со счетов владельцев таких зараженных мобильных устройств. Один из наиболее распространенных способов хищения — перевод через СМС- банкинг. Схема такого хищения состоит из следующих шагов:

1. Троянская программа пересылает все СМС на сервер злоумышленника.

2. Злоумышленник ищет на сервере СМС с уведомлениями от банков. Например, после совершения покупок, в них содержится информация о балансе банковского счета.

3. Если владелец телефона является клиентом банка, который предоставляет услугу СМС-банкинга, то злоумышленник создает задание вредоносной программе на отправку СМС с информацией о переводе денежных средств на номер банка. При этом все дальнейшие уведомления от банка будут скрываться на телефоне владельца счета, и передаваться на сервер злоумышленника.

4. Банк отправляет код подтверждения операции на перевод денежных средств по СМС.

5. Троянская программа перехватывает СМС от банка, скрывает это СМС от пользователя и передает его текст на сервер злоумышленника.

6. Злоумышленник создает задание вредоносной программе на отправку СМС с кодом подтверждения на номер банка.

7. Вредоносная программа выполняет задание, в результате чего операция перевода завершается.

Описанные выше шаги часто автоматизируются, и деньги могут списывать с вашего банковского счета несколько дней небольшими суммами.

Программы вымогатели. Некоторое время назад в Интернете появились программы, загружающие на экраны компьютера блокирующие окна, которые сложно закрыть. Чтобы их убрать, необходимо было заплатить атакующему злоумышленнику. Антивирусные компании очень скоро разработали средства, которые могли противодействовать таким вредоносным программам — коды разблокировки. Эти коды они выставляли на своих сайтах. Если коды разблокировки по каким-либо

причинам оказывались недоступными, всегда можно было переустановить ОС. При этом данные оставались в сохранности, но необходимо было переустанавливать и все нужные программы.

Ситуация изменилась, когда хакеры начали шифровать файлы и требовать деньги не за разблокировку компьютера, а за ключ дешифровки. Средняя сумма — 400 долларов. С развитием мобильных устройств часть важных для пользователя данных стала храниться в гаджетах. Поэтому хакеры начали делать аналогичные программы и для мобильных устройств.

На этом взломщики не остановились. Они поняли, что одними из самых платежеспособных пользователей являются владельцы iPhone. Но заразить технику Apple сложнее из-за сильных ограничений на установку программ из недостоверных источников. Для атак на владельцев iPhone хакеры пользуются следующей тактикой:

1. Скупают или сами подбирают пароли от сервиса iCloud (фирменное облачное хранилище данных от компании Apple).

2. Получив доступ, меняют привязанный адрес электронной почты к сервису iCloud и пароль.

3. В сервисе iCloud есть информация обо всех ваших устройствах и, конечно же, возможность блокировать их работу, что злоумышленники и делают. При этом Apple при блокировке через iCloud позволяет задать сообщение, которое будет показано на экране. В нем хакер указывает адрес, на который нужно написать, чтобы получить инструкции по оплате за разблокировку устройства.

4. Утрата доступа к данным и устройству не является большой потерей для многих владельцев техники Apple, поэтому они достаточно быстро соглашаются на оплату.

Мошеннические интернет-магазины и сервисы. Это одна из самых простых схем воровства средств честных граждан.

На просторах Интернета существует множество ресурсов, где предлагают купить товары по очень привлекательным ценам, но с предварительной оплатой. Многие идут на риск и в итоге остаются и без товаров, и без денег. Всплески появления таких фальшивых ресурсов часто отмечаются перед большими праздниками.

Сезонные мошенничества. Кроме псевдомагазинов есть и сезонные мошенничества. Например, перед сезоном отпусков появляются фальшивые туристические операторы, сервисы по продаже авиабилетов или бронированию отелей. Иногда такие сервисы даже присылают вам

электронные билеты и квитанции на бронь гостиницы. Но они являются поддельными, что выясняется только в самый последний момент.

Защита от кибермошенников. В сети «Интернет» можно найти множество толковых рекомендаций по защите от мошенников. Тем не менее, для надежной защиты требуется всестороннее обучение кибербезопасности, начиная со школы. Это — задача государства, органов образования. Причем, обучать с детства надо не только защите от вирусов и мошенников, но и от кибер-педофилов, от вовлечения в секты, экстремистские группы и клубы самоубийц типа «синих китов».

В заключение приведем обобщенные данные правоохранительных органов, Давосского форума 2017 года и конференции Всемирного банка о десяти основных сферах деятельности мировой организованной преступности, в которых активно задействован киберкриминал:

1. Финансовые преступления, включая незаконное обогащение, отмыв и преступное перемещение финансовых ресурсов, капиталов и активов.

2. Производство, хранение, транспортировка и продажа контрафактной продукции.

3. Хищение и противозаконное использование интеллектуальной собственности.

4. Наркоторговля.

5. Незаконная торговля оружием.

6. Работорговля.

7. Незаконное изъятие, хранение, транспортировка и использование человеческих органов для трансплантации.

8. Организованная педофилия.

9. Незаконный игорный и лотерейный бизнес (включая создание виртуальных казино, противозаконных компьютерных игр, предполагающих безлицензионную монетизацию и т. п.).

10. Широкий круг преступлений экологического характера (незаконные операции с городскими и промышленными отходами, отлов, транспортировка, сбыт редких животных, птиц, пресмыкающихся и т. д.).

Контрольные вопросы:

1. Назовите угрозы информации и источники угроз.

2. Перечислите уязвимые компоненты компьютеров, компьютерных систем и сетей.

3. Назовите виды компьютерных преступлений в отношении граждан.

Лекция 3. Формализованные требования к программно-аппаратной защите информации

Вопросы лекции:

3.1. Политика и показатели безопасности средств вычислительной техники и автоматизированных систем.

3.2. Формализованные требования к защите объектов программно-аппаратной защиты информации.

3.3. Новое поколение нормативно-технических документов по безопасности информации.

Ранее мы убедились, что пространство угроз компьютерной информации велико и разнообразно. Столь же велики и разнообразны программно-аппаратные методы и средства противодействия этим угрозам. Поэтому задача выбора средств и методов противодействия угрозам, осуществляемая на этапе обоснования проекта системы защиты информации, не является тривиальной. В настоящее время в России и в мире наибольшее распространение получили два подхода к решению этой задачи.

Первый подход основан на проверке соответствия уровня защищенности КС заданным требованиям в области информационной безопасности. Эти требования могут быть заданы в виде классов защищенности, как это сделано в руководящих документах ФСТЭК, в виде профилей защиты, разработанных в соответствии со стандартом ИСО/МЭК-15408, или в виде какого-либо другого набора требований. При таком подходе цель проектирования считается достигнутой, если проект обеспечивает выполнение данного набора требований. Задачу разработки такого проекта можно представить в виде задачи математического программирования: выбрать такой набор средств защиты информации, который обеспечивал бы выполнение данного набора требований и при этом был бы минимальным по стоимости:

$$\sum_{i=1}^{n} c_j x_j \underset{X}{\Rightarrow} min,$$

$$f_i(X) \geq b_i,\ X \geq 0,$$

где: n — количество видов ПАСЗИ, x_j — количество средств защиты информации j-го вида, $X=\{x_1, x_2, \ldots, x_n\}$, $f_i(X)$ — формула зависимости показателя i-го вида от количества средств защиты, b_i — требуемая величина i-го показателя. Основной недостаток такого подхода заключается в том, что, если требуемый уровень защищенности жестко не задан, определить его достаточно сложно.

Второй подход основан на оценке и управлении рисками. Принципы этого подхода описываются следующим набором постулатов:

— абсолютно надежную систему защиты информации создать невозможно;

— необходим баланс между затратами на защиту информации и получаемым эффектом, заключающимся в снижении потерь от нарушений безопасности;

— стоимость средств защиты не должна превышать стоимости защищаемой информации;

— затраты нарушителя на НСД к информации не должны превышать эффект, который он в результате получит.

Эта модель также может быть описана как задача математического программирования:

$$\sum_{i=1}^{n} Z(X) \underset{X}{\Rightarrow} max,$$

$$f(X) \leq b, \; X \geq 0.$$

Здесь: Z(X) — показатель, выражающий разницу между получаемым эффектом и затратами на защиту информации; $X=\{x_1, x_2, \ldots, x_n\}$ — вектор, показывающий количество средств защиты каждого из n видов, установленных на объекте; *f(X)* — формула зависимости затрат на систему защиты информации от количества средств защиты; b — максимально допустимые затраты на систему защиты информации. В данной лекции основное внимание уделено первому подходу.

3.1. Политика и показатели безопасности средств вычислительной техники и автоматизированных систем

Задачи защиты компьютерной информации и требования к системе защиты объективны, порождены практическим опытом эксплуатации СВТ, АС и во многом близки, как для больших распределенных вычислительных систем, так и для одиночных ПК, работающих в одно- или многопользовательском режиме.

Система защиты информации должна обеспечивать надежную, т. е. бесперебойную, устойчивую и правильную работу СВТ (АС), оперативный доступ сотрудников к информации в соответствии с предоставленными им полномочиями, возможность восстановления информации в случае ее случайной утраты или уничтожения вследствие возникновения аварийных ситуаций и многое другое. В целом система мер по защите информации должна воплощать в жизнь, разработанную на предприятии с участием соответствующих специали-

стов и утвержденную его руководителем, политику информационной безопасности (ПБ).

Политика безопасности — это совокупность принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности. ПБ оформляется в виде документа (набора документов), который должен быть доступен всем сотрудникам, и, в первую очередь, отвечающим за обеспечение режима информационной безопасности на предприятии. Этот документ определяет основные цели политики информационной безопасности и область ее применения, а также ее значение как механизма, позволяющего сотрудникам предприятия коллективно использовать информацию.

В документе рядовые пользователи и ответственные за безопасность сотрудники должны найти разъяснение мер, принципов, стандартов и конкретных вариантов реализации политики безопасности, требований к ее соблюдению, общих и конкретных обязанностей по обеспечению режима информационной безопасности, включая выполнение правовых и договорных актов.

Политика разрабатывается в соответствии с имеющейся нормативной базой, многие ее разделы являются законодательно необходимыми. Разработка ПБ — дело творческое, но и отказываться от опыта специалистов не разумно. Существуют специализированные программные комплексы, осуществляющие формализованный анализ ПБ на полноту и соответствие требованиям нормативных актов. Большое внимание политика безопасности обычно уделяет специальным мероприятиям, обеспечивающим защиту информации от несанкционированного доступа злоумышленника к конфиденциальным данным.

Степень безопасности информации в СВТ и АС оценивается по величине показателей (критериев) защищенности. Формально показатель задается как некоторая функция, по значению которой судят о защищенности СВТ (АС). Критерий защищенности формулируется на основе выбранных показателей и представляет собой решающее правило, которое позволяет оценить, достаточно ли защищена система.

Руководящие документы ГТК (ФСТЭК) предлагают две основных группы показателей (критериев) защищенности информации: показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем (АС) обработки данных. Первая группа позволяет оценить степень защищенности (правда только относительно угроз типа НСД) отдельно

поставляемых потребителю компонентов СВТ, а вторая рассчитана на полнофункциональные системы обработки данных.

Отличие этих двух групп обусловлено тем, что СВТ разрабатываются и поставляются потребителям лишь как элементы информационно-телекоммуникационных систем, из которых в дальнейшем строятся функционально ориентированные АС. Следовательно, СВТ не содержат пользовательской информации.

При создании АС появляются такие отсутствующие у СВТ характеристики, как:

— пользовательская информация;

— полномочия пользователей;

— модель нарушителя;

— технология обработки информации.

В отдельный класс выделяются требования по защите СВТ и АС от НСД к информации с использованием межсетевых экранов и систем обнаружения вторжений.

3.2. Формализованные требования к защите объектов программно-аппаратной защиты информации

Формализованные требования к защите средств вычислительной техники

Требования к защите СВТ формализуют условия защищенности отдельно взятого средства (ОС, СУБД, приложения и пр.). Классификацию СВТ по уровню защищенности от НСД устанавливает руководящий документ (РД), утвержденный Гостехкомиссией России в 1992 году «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации». Данный РД устанавливает классификацию отдельно взятых СВТ (ОС, СУБД, приложения) по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований.

Установлено семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий первый. 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.

Показатели защищенности и установленные требования к классам приведены в таблице 3.1.

Таблица 3.1

Требования к показателям защищенности СВТ от НСД

Наименование показателя	Класс защищенности					
	6	**5**	**4**	**3**	**2**	**1**
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	–	–	+	=	=	=
Очистка памяти	–	+	+	+	=	=
Изоляция модулей	–	–	+	=	+	=
Маркировка документов	–	–	+	=	=	=
Защита ввода/вывода на отчужденный физический носитель	–	–	+	=	=	=
Сопоставление пользователя с устройством	–	–	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантия проектирования	–	+	+	+	+	+
Регистрация	–	+	+	+	=	=.
Взаимодействие пользователя с комплексом средств защиты (КСЗ)	–	–	–	+	=	=
Надежное восстановление	–	–	–	+	=	=
Целостность КСЗ	–	+	+	+	=	=
Контроль модификации	–	–	–	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Текстовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:

«–» — нет требований к данному уровню;

«+» — новые или дополнительные требования;

«=» — требования совпадают с требованиями предыдущего уровня.

Для примера разъясним требования для СВТ шестого класса защищенности. В этом случае достаточно наличие дискреционного принципа контроля доступа, системы аутентификации и идентификации, системы тестирования и документации на СВТ. Документация должна включать в себя:

— краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем;

— руководство по КСЗ. Данный документ адресован администратору защиты и должен содержать: описание контролируемых функций, руководство по генерации КСЗ, описание старта СВТ и процедур проверки правильности старта;

— тестовая документация. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования;

— конструкторская (проектная) документация. Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

Формализованные требования к защите автоматизированных систем

Требования к защите АС 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.

Для различного класса автоматизированных систем документ регламентирует выполнение требований, приведенных в таблице 3.2.

Таблица 3.2

Требования по защите информации от НСД для АС

Подсистемы и требования	Класс защищенности								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. *Подсистема управления доступом* 1.1. Идентификация. Проверка подлинности и контроль доступа объектов:									
− в систему	+	+	+	+	+	+	+	+	+
− к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
− к программам				+		+	+	+	+
– 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 доступа 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, 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 носителей	+	+	+	+	+	+	+	+	+
2.4. Сигнализация попыток нарушения							+	+	+

Подсистемы и требования	Класс защищенности								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
3. *Криптографическая подсистема*									
3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группа субъектов) на различных 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 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:

« » — нет требований к данному уровню;

«+» — новые или дополнительные требования;

«=» — требования совпадают с требованиями предыдущего уровня.

Классы делятся на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса — 2Б и 2А.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.

Все перечисленные требования должны обеспечиваться средствами самой КС автоматически. Каждый сотрудник предприятия должен быть вынужден гарантированно выполнять требования политики безопасности, а не только под воздействием силы приказов и распоряжений начальников. На предприятии должен быть организован такой режим функционирования АС, который просто не позволит пользователю работать с конфиденциальными данными в незащищенном режиме. Перечисленные выше требования защиты АС от НСД вытекают из опыта, здравого смысла и давно существующего порядка работы с конфиденциальной информацией (на бумажных или электронных носителях). Этот набор требований далеко не полон, не противоречит официальным руководящим документам, однако он не затрагивает специальных вопросов проектирования комплекса защиты информации, параметров функциональности средств и механизмов защиты, разработки необходимой документации, тестирования СЗИ, контроля защищенности АС.

Между классами СВТ и классами АС существует определенная взаимосвязь. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы. Приведем соответствие между классами АС и степенями конфиденциальности информации:

— классы 1А, 2А, 3А включают АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом «особой важности»;

— класс 1Б включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом «совершенно секретно»;

— класс 1В включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом «секретно»;

— классы 1Г, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию — служебная тайна;

— классы 1Г, 1Д, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию — персональные данные, коммерческая тайна.

В компактном виде это соответствие приведено в таблице 3.3.

Таблица 3.3

Соответствие между классами АС и степенями конфиденциальности информации

Гриф сведений	Государственная тайна			Конфиденциальная информация	
	Особой важности	Сов. секретно	Секретно	Служебная тайна	Персон. данные, коммерч. тайна
Классы АС	1А, 2А, 3А	1Б	1В	1Г, 2Б, 3Б	1Г, 1Д, 2Б, 3Б

Требования к уровню отсутствия недекларированных возможностей

Недекларированные возможности — это функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и целостности обрабатываемой информации.

Руководящим документом ФСТЭК «Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей» (Утвержден решением Председателя Гостехкомиссии РФ от 04.06.1999 г.) установлена классификация отечественного и иностранного программного обеспечения по уровню отсутствия недекларированных возможностей (рис. 3.1). Всего таких уровней — четыре. Четвертый уровень соответствует конфиденциальной информации, остальные три — информации, содержащей государственную тайну. При этом: третий уровень отсутствия недекларированных возможностей соответствует секретной информации, второй — совершенно секретной, первый — особой важности.

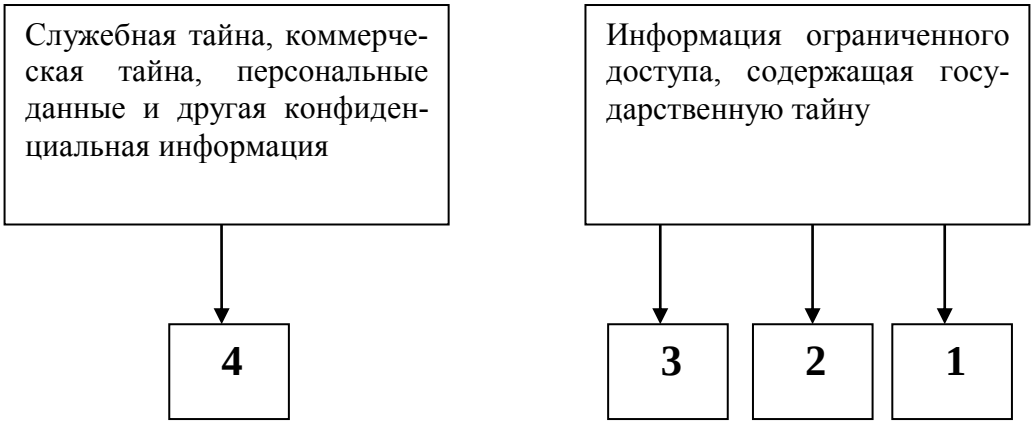

Рис. 3.1. Классификация по степени соответствия уровня контроля недекларированных возможностей уровням защищенности от НСД

В таблице 3.4 приведены данные по требованиям к каждому из уровней отсутствия недекларированных возможностей.

Таблица 3.4

Требования к уровням отсутствия недекларированных возможностей

№	Наименование требования	Уровень контроля			
		4	**3**	**2**	**1**
	Требования к документации				
1	Контроль состава и содержания документации				
1.1	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4	Пояснительная записка (ГОСТ 19.404-79)	–	+	=	=
1.5	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2	Контроль исходного состояния ПО	+	=	=	=
3	Статический анализ исходных текстов программ				
3.1	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3	Контроль связей функциональных объектов по управлению	–	+	=	=

№	Наименование требования	Уровень контроля			
		4	3	2	1
3.4	Контроль связей функциональных объектов по информации	–	+	=	=
3.5	Контроль информационных объектов	–	+	=	=
3.6	Контроль наличия заданных конструкций в исходных текстах	–	–	+	+
3.7	Формирование перечня маршрутов выполнения функциональных объектов	–	+	+	=
3.8	Анализ критических маршрутов выполнения функциональных объектов	–	–	+	=
3.9	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	–	–	+	=
4	Динамический анализ исходных текстов программ				
4.1	Контроль выполнения функциональных объектов	–	+	+	=
4.2	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	–	+	+	=
5	Отчетность	+	+	+	+

Обозначения:

«–» — нет требований к данному уровню;

«+» — новые или дополнительные требования;

«=» — требования совпадают с требованиями предыдущего уровня.

Примечание: Требования ФСТЭК к иным средствам защиты информации будут описаны позже.

3.3. Новое поколение нормативно-технических документов по безопасности информации

Общие критерии информационной безопасности. Стандарты ИСО/МЭК 15408

Одним из наиболее важных международных документов в области информационной безопасности является международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», сокращенно называемый часто «Общие критерии». На самом деле ISO/IEC 15408 является метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. Он содержит обобщенный опыт ряда государств в области ин-

формационной безопасности и подвергается постоянным уточнениям и доработкам. В России «Общие критерии» представлены в виде:

— национального стандарта «ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть I. Введение и общая модель». Утвержден приказом Росстандарта РФ от 15.11.2012 г. № 814-ст;

— национального стандарта «ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 2. Функциональные требования безопасности». Утвержден приказом Росстандарта РФ от 8.11.2013 г. № 1339-ст;

— национального стандарта «ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 3. Требования доверия к безопасности». Утвержден приказом Росстандарта РФ от 8.11.2013 г. № 1340-ст;

— РД ФСТЭК Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. 2002 г.

В общих критериях главное внимание уделяется защите от несанкционированного доступа. Модификация или потеря доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов информационной безопасности остались не рассмотренными. В документе проведена классификация набора требований доверия к безопасности информации, определены структуры их группирования и принципы использования, введены семь базовых оценочных уровней доверия (ОУД), (табл. 3.5), и шесть промежуточных — оценочный уровень доверия усиленный, которые содержат базовый уровень и необходимые документы высшего уровня доверия.

Таблица 3.5

Оценочные уровни доверия ИС

Класс доверия	Семейство доверия	Компоненты доверия и оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Управление конфигурацией	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Поставка и эксплуатация	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Разработка	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Руководства	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Требования безопасности, содержащиеся в данном документе, могут уточняться и дополняться по мере совершенствования нормативно-правовой базы, развития информационных технологий и совершенствования методов обеспечения информационной безопасности.

Каждому классу доверия присвоено уникальное имя. Это имя указывает на тематические разделы, на которые распространяется данный класс доверия. Уникальная форма имени класса доверия состоит из латинской буквы *A*, за которой следуют еще две латинские буквы. Каждый класс доверия содержит, по меньшей мере, одно семейство доверия.

Каждому семейству доверия присвоено уникальное имя. Это имя содержит описательную информацию по тематическим разделам, на которые распространяется данное семейство доверия. Каждое семей-

ство доверия размещено в пределах класса доверия, который включает в себя другие семейства той же направленности.

Уникальная краткая форма имени семейства доверия является основным средством для ссылки на семейство доверия и включает в себя краткую форму имени класса и символ подчеркивания, за которым следуют три буквы латинского алфавита, относящиеся к имени семейства.

Основной целью *Общих Критериев* является повышение доверия к безопасности продуктов и систем информационных технологий. Положения ОК направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политики безопасности с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию «эффективность — стоимость».

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, с учетом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в стандарте. Допускается использование и других требований безопасности. При этом уровень детализации и способ выражения требований, представленных в настоящем стандарте, должны использоваться в качестве образца. Требования безопасности могут задаваться заказчиком в техническом задании на разработку продуктов и систем ИТ самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов и систем ИТ, могут оформляться в виде структуры, именуемой «Профиль защиты», определенный как набор требований, состоящий только из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Профиль защиты специфицирует совокупность требований, которые являются необходимыми и достаточными для достижения поставленных целей безопасности.

Результатом оценки безопасности должен быть общий вывод, в котором описана степень соответствия объекта оценки функциональным требованиям и условиям гарантированности.

Помимо Общих критериев в Российской Федерации необходимо дополнительно руководствоваться:

— национальным стандартом «ГОСТ 54581-2011. Информационная технология. Методы и средства обеспечения безопасности. Осно-

вы доверия к безопасности ИТ. Часть 1. Обзор и основы». Утвержден Приказом Росстандарта от 01.12.2011 г. № 689-ст;

— национальным стандартом «ГОСТ 54582-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 2. Методы доверия». Утвержден Приказом Росстандарта от 01.12.2011 г. № 690-ст;

— национальным стандартом «ГОСТ 54583-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 3. Анализ методов доверия». Утвержден Приказом Росстандарта от 01.12.2011 г. № 691-ст.

В целом стандарты не меняют сложившейся в Российской Федерации методологии защиты, но по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости значительно превосходят действующие в настоящее время нормативно-методические документы.

Стандарты управления информационной безопасностью ИСО/МЭК 27000

США и страны Европы в вопросах информационной безопасности, наряду с нормативным подходом, основанным на стандарте ИСО/МЭК 15408, повсеместно применяют рисковую модель, в основе которой лежит стандарт ИСО/МЭК 27000. Все бизнес-процессы зарубежных компаний, применяющих этот стандарт, однозначно описаны и исполняются строго «по учебнику». Благодаря этому руководители систем информационной безопасности четко понимают, какие инциденты могут возникнуть, с какой вероятностью и что они за собой повлекут.

В настоящее время (2020) данная серия стандартов Российской Федерацией в полном объеме не принята. Приняты только следующие нормативные документы:

— национальный стандарт «ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Утвержден приказом Росстандарта от 27.12.2006 г. № 375-ст. Данный стандарт выдвигает требования к разработке, внедрению, совершенствованию и сертификации системы управления информационной безопасностью (СУИБ). Он покрывает все типы организаций (коммерческие предприятия, государственные агентства и некоммерческие организации). Стандарт уточняет требования на установку, выполнение, обработку, мониторинг, оценку, поддержание и улучшение доку-

ментированных функций системы управления информационной безопасностью в контексте процесса управления рисками организации. Также стандарт уточняет требования по установке настроек системы защиты удовлетворяющих индивидуальным требованиям организации или ее частей, методике проведения аудита безопасности (рис. 3.2);

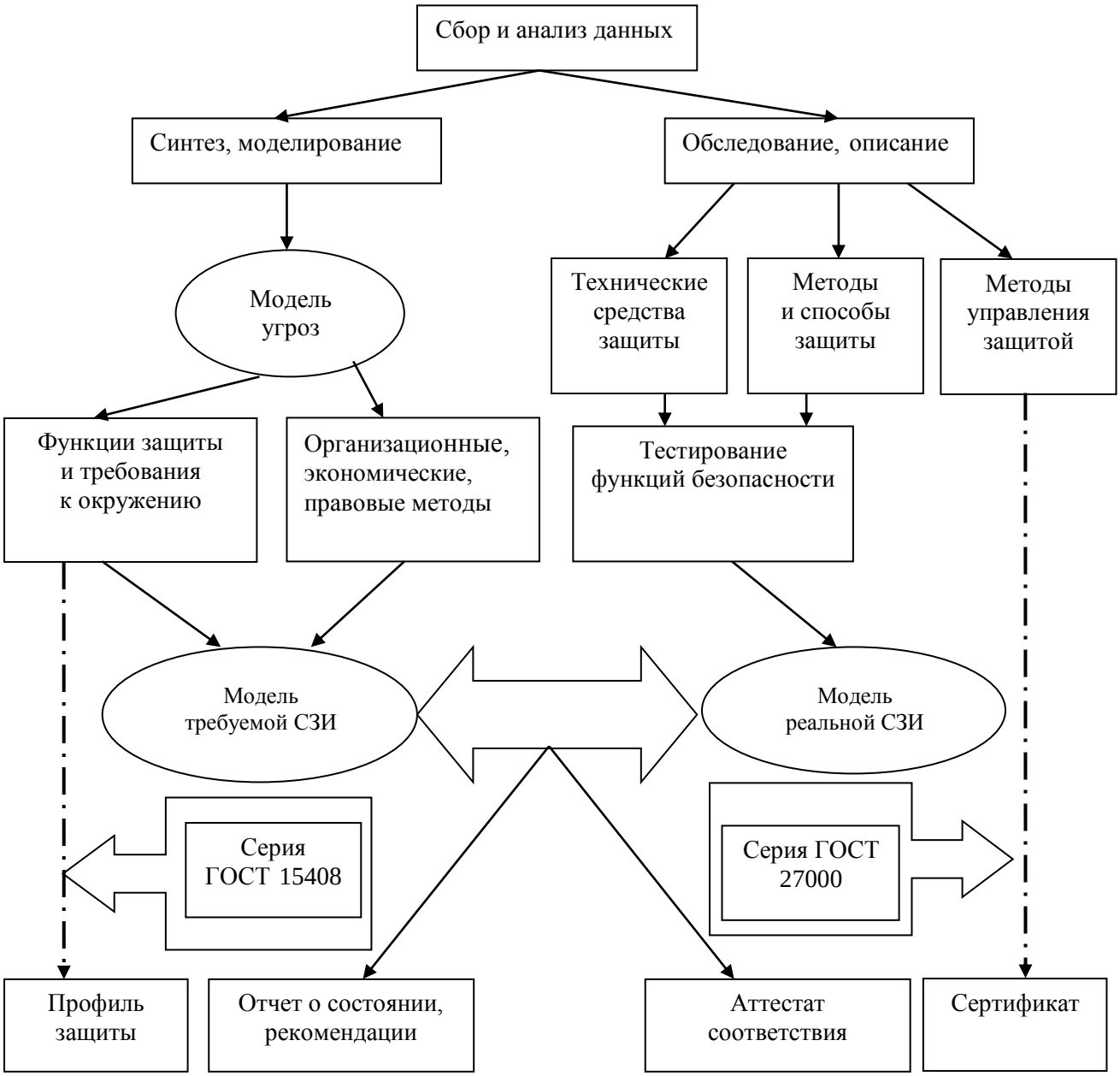

Рис. 3.2. Методика проведения аудита безопасности

— национальный стандарт «ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Требования». Утвержден приказом Росстандарта от 24.09.2012 г. № 423-ст с дополнениями;

— национальный стандарт «ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002». Утвержден приказом Росстандарта от 24.09.2012 г. № 424-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса». Утвержден приказом Росстандарта от 24.09.2012 г. № 426-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности». Утвержден приказом Росстандарта от 15.11.2012 г. № 812-ст.

Эти стандарты определяют основную базовую функциональность и спецификацию архитектуры системы информационной безопасности (рис. 3.2) и содержат 39 фундаментальных задач информационной безопасности. Эти задачи являются отправной точкой для определения набора принципов формирования политики информационной безопасности. Данные стандарты представляют собой скорее общие рекомендации, а не конкретные требования.

Вопросы аудита и сертификации изложены в Национальном стандарте «ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения». Утвержден приказом Росстандарта от 01.12.2011 г. № 681-ст и в национальном стандарте «ГОСТ Р ИСО/МЭК 27006-2008. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности». Утвержден приказом Росстандарта от 18.12.2007 г. № 524-ст.

Руководство по управлению безопасностью в сфере информационных и телекоммуникационных технологий (модель защиты информационной и телекоммуникационной системы, методику оценки риска и ущерба, требования к администратору по безопасности сети) содержат следующие три стандарта:

— национальный стандарт «ГОСТ Р ИСО/МЭК 13335-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности ин-

формационных и телекоммуникационных технологий». Утвержден приказом Росстандарта от 19.12.2006 г. № 317-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Утвержден приказом Росстандарта от 30.11.2010 г. № 632-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 13335-5-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети». Утвержден приказом Росстандарта от 19.12.2006 г. № 317-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции». Утвержден приказом Росстандарта от 01.12.2011 г. № 683-ст. Это первый стандарт из семитомного стандарта серии 27033, который содержит общие требования к построению системы защиты вычислительных сетей. Международные требования по проектированию и реализации сетевой безопасности, рискам, методам проектирования средств контроля и управления для типовых сценариев, шлюзов безопасности, виртуальных частных сетей, IP-конвергенции и беспроводной связи в Российской Федерации пока не приняты.

Требования к построению систем защиты информации от скрытых угроз изложены в следующих документах:

— национальный стандарт «ГОСТ Р ИСО/МЭК 53113-1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения». Утвержден приказом Росстандарта от 18.12.2008 г. № 531-ст;

— национальный стандарт «ГОСТ Р ИСО/МЭК 53113-2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов». Утвержден приказом Росстандарта от 15.12.2009 № 841-ст.

Базовый механизм управления инцидентами информационной безопасности содержит национальный стандарт «ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов

информационной безопасности». Утвержден приказом Росстандарта от 27.12.2007 г. № 513-ст.

Новое поколение стандартов в области защиты информации отличается как от предыдущего поколения, так и от Руководящих документов ФСТЭК большей формализацией процесса обеспечения безопасности и более детальным комплексным учетом качественно и количественно проверяемых и управляемых показателей информационной безопасности. Комплексный учет предполагает комплексный подход к управлению безопасностью, когда на соответствие определенным правилам проверяется не только программно-аппаратная составляющая защиты информации, но и организационно-административные меры по ее обеспечению.

Предлагаемый в стандарте метод аудита является прогностическим, а выводы его носят вероятностно-прогностический характер. Принципиально отличаются и документы, возникающие по результатам аудита. Как правило, это оценочные отчеты, содержащие в то же время весьма конкретные и жесткие рекомендации по приведению внутренних процессов и регламентов в соответствие общепринятым стандартам и практикам.

Контрольные вопросы:

1. Назовите показатели безопасности средств вычислительной техники и автоматизированных систем.
2. Какие формализованные требования предъявляются к защите автоматизированных систем?
3. Назовите нормативно-технические документы по безопасности информации.

Лекция 4. Задачи и классификация программно-аппаратных средств защиты информации

Вопросы лекции:

4.1. Задачи программно-аппаратной защиты информации.

4.2. Классификация программно-аппаратных средств защиты информации.

4.3. Средства защиты, встроенные в аппаратуру.

4.4. Средства защиты информации, встроенные в операционную систему.

4.5. Автономные средства защиты информации.

4.6. Специализированные системы защиты компьютерной информации.

4.7. Сетевая защита в компьютерах и компьютерных сетях.

Известно, что система защиты информации представляет собой взаимоувязанный комплекс правовых, организационных, технических, криптографических, программно-аппаратных, стеганографических, страховых, морально-этических и психологических средств и методов защиты информации. Причем граница между этими средствами и методами подчас размыта. Поэтому при изучении ПАЗИ необходимо учитывать взаимосвязь различных подсистем с программно-аппаратными средствами.

4.1. Задачи программно-аппаратной защиты информации

В первой лекции мы дали определение объекта и предмета ПАЗИ. Прежде чем переходить к характеристике задач ПАЗИ, дадим эти определения еще раз, несколько упростив формулировки.

Под объектом ПАЗИ будем понимать автономный компьютер, КС, автоматизированную систему обработки данных или автоматизированную систему управления.

Под предметом ПАЗИ будем понимать программы и информацию, хранящуюся, циркулирующую или обрабатываемую в компьютерах, КС, автоматизированных системах обработки данных и в автоматизированных системах управления.

Основными целями ПАЗИ являются обеспечение конфиденциальности, целостности и доступности (для легальных пользователей) информации в компьютерах, КС, автоматизированных системах обработки данных и в автоматизированных системах управления.

Наиболее важными задачами ПАЗИ являются:

— защита от несанкционированного доступа к информационным ресурсам КС со стороны внутренних и внешних нарушителей;

— разграничение доступа пользователей к ресурсам КС;

— контроль устройств, подключаемых к компьютерам;

— обнаружение вторжений в КС;

— антивирусная защита;

— межсетевое экранирование сетевого трафика;

— авторизация сетевых соединений;

— защита компьютерных программ от исследования;

— защита конфиденциальной информации, передаваемой по незащищенным сетям.

4.2. Классификация программно-аппаратных средств защиты информации

В настоящее время не существует единой классификации программно-аппаратных средств защиты компьютерной информации. Классифицируют эти средства по разным признакам. Ниже приведена классификация по трем признакам: по защищаемому объекту, по функциональному назначению и по месту установки.

По защищаемому объекту можно выделить два класса СЗИ в КС (см. рис. 4.1):

— средства защиты информации в компьютерах;

— средства защиты информации сетевого действия — средства защиты от НСД к информации в сетях передачи данных.

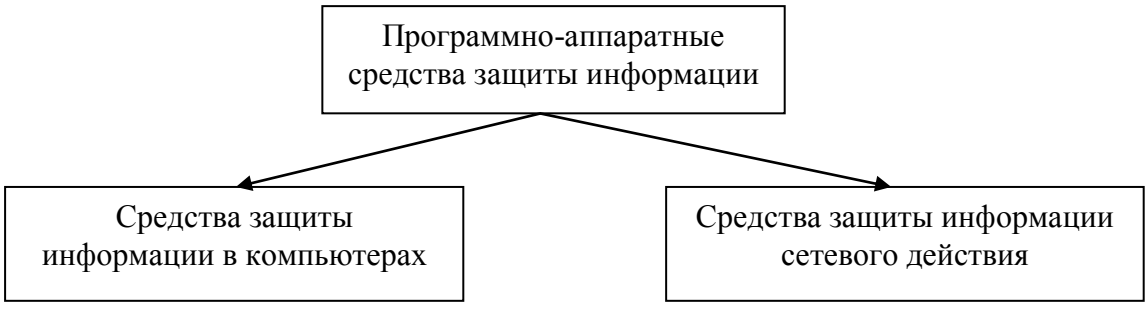

Рис. 4.1. Классификация программно-аппаратных средств по защищаемым объектам

По функциональному назначению ПАСЗИ делят различными способами. Так ФСТЭК в качестве различных классов, сертифицированных по требованиям безопасности информации средств защиты ин-

формации, рассматривает: межсетевые экраны, средства обнаружения вторжений, антивирусные средства, средства доверенной загрузки, средства контроля съемных носителей, средства контроля отсутствия недекларированных возможностей.

Тот же ФСТЭК в РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденном Гостехкомиссией России, средства защиты компьютерной информации объединяют в четыре подсистемы:

— подсистема управления доступом;

— подсистема регистрации и учета;

— криптографическая подсистема;

— подсистема обеспечения целостности.

По месту установки программно-аппаратные средства защиты информации можно поделить на четыре класса:

— аппаратные средства;

— средства ОС;

— автономные средства, включаемые в состав системы защиты при необходимости;

— специализированные (добавочные) системы защиты компьютерной информации (СЗКИ).

Заметим, что одни и те же средства по одной классификации могут входить в состав разных классов по другой. Например, межсетевые экраны (классификация ФСТЭК) могут быть автономными, входить в состав ОС или в состав специализированных систем защиты компьютерной информации (классификация по месту установки).

Приведем краткую характеристику каждого класса СЗИ по месту установки.

Аппаратные средства — это средства защиты информации, встроенные в BIOS компьютера.

Средства операционных систем — это программные средства защиты информации, встроенные в ОС.

Автономные средства — это программы, выполняющие отдельные функции по защите информации. Они включаются в состав системы защиты информации, если средств ОС оказывается недостаточно. К автономным средствам относятся: межсетевые экраны, системы обнаружения вторжений, средства гарантированного удаления файлов и пр. Большинство перечисленных средств входит и в состав ОС последних поколений. Однако, поскольку эти ОС, в силу причин,

которые будут указаны ниже, имеют множество лазеек, позволяющих обойти эти средства, в КС часто устанавливаются автономные средства, как правило, отечественного производства.

Специализированные (добавочные) программные (программно-аппаратные) системы защиты компьютерной информации устанавливаются при жестких требованиях к безопасности информации. Эти системы содержат, как правило, достаточно полный набор автономных средств защиты информации. Так, например, СЗКИ Dallas Lock содержит: средства организации доверенной загрузки, средства создания замкнутой программной среды, средства реализации дискреционной и мандатной модели разграничения доступа, межсетевой экран, средства гарантированной очистки памяти и пр.

Кратко остановимся на возможностях защиты информации средствами каждого из четырех вышеназванных классов. Более детальная информация будет приведена в дальнейшем.

4.3. Средства защиты, встроенные в аппаратуру

Базовая система ввода-вывода — BIOS (Basic Input Output System) представляет собой набор программ настройки и конфигурирования ПК. Эти программы встроены в аппаратное обеспечение ПК (хранятся в энергонезависимой памяти на материнской плате компьютера — CMOS) и предоставляют ему функции управления самого низкого уровня, организуя выполнение команд ЦП. Так BIOS в IBM подобных ПК выполняет ряд функций, среди которых выделим функции по защите информации: функцию установки пароля на вход в BIOS и установки пароля на загрузку ОС, функцию отключения USB портов, функцию смены очередности устройств, с которых загружается ОС.

К сожалению, пароли, равно как и другие настройки, устанавливаемые с помощью программы SETUP BIOS легко обойти. Поэтому на практике они используются нечасто.

4.4. Средства защиты информации, встроенные в операционную систему компьютера

В ранних версиях ОС встроенные средства защиты информации практически отсутствовали, а в последних версиях, например, в ОС Windows 10, система защиты информации решает с приемлемой степенью эффективности почти все вышеназванные задачи программно-аппаратной защиты. Недоверие к встроенным средствам вызвано тем,

что ОС имеют, как правило, много «дыр», используя которые злоумышленники проникают в компьютеры жертв. Кроме того, эти ОС разработаны, как правило, компаниями США и к ним полный доступ имеют американские спецслужбы. Для устранения последнего недостатка в России разработаны две линейки отечественных ОС: РОСА — разработки российской компании «Научно-технический центр информационных технологий «РОСА» (НТЦ ИТ РОСА) и Astra Linux — разработки российской компании «РусБИТех» («Русские базовые информационные технологии»).

При использовании иностранных ОС в ИС с высокими требованиями к информационной безопасности, поверх ОС часто устанавливаются добавочные СКЗИ.

Типовая современная система защиты ОС содержит:

1) средства аутентификации и идентификации;

2) средства разграничения доступа;

3) средства оперирования с носителями информации и их защиты;

4) средства шифрования файлов;

5) средства защиты от вредоносного ПО, включая:

— встроенный в ОС межсетевой экран. В ОС компании Microsoft межсетевой экран появился в Windows XP SP2;

— подсистему автоматического обновления. Современные ОС являются очень сложными программными продуктами, и хакерам подчас удается найти в них уязвимости, позволяющие получить контроль над компьютером. Когда об этом становится известно программистам компании — производителя ОС (например, Microsoft), теоретически сразу же выпускается обновление системы, ликвидирующее уязвимость. На практике эти уязвимости своевременно устраняются не всегда. Тем не менее, своевременное обновление Windows позволит защититься от взлома с использованием большинства известных уязвимостей.

— Defender — сканер системы. Например, в Windows Defender входит ряд модулей безопасности, отслеживающих подозрительные изменения в определенных сегментах системы в режиме реального времени. Также программа позволяет быстро удалять установленные приложения ActiveX[1]. С помощью доступа к сети Microsoft SpyNet есть возможность отправлять сообщения о подозрительных объектах

[1] ActiveX — технология на основе которой создаются компоненты для программирования сайтов под Интернет эксплорер.

в компанию Microsoft, для определения его возможной принадлежности к spyware (шпионским программам). Заметим, что для решения аналогичной задачи, только на уровне государства, в нашей стране под началом 8 центра ФСБ создается государственная система сбора и обмена информацией о компьютерных атаках на территории Российской Федерации и ее заграничных учреждений (ГОССОПКА).

4.5. Автономные средства защиты информации

Автономные средства защиты информации это отдельные аппаратные и программные средства, включаемые в состав СЗИ, если средств ОС для обеспечения безопасности недостаточно. К числу таких средств относятся:

— программы надежного стирания (Ccleaner, Eraser, File Shreder и др.);

— программы удаления остаточных данных и остатков программ (тот же Ccleaner, Uninstall Tool, Soft Organizer и др.);

— программы восстановления удаленных файлов (Undelete, Free Undelete, USB Flash Drive Recovery и др.);

— программы управления USB портами (USB manager, USB deview, Shelmedia и др.);

— антивирусные программы (Kaspersky Lab, Doktor Web, 360 Total Security и др.);

— межсетевые экраны, системы обнаружения вторжений, виртуальные частные сети;

— сканеры безопасности (Nmap, Xspider, СканерВС и др.);

— программы защиты от исследования: дизассемблеры и отладчики (IDA Pro, IDA Freeware, Olly Debugger, Sysel Kernel Debugger и др.) и пр.

В настоящее время в сети «Интернет» имеется очень большое количество этих средств, как коммерческих, так и бесплатных — средств свободного распространения. Собирать из этих средств систему защиты информации, дополняющую ОС — дело хлопотное и неблагодарное. Поэтому, если средств ОС недостаточно, то организации обычно предпочитают закупать добавочные СЗКИ. Исключение составляют антивирусные программы, которые в настоящее время есть практически на каждом компьютере.

4.6. Специализированные системы защиты компьютерной информации

Специализированные (добавочные) системы защиты информации (СЗКИ или UTM системы) — мощные программы, которые работают совместно с ОС и позволяют эффективно решать задачи по защите информации: отслеживать работу внутренних пользователей системы, обеспечивать передачу конфиденциальных данных по открытым каналам и пр. Иногда эти средства называют комплексными. К этому классу средств защиты можно отнести отечественные программно-аппаратные комплексы «Страж NT», «Аккорд», «Dallas Lock», «Secret NET» и др. Отметим, что эти средства не предназначены для антивирусной защиты напрямую и существуют, как правило, вместе с ними. Эти средства встраиваются между BIOS и MBR.

Как известно, при включении питания в ходе стандартной загрузки компьютера начинает работу программа самотестирования POST (Power-On Self-Test). После тестирования из ПЗУ BIOS в оперативную память компьютера загружается главная загрузочная запись — MBR (Master Boot Record), на которую передается управление компьютером. Программа первоначальной загрузки (Non-System Bootstrap — NSB — несистемный загрузчик) является первой частью MBR. NSB анализирует таблицу разделов жесткого диска (Partition Table), являющуюся второй частью MBR, и определяет по ней расположение (номера сектора, цилиндра и стороны) активного раздела, содержащего рабочую версию ОС. Определив активный (загрузочный) раздел жесткого диска, программа NSB считывает его нулевой сектор (Boot Record — BR — загрузочную запись) и передает ей управление. Алгоритм работы загрузочной записи зависит от ОС, но обычно состоит в запуске непосредственно ОС или программы — загрузчика ОС.

Добавочные СЗИ, как правило, имеют аппаратную составляющую и обеспечивают идентификацию и аутентификацию пользователей, проверку целостности критичных системных файлов и аппаратных средств до загрузки ОС. Основными функциональными «обязанностями» этих СЗИ являются:

— организация доверенной загрузки с возможностью идентификации и аутентификации пользователей при помощи ключевых дискет, электронных ключей Touch memory, USB-ключей eToken R2, eToken Pro, Guardant и т. п., включая авторизацию пользователей во временной области;

— контроль целостности системных областей жесткого диска, назначенных администратором безопасности системы;

— контроль целостности конфигурации аппаратных средств;

— регистрацию событий доступа в энергонезависимой памяти.

Разработчики этого класса СЗИ заявляют свои продукты как «комплексы» защиты АС от НСД и оснащают их дополнительными функциональными возможностями, реализующими меры защиты в работающей КС:

— дискреционная и (или) мандатная модели разграничения доступа пользователей к защищаемым ресурсам и прикладным программам;

— создание для пользователей замкнутой программной среды;

— контроль потоков защищаемой информации;

— очистка освобождаемой памяти и дискового пространства;

— контроль целостности запускаемых программ и баз данных;

— аудит доступа к защищаемым ресурсам;

— управление вводом/выводом на отчуждаемые носители.

Рассмотрим кратко назначение и возможности некоторых из этих средств.

СЗИ «Страж NT» разработано научно-исследовательским институтом проблем управления, информатизации и моделирования Академии военных наук (ЗАО «НИИ УИМ АВН»). Аппаратная часть комплекса предназначена для идентификации пользователей на основе электронных ключей Touch Memory. В то же время идентификация пользователей в «Страж NT» может осуществляться за счет использования ключевых дискет, которые создаются самим средством для каждого пользователя. В качестве средства аутентификации применяется пароль. Средство обеспечивает доверенную загрузку путем модификации главной загрузочной записи жесткого диска.

Изделие «Dallas Lock», разработанное ООО «Конфидент», — это комплексное средство защиты, в котором доверенная загрузка осуществляется путем аутентификации пользователей на основе электронных идентификаторов Touch Memory.

При инициализации системы на компьютере модифицируется главная загрузочная запись жесткого диска. СЗИ «Dallas Lock» позволяет осуществлять защиту приватных данных путем шифрования указанной области данных на жестком диске компьютера (например, загрузочной записи логического раздела диска).

Комплексное средство защиты информации «Secret Net» разработано ЗАО НИП «ИНФОРМЗАЩИТА», ныне — «Код безопасности»

(г. Москва). При аутентификации пользователей СЗИ может работать с различными электронными картами памяти (iButton, eToken, Smart Card, Proximity Card). Программная часть «Secret Net» представляет собой надстройку над стандартной системой безопасности MS Windows и начинает работать после загрузки основных модулей ОС.

Последняя версия (2020) программно-аппаратного средства Secret Net — Secret Net Studio предназначена для обеспечения безопасности ИС на компьютерах, функционирующих под управлением ОС MS Windows 10/8/7/Vista и WindowsServer 2012/2008. При использовании соответствующих подсистем изделие обеспечивает:

— защиту от НСД к информационным ресурсам компьютеров;

— контроль устройств, подключаемых к компьютерам;

— обнаружение вторжений в ИС;

— антивирусную защиту;

— межсетевое экранирование сетевого трафика;

— авторизацию сетевых соединений;

— централизованное управление функционированием средства.

Система Secret Net Studio состоит из следующих трех программных пакетов, устанавливаемых на компьютерах:

— «Secret Net Studio» (клиент);

— «Secret Net Studio — Сервер безопасности»;

— «Secret Net Studio — Центр управления».

Для обеспечения корректной доверенной загрузки СЗИ «Secret Net» необходимо использовать совместно с аппаратными средствами, например, электронным замком «Соболь-PCI».

Аппаратный модуль доверенной загрузки (АМДЗ) СЗИ «Аккорд», разработанный ОКБ САПР, имеет плату расширения, вставляемую в PCI-слот защищаемого компьютера. СЗИ перехватывает управление компьютером после выполнения BIOS процедуры POST. В качестве идентификаторов выступают электронные ключи Touch memory. Поставляемый в комплекте СЗИ считыватель этих устройств работает непосредственно с аппаратным модулем, а не подключается к стандартным портам ПЭВМ. Контрольные суммы проверяемых на целостность системных областей ОС и аппаратных средств хранятся в энергонезависимой памяти аппаратного модуля.

В последнее десятилетие на российском рынке стали появляться средства комплексной защиты информации, сочетающие в себе функции СЗИ от НСД и СКЗИ. Одним из таких средств является модификация комплекса «Аккорд» — «Аккорд-СБ», представляющее собой про-

граммно-аппаратный комплекс, включающий и аппаратный модуль доверенной загрузки, и аппаратный модуль криптографической защиты. Аппаратно-программный комплекс защиты информации «Secret Net» кроме широкого арсенала средств защиты от несанкционированного доступа предоставляет пользователю возможность создавать зашифрованные каталоги для хранения персональных данных.

К добавочным средствам защиты компьютерной информации можно отнести также DLP-системы (DLP — Data Leak Prevention — предотвращение утечки данных). Если рассмотренные выше добавочные средства информационной безопасности в основном решают задачи предотвращения проникновения злоумышленников внутрь системы, то DLP-системы предназначены для предотвращения утечек конфиденциальной информации из ИС наружу.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой ИС изнутри наружу. Эти системы способны выполнять и множество других функций: выявление внутренних злоумышленников, проверка качества выполнения сотрудниками своих обязанностей и пр. Среди отечественных DLP-систем выделим:

— DLP-систему InfoWatch группа компаний InfoWatch;

— DLP-систему «Контур информационной безопасности» компании СерчИнформ»;

— DLP-систему SecureTower компании Falcongaze.

Отметим, что компания InfoWatch тесно связана с компанией «Лаборатория Касперского» и ее продукты занимают до 30 % (по некоторым данным до 50 %) рынка DLP-систем в России.

4.7. Сетевая защита в компьютерных системах и сетях

Сетевая защита в КС реализуется в основном с использованием технологии межсетевых экранов, технологии обнаружений вторжений и технологии виртуальных частных сетей.

Межсетевой экран (нем. Brandmauer — противопожарная стена, англ. Firewall — противопожарная стена) — локальное или функционально-распределенное аппаратно-программное или программное средство, реализующее контроль над информацией, передающейся между двумя сетями или между сетью и автономным компьютером (рис. 4.2).

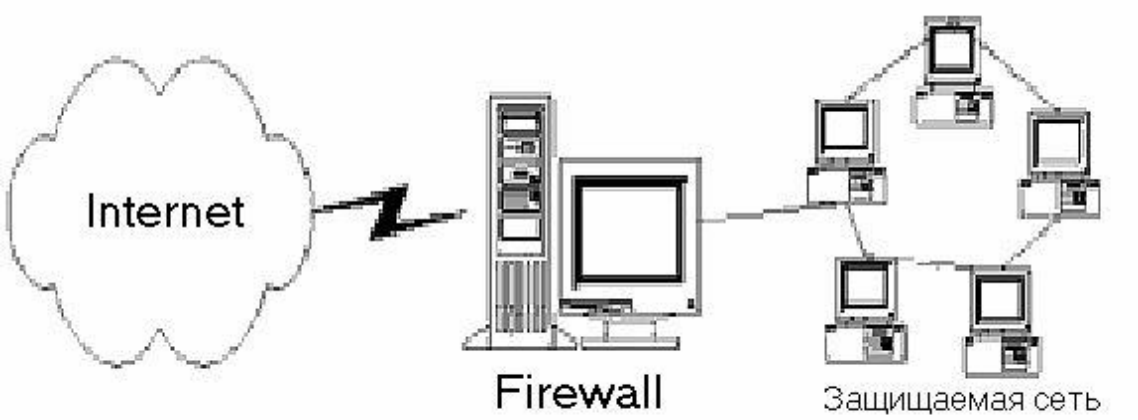

Рис. 4.2. Защита КС с помощью МЭ

Межсетевой экран просматривает пакеты, проходящие через него в обоих направлениях, и принимает решение об их пропуске или уничтожении. Таким образом, межсетевой экран защищает каждую из сетей, между которыми он расположен, друг от друга. Межсетевой экран является первым рубежом в системе эшелонированной обороны от сетевых атак.

Система обнаружения (предотвращения) вторжений — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в КС или сеть либо несанкционированного управления ими в основном через сеть «Интернет». Соответствующий английский термин — Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный по отношению к межсетевым экранам уровень защиты КС и являются вторым рубежом в системе эшелонированной обороны от сетевых атак.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность КС. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Виртуальные частные сети (Virtual Private Network — VPN) — это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия. Средства защиты сетевого действия (программные или аппаратно-программные) устанавливаются на тех компьютерах в составе локальной вычислительной сети, обмен информацией между которыми в открытом режиме

нецелесообразен. СЗИ этого класса основываются на криптографических методах защиты с использованием механизма открытых ключей.

Пусть имеются две территориально удаленные друг от друга локальные сети, принадлежащие одной организации и объединенные через Интернет. Соединения могут устанавливаться между любыми компьютерами этих сетей (рис. 4.3).

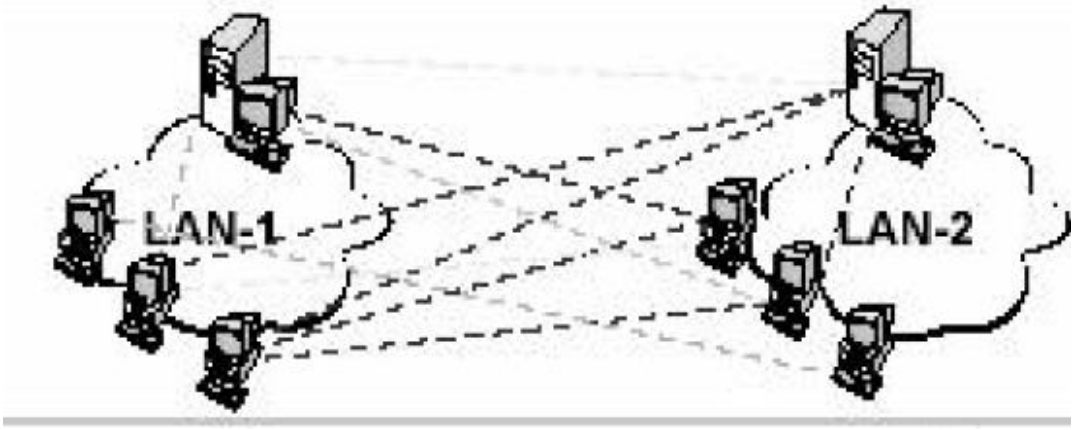

Рис. 4.3. Объединение двух локальных сетей через Интернет

Реальные соединения устанавливаются через посредников — черных ящиков, устанавливаемых на входе каждой локальной сети (рис. 4.4).

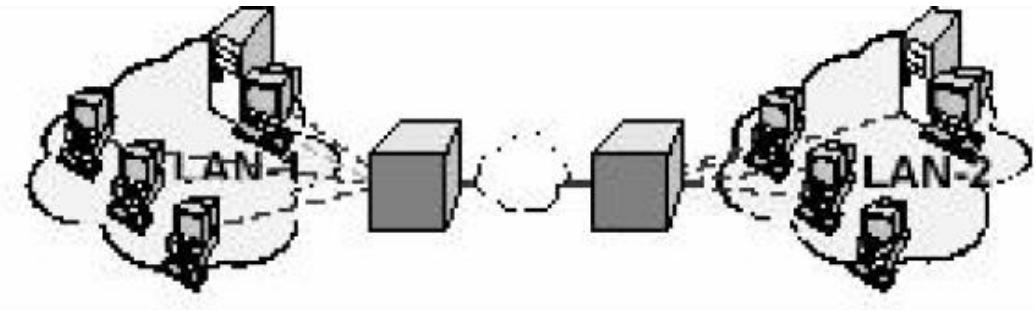

Рис. 4.4. Организация VPN-сети

Задача черных ящиков так отработать трафик между локальными сетями, чтобы злоумышленник не мог нарушить конфиденциальность, целостность и подлинность передаваемой информации. То есть передаваемая информация, включая ее содержимое, адреса отправителей и получателей, должна быть зашифрована и подписана.

Кроме того, задача черных ящиков защитить ЛВС от НСД к ним из сети «Интернет». Внешний наблюдатель может лишь увидеть, что идет зашифрованный обмен между двумя черными ящиками. При от-

правке пакетов по сети VPN применяется туннелирование, т. е. в пакетах, которые идут по открытой сети, в качестве адресов фигурируют только адреса черных ящиков, внутри ЛВС трафик передается в открытом виде, а его защита осуществляется только тогда, когда он попадает в туннель.

Если компьютер работает в незащищенном режиме, то в составе ЛВС он присутствует как равноправная рабочая станция. Перевод компьютера в защищенный режим означает шифрование всего входящего/исходящего трафика, включая адресную и служебную информацию, или только пакетированных данных. ПЭВМ, на которых не установлено соответствующее программное (аппаратно-программное) обеспечение просто не «видят» в сети станции, работающие под управлением сетевых СЗИ.

Все вышеотмеченное позволяет сделать вывод о том, что технология VPN решает задачи обеспечения конфиденциальности и целостности информации. Задачу обеспечения доступности информации технология VPN не решает. Классическим примером комплексного средства защиты, включающего в себя VPN, является принятое на вооружение МВД России отечественное программно-аппаратное средство сетевой защиты ViPNet, разработанное компанией «ИнфоТеКС» (Информационные Технологии и ТелеКоммуникационные Системы, г. Москва). Сетевые решения и технология ViPNet позволяют:

— защищать передачу данных, файлов, видеоинформации и переговоры, информационные ресурсы пользователя и корпоративной сети при работе с любыми приложениями Интернет/Интранет;

— создавать в открытой глобальной сети «Интернет» закрытые корпоративные Интранет-сети.

Контрольные вопросы:

1. Какие задачи решает ПАЗИ?
2. Как классифицируются ПАСЗИ?
3. Какие средства защиты, встроены в аппаратуру?
4. Какие средства защиты информации, встроены в операционную систему?
5. Назовите автономные СЗИ.
6. Какие специализированные системы защиты компьютерной информации применяются в настоящее время?

Лекция 5. Разграничение доступа к информации

Вопросы лекции:

5.1. Базовые функции подсистемы управления доступом.

5.2. Идентификация, аутентификация и авторизация.

5.3. Управление доступом пользователей к защищаемым ресурсам.

5.4. Модели доступа.

5.5. Корректность и полнота реализации политики разграничения доступа.

5.6. Создание замкнутой рабочей среды для пользователей.

В лекции посвященной классификации программно-аппаратных средств защиты информации мы привели решаемые с их помощью задачи. Одной из наиболее важных среди этих задач является задача защиты от НСД к информационным ресурсам со стороны внутренних и внешних нарушителей. Программно-аппаратные средства решения этой задачи состоят из следующих компонент (рис. 6.1):

— подсистема управления доступом;

— подсистема регистрации и учета;

— криптографическая подсистема;

— подсистема обеспечения целостности,

— подсистема антивирусной защиты,

— подсистема управления системой защиты информации от НСД.

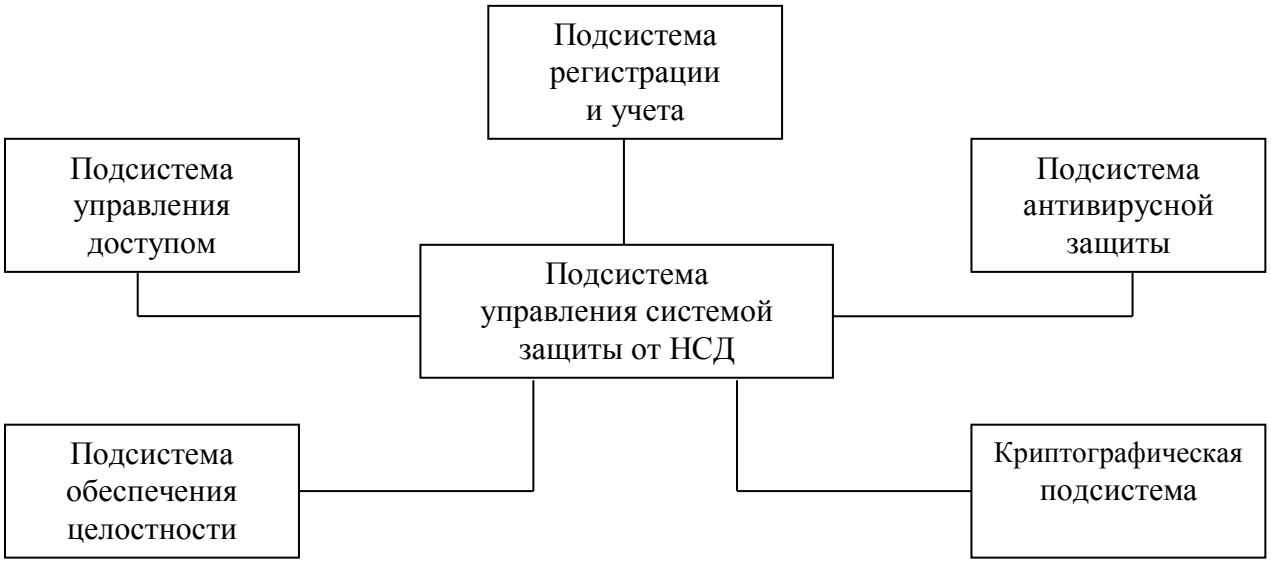

Рис. 5.1. Состав системы защиты информации от НСД

Часть из этих подсистем реализована в составе ОС, но может дополнительно быть реализована вне ее (например, в составе специали-

зированных систем защиты компьютерной информации), а часть — подсистема антивирусной защиты, криптографическая подсистема и подсистема обеспечения целостности — обычно реализуется вне ОС. Здесь мы рассмотрим подсистему управления доступом.

5.1. Базовые функции подсистемы управления доступом

Подсистема управления доступом является основополагающей для реализации защиты от НСД. Остальные подсистемы реализуются в предположении, что механизмы защиты данной подсистемы могут быть преодолены злоумышленником. В частности, остальные подсистемы могут использоваться:

— для контроля действий пользователя — подсистема регистрации и учета;

— для противодействия возможности прочтения похищенной информации (например, значений паролей и данных) — 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 — подсистема обеспечения целостности.

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

Неотъемлемой частью системы защиты СЗИ от НСД является подсистема антивирусной защиты. Однако ее принято рассматривать как самостоятельную компоненту программно-аппаратной защиты информации. Мы так и поступим. Здесь же только заметим, что никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам.

К базовым функциям подсистемы управления доступом относятся (рис. 5.2):

— идентификация, аутентификация и авторизация пользователей;

— управление доступом пользователей к защищаемым ресурсам;

— создание замкнутой рабочей среды для пользователей.

Рис. 5.2. Базовые функции подсистемы управления доступом

Рассмотрим реализацию каждой из этих подсистем по отдельности.

5.2. Идентификация, аутентификация и авторизация

Идентификацию, аутентификацию и авторизацию можно считать основой программно-аппаратных средств разграничения доступа. Это «первая линия обороны», проходная информационного пространства организации. Для однозначного понимания последующего материала, введем несколько определений, заимствованных из РД ФСТЭК от 30.03.1992 г.: Защита от несанкционированного доступа к информации. Термины и определения.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Идентификация состоит из процедур и механизмов, позволяющих внешним агентам уведомлять систему об их личности. В вышеприведенном определении разделены понятия уведомления системы и гарантия того, что уведомление корректно. Поэтому идентификацию обычно объединяют со вторым типом процедур или механизмов, называемым аутентификацией.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «*аутентификация»* иногда используют словосочетание «проверка подлинности». С процедурами идентификации и аутентификации принято связывать еще одну процедуру — процедуру авторизации.

Авторизация — процесс назначения пользователю или субъекту прав доступа к объектам системы, прав управления этим доступом, а также контроля соблюдения этих прав. Авторизация — это не то же самое что идентификация и аутентификация: идентификация — это называние лицом себя системе; аутентификация — это установление соответствия лица названному им идентификатору; а авторизация — предоставление этому лицу возможностей в соответствие с положенными ему правами или проверка наличия прав при попытке выполнить какое-либо действие. Например, авторизацией являются лицензии на осуществление определенной деятельности.

К механизмам идентификации и аутентификации, кроме установления личности субъекта относятся следующие функции:

— добавление новых идентификаторов в систему с обеспечением аутентифицирующей информации и удаление устаревших идентификаторов и соответствующей аутентифицирующей информации;

— генерация, изменение и просмотр авторизованными пользователями информации аутентификации;

— проверка целостности и предотвращение неавторизованного использования информации аутентификации;

— ограничение количества попыток ввода некорректной информации идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

— нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т. п.);

— нечто, чем он владеет (личную карточку, смарт-карту, бейдж или иное устройство аналогичного назначения);

— нечто, что есть часть его самого (голос, отпечатки пальцев, снимок сетчатки глаза и т. п., т. е. свои биометрические характеристики).

Таким образом, методами аутентификации пользователей являются (рис. 5.3):

— парольная аутентификация;

— маркеры аутентификации;

— биометрическая аутентификация.

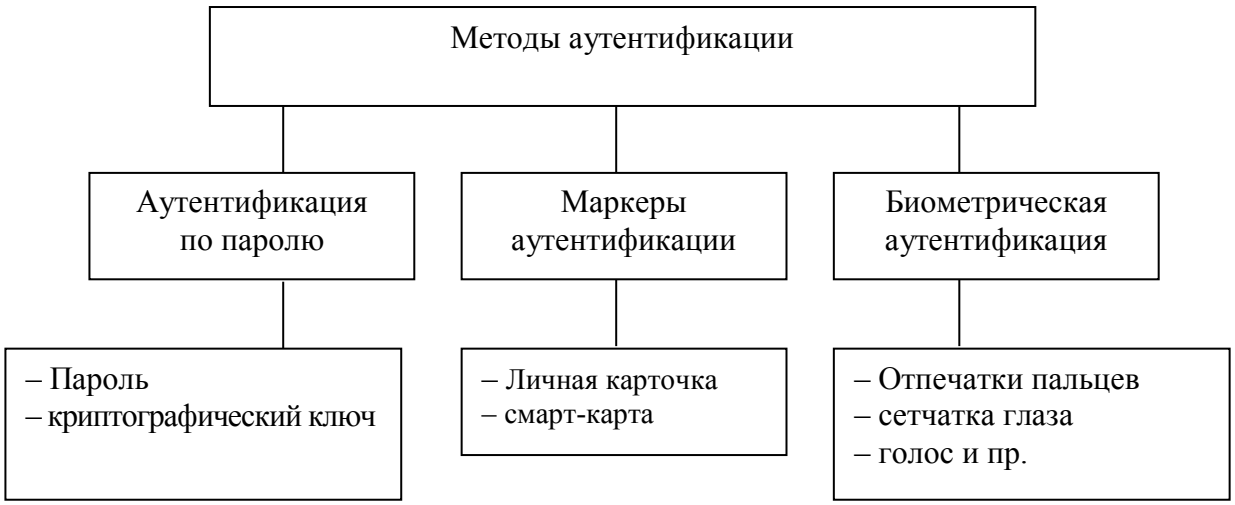

Рис. 5.3. Аутентификация (проверка подлинности) пользователей

Парольная аутентификация. Главное достоинство парольной аутентификации — простота и привычность. Пароли давно встроены в ОС и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности по следующим причинам:

1. Многие не знают, как выбрать сильный пароль. Очень часто используются короткие пароли (меньше четырех символов). Короткий пароль позволяет применить атаку «в лоб», т. е. хакер будет перебирать предположительные пароли, пока не подберет нужный. Если пароль имеет длину два символа (и это буквы русского алфавита), то число возможных комбинаций будет всего 1024 (32^2=1024). При длине пароля восемь символов, число комбинаций увеличивается примерно до 1099,5 млрд.

Существуют формулы для оценки времени атаки в лоб (перебора паролей). Эти формулы реализованы в некоторых сервисах, например, у компании BetterBuys есть бесплатный сервис, который определяет, сколько времени нужно для взлома конкретного пароля методом brute-force (полного перебора). Аналогичный сервис есть у лаборатории Касперского (Kaspersky Secure Password Check). Опишем метод в его наиболее простом варианте.

Пусть количество символов в алфавите паролей равно A, а длина пароля равна L. Тогда количество возможных паролей рассчитывается по формуле $S=A^L$, а ожидаемое безопасное время T_0 (полупроизве-

дение числа возможных паролей на время, требуемое для того, чтобы попробовать каждый пароль из последовательности запросов) — по формуле $T_0 = A^L \times t/2$, где t — время на ввод одного пароля.

Пусть $P_б$ — вероятность того, что пароль не будет взломан в течение времени $T_б$. Эта вероятность рассчитывается по формуле $P_б = T_б/(t \times A \times L)$, при условии, что $T_б/< A \times L$. Если последнее условие не выполняется, то $P_б$=1. Отсюда, задавшись вероятностью $P_б$, временем t и количеством символов алфавита A, мы можем найти минимально необходимую длину пароля, $L \geq [(ln(P_б) + ln(t) - ln(T_б)]/ln(A)$.

В более сложных вариантах учитывается статистика паролей по частоте и прочие нюансы.

2. Применяются легко угадываемые и слабые пароли. Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т. п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия пользователя.

Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил «карамба»; разумеется, этим же словом открывался сверхсекретный сейф.

Наглядный пример того, как слабые пароли помогают взламывать системы, — червь Морриса. В 1988 году студент Корнеллского университета Роберт Моррис разработал программу, которая распространялась через Интернет. Эта программа использовала несколько уязвимых мест для получения доступа к КС и воспроизведения самой себя. Одним из уязвимых мест были слабые пароли. Программа наряду со списком наиболее распространенных паролей использовала следующие пароли: пустой пароль, имя учетной записи, добавленное к самому себе, имя пользователя, фамилию пользователя и зарезервированное имя учетной записи. Этот червь в свое время нанес ущерб достаточно большому количеству систем и весьма эффективно вывел из строя Интернет.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

В основе парольной аутентификации лежит протокол аутентификации субъекта информационного взаимодействия, с помощью кото-

рого пользователь доказывает, что он знает свой пароль. При этом аутентификация происходит без разглашения самого пароля. Пароль, введенный пользователем, сравнивается с паролем, хранящимся в памяти компьютера и, при их совпадении, пользователь допускается к работе на компьютере в пределах отведенных ему полномочий.

Места хранения паролей известны. Так в ОС Microsoft Windows 7, пароли пользователей хранятся в реестре по адресу (C:/Windows/System32/config/SAM). Если бы они хранились в открытом виде, то их легко можно было бы найти. Поэтому пароли хранятся в зашифрованном виде. Шифруются они с помощью односторонних функций или известных алгоритмов шифрования, например, с помощью алгоритма DES. Рассмотрим механизм шифрования с помощью односторонних функций.

Односторонней называется такая функция y=f(x), что найти *y* при известном значении *x* достаточно легко, а найти *x* при известном значении *y* практически невозможно. При хорошей односторонней функции сложно также найти такие два значения x_1 и x_2, что $f(x_1) = f(x_2)$.

Пусть мы вводим пароль *x*. Система аутентификации с помощью односторонней функции находит *y* и записывает *y* в файл паролей. Все шифрованные пароли имеют обычно фиксированную длину. Взлом такого пароля возможен только методом полного перебора: злоумышленник вводит логин и пароль. Компьютер по логину находит шифрованный пароль и сравнивает его с введенным паролем. Злоумышленник вводит другой пароль и т. д., пока введенный им пароль не совпадет с паролем в файле паролей.

В некоторых системах применяются одноразовые пароли. Для таких паролей обычно применяется метод «запрос — ответ» или метод «ответ».

Учетная запись пользователя — совокупность идентификатора, пароля и, возможно, дополнительной информации описания пользователя. Учетная запись хранится в базе данных парольной системы.

Альтернативой паролям являются смарт-карты (маркеры аутентификации) и биометрия. Однако развертывание таких систем связано с дополнительными расходами

Маркеры аутентификации. Для установления личности применяются *смарт-карты* использование которых уменьшает риск угадывания пароля. Однако если смарт-карта украдена, и это — единственная форма установления подлинности, то похититель сможет замаскироваться под легального пользователя КС. Смарт-карты не смогут

предотвратить атаку с использованием уязвимых мест, поскольку они рассчитаны на правильный вход пользователя в систему.

Еще одна проблема — это стоимость смарт-карт, за каждую нужно заплатить от 50 до 100 долларов. Организации с большим количеством служащих потребуются серьезные затраты на оплату такой безопасности.

Биометрические системы — еще один механизм аутентификации, который значительно уменьшает вероятность угадывания пароля.

Существует множество биометрических сканеров для верификации следующего:

— отпечатков пальцев;
— сетчатки/радужной оболочки;
— отпечатков ладоней;
— конфигурации руки;
— конфигурации лица;
— голоса.

Биометрия представляет собой совокупность автоматизированных методов *идентификации* и/или *аутентификации* людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности *отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица* и т. п. К поведенческим характеристикам относятся *динамика подписи* (ручной), стиль *работы с клавиатурой*. На стыке физиологии и поведения находятся анализ особенностей *голоса и распознавание речи*. Каждый подход предполагает использование определенного устройства для идентификации человеческих характеристик. Обычно эти устройства довольно сложны, чтобы исключить попытки обмана. Например, при снятии отпечатков пальцев несколько раз проверяются температура и пульс. При использовании биометрии возникает множество проблем, включая стоимость развертывания считывающих устройств и нежелание сотрудников их использовать.

5.3. Управление доступом пользователей к защищаемым ресурсам

После идентификации, аутентификации и авторизации пользователя система защиты должна постоянно контролировать правомерность его доступа компьютерным ресурсам. При попытке доступа пользователя к какому-либо ресурсу система защиты должна проанализировать его полномочия, находящиеся в соответствующей базе

данных, и разрешить доступ только в случае соответствия запроса на доступ пользовательским полномочиям.

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением доступа или управлением доступом, а подсистему защиты, выполняющую эти функции — подсистемой разграничения доступа или управления доступом к ресурсам КС (рис. 5.4).

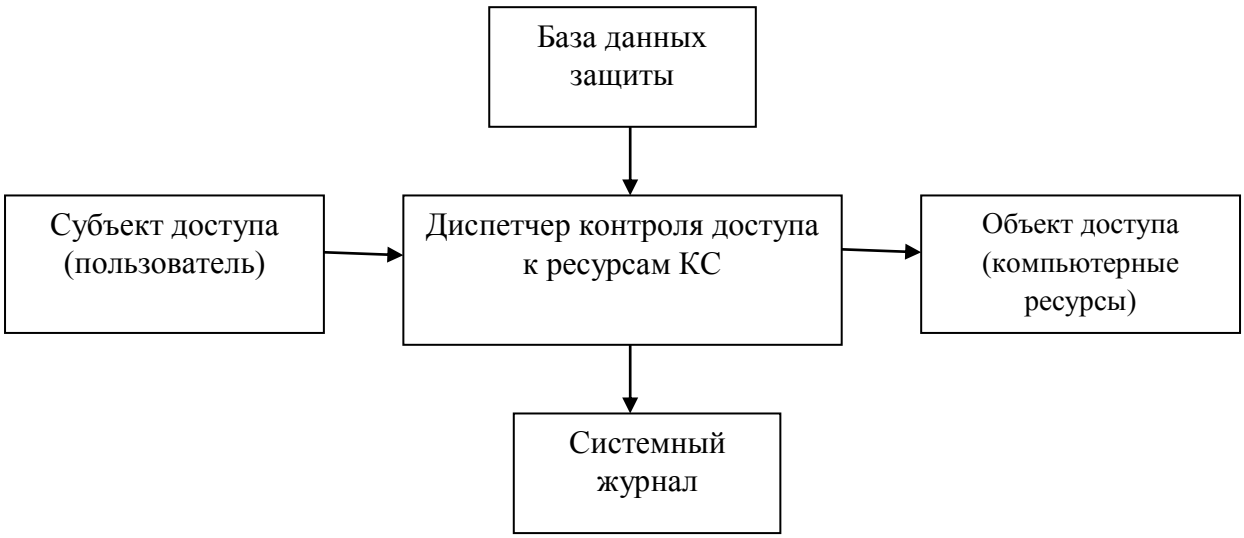

Рис. 5.4. Подсистема управления доступом к ресурсам КС

Средства разграничения доступа позволяют специфицировать и контролировать действия, которые субъекты — пользователи и процессы могут выполнять над объектами — информацией и другими компьютерными ресурсами. Логическое управление доступом, реализуемое после идентификации и аутентификации пользователей, — это один из основных способов, призванный обеспечить конфиденциальность, целостность и подлинность информационных объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей.

Механизмы управления доступом лежат в основе защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к объектам КС. Наличие этих механизмов необходимо, даже если в системе работает только один пользователь. Тогда этот единственный пользователь является администратором системы и при необходимости он может создавать учетные записи другим пользователям.

Подсистема разграничения доступа к компьютерным ресурсам реализует концепцию единого диспетчера доступа, являющегося посредником при всех обращениях субъектов к объектам.

Диспетчер доступа должен выполнять следующие функции:

— проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты (правил разграничения доступа);

— при необходимости регистрировать факт доступа и его параметры в системном журнале регистрации.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

— идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т. п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;

— атрибуты субъекта (метка безопасности, группа пользователя и т. п.). Метки безопасности — основа принудительного (мандатного) управления доступом;

— роли — основа ролевого управления доступом.

Если при попытке доступа пользователя к компьютерным ресурсам подсистема разграничения определяет факт несоответствия запроса на доступ пользовательским полномочиям, то доступ блокируется, и могут предусматриваться следующие санкции за попытку НСД:

— предупреждение пользователя;

— отключение пользователя от вычислительной системы на некоторое время;

— полное отключение пользователя от системы до проведения административной проверки;

— подача сигнала службе безопасности о попытке НСД с отключением пользователя от системы;

— регистрация попытки НСД.

5.4. Модели доступа

Общие сведения

Механизмы управления доступом реализуют модели, которые, во-первых, определяют правила разграничения доступа субъектов к объектам, а, во-вторых, — правила обработки запросов доступа к защищаемым ресурсам. Рассмотрим некоторые из этих моделей.

Одной из первых моделей доступа была *модель Биба* (1977). В этой модели все субъекты и объекты распределяются по несколь-

ким уровням доступа. Затем на их взаимодействие накладываются следующие ограничения:

— субъект не может вызывать на исполнение объекты с более низким уровнем доступа;

— субъект не может модифицировать объекты с более высоким уровнем доступа.

Модель Гогена-Мезигера (1982). Субъекты и объекты в данной модели делятся на группы (домены). Система при каждом действии может переходить из одного разрешенного состояния только в несколько других. Переход из одного состояния в другое выполняется по правилам, задаваемым таблицей разрешений. В этой таблице указано, какие операции может выполнять субъект из одного домена с объектами другого домена.

Известны и другие модели: *сазерлендская модель* (1986), *модель Кларка-Вильсона* (1987), *ролевая модель, дискреционная модель, мандатная модель* и т. д. В настоящее время наибольшее распространение получили дискреционная (матричная), мандатная (многоуровневая) и ролевая модели.

Руководящие документы ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 30.03.1992 г. и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30.03.1992 г. определяют, что основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является дискреционная модель управления доступом, а при обработке сведений секретного характера — мандатная модель управления доступом.

Дискреционная модель доступа

В терминах дискреционной модели управления доступом (discretionary access control — DAC) — модели Харрисона-Руззо-Ульмана, состояние системы защиты описывается тройкой (*S*, *O*, *M*), где: *S* — множество субъектов, *O* — множество объектов, *M* — матрица доступа. Значение элемента *M*(*S*,*O*) определяет права доступа субъекта *S* к объекту *O*. Права доступа регламентируют способы обращения субъекта к различным типам объектов. В частности, права доступа субъектов к файловым объектам обычно определяются как: чтение — *R*, запись — *W* и выполнение — *E*.

Основу дискреционной модели составляет, как правило, матрица доступа, в которой каждому субъекту соответствует своя строка, а каждому объекту — свой столбец. В клетках на пересечении строк и столбцов указывается, какие права доступа имеет данный субъект по отношению к данному объекту (табл. 5.1). Как следует из данной таблицы, субъекту *m* разрешен доступ по чтению и записи к объекту 1, не разрешен никакой вид доступа к объекту 2 и разрешен доступ к объекту *n* по выполнению.

Таблица 5.1

Матрица доступа субъектов к объектам

Субъекты доступа	**Объекты доступа**			
	Объект 1	**Объект 2**	**„„**	**Объект n**
Субъект 1	R		„„	R,W
Субъект 2		R,W, E	„„	R
…	…	…	…	…
Субъект m	R,W		„„	E

В дискреционных моделях исключительно важным является понятие собственника объекта. Каждый объект имеет собственника. Собственник имеет все права доступа к своему объекту, а иногда — и право передавать часть или все свои права другим пользователям. Кроме того, собственник объекта определяет права других пользователей к своему объекту, т. е. политику безопасности по отношению к своему объекту.

Возможны несколько подходов к построению систем дискреционного управления доступом:

— распределенная схема администрирования, в которой имеется несколько собственников информации. Каждый собственник имеет право устанавливать права доступа других субъектов к своим объектам;

— централизованная схема администрирования, в которой система имеет одного выделенного субъекта — суперпользователя (обычно это администратор системы), который имеет право устанавливать права владения для всех остальных субъектов системы;

— субъект с определенным правом доступа может передать это право любому другому субъекту.

Сколь-нибудь гарантированную защиту информации можно реализовать только при принятии концепции полностью централизованной схемы администрирования, что подтверждается известными угрозами ОС.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве ОС.

Прямолинейное представление матрицы доступа невозможно (поскольку она очень большая), да и не нужно (поскольку она разрежена, т. е. большинство клеток в ней пусто). Существует два компактных варианта представления этой матрицы:

1. *Листы возможностей*. В этом варианте для каждого субъекта S_i создается лист (файл) всех объектов, к которым имеет доступ данный субъект.

2. *Листы контроля доступа* (ACL, Access Control List). В этом варианте для каждого объекта создается список всех субъектов, имеющих к нему право доступа.

Компактность представления матрицы доступа в обоих вариантах достигается за счет того, что пустые клетки не учитываются.

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:

— система защиты должна контролировать доступ наименованных субъектов к наименованным объектам (файлам, папкам, программам и пр.);

— для каждой пары субъект — объект должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать, исполнять и т. д.);

— система защиты должна иметь механизм, реализующий дискреционные правила разграничения доступа;

— контроль доступа должен быть применим к каждому объекту и каждому субъекту;

— механизм реализации дискреционного принципа контроля доступа должен предусматривать возможности санкционированного изменения правил и прав разграничения доступа, в том числе — возможность изменения списка субъектов и объектов;

— возможность изменять правила и права разграничения доступа должна быть предоставлена выделенным субъектам (администрации, службе безопасности и т. п.);

— должны быть предусмотрены средства управления, ограничивающие распространения прав на доступ.

К достоинствам дискреционной политики безопасности можно отнести простую реализацию системы разграничения доступа. Большинство КС обеспечивают выполнение именно этой политики безопасности.

Наиболее ощутимый недостаток дискреционной политики безопасности — излишняя детализация описания отношений субъектов и объектов. Такая детализация усложняет администрирование системы защиты, что приводит к возникновению ошибок. Еще один недостаток связан с тем, что дискреционная модель не выдерживает атак типа «троянский конь». К недостаткам относится также статичность определенных в ней правил разграничения доступа, не учитывающих динамику изменений состояния КС. Наконец, при использовании дискреционной политики безопасности возникает вопрос об определении правил распространения прав доступа и об анализе их влияния на безопасность КС.

В общем случае при использовании дискреционной политики безопасности перед системой защиты, которая при санкционировании доступа субъекта к объекту руководствуется некоторым набором правил, возникает алгоритмически неразрешимая задача проверки, не приведут ли действия субъекта, делегирующего свои права доступа другим субъектам, к нарушению политики безопасности.

Большинство ОС (Windows, Linux и др.) и СУБД реализует именно дискреционное управление доступом и, как правило, на механизме ACL.

Мандатная модель управления доступом

Недостатков, присущих дискреционным моделям, лишены мандатные модели управления доступом (mandatory access control — MAC). Классическими примерами мандатных моделей являются модель конечных состояний Белла-ЛаПадула и решетчатая модель Д. Деннинга. Эти модели основываются на правилах секретного документооборота, применяемых во многих странах, в том числе и в России.

Мандатная модель предполагает формализацию процедуры назначения прав доступа посредством использования меток конфиденциальности (мандатов), назначаемых субъектам и объектам доступа. Для субъекта метки могут определяться в соответствии с его

уровнем допуска к информации (формой допуска), а для объекта — признаками конфиденциальности информации (степенью секретности информации). Права доступа субъекта и характеристика конфиденциальности объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности. Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений (секретно, совершенно секретно, совершенно секретно особой важности).

Основу реализации мандатного управления доступом составляют:

— формальное сравнение метки субъекта, запросившего доступ и метки объекта, к которому этот запрос относится;

— принятие решения о предоставлении доступа на основе двух правил, в основе которых лежит противодействие снижению уровня защищаемой информации. Суть этих правил заключается в следующем (рис. 5.5):

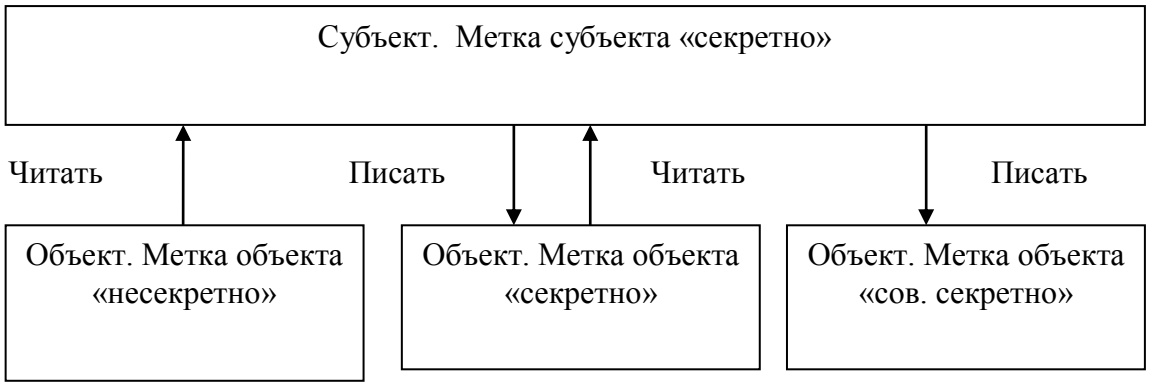

Рис. 5.5. Правила мандатной модели доступа

1. Субъект имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности. Это правило обеспечивает защиту информации, обрабатываемой более высокоуровневыми пользователями, от доступа со стороны низкоуровневых пользователей.

2. Субъект имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности. Это правило предотвращает намеренное или случайное доведение высокоуровневой информации до низкоуровневых пользователей.

Многоуровневая модель предупреждает возможность преднамеренного или случайного снижения уровня конфиденциальности защищаемой информации за счет ее утечки или умышленного пере-

носа. Эта модель препятствует переходу информации от объекта с более высоким уровнем конфиденциальности и узким набором категорий доступа к объекту с меньшим уровнем конфиденциальности и более широким набором категорий доступа. Таким образом, основная цель мандатной политики безопасности — предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем.

Практика свидетельствует, что мандатные модели более соответствуют потребностям жизни, чем дискреционные. При этом, так как отдельно взятые категории одного уровня равнозначны, чтобы их разграничить, наряду с многоуровневой мандатной моделью требуется применение матричной модели.

Многоуровневые модели делают значительно проще процедуру администрирования: как исходной настройки разграничительной политики доступа, так и последующего включения (исключения) новых объектов и субъектов доступа. Для этих моделей задача проверки безопасности является алгоритмически разрешимой.

Ролевая модель управления доступом

Ролевой моделью управления доступом (RBAC — role-based access control) называется способ построения систем разграничения доступа авторизованных пользователей. Ролевая модель управления доступом есть результат развития дискреционной модели. Вместе с тем, эта модель обладает рядом новых свойств: управление доступом в ней осуществляется на основе определения прав доступа для ролей, путем сопоставления ролей пользователям и установки правил, регламентирующих использование ролей во время сеансов.

Понятие «субъект» здесь заменяется на понятия пользователь и роль: пользователь — это человек, работающий с системой и выполняющий определенные обязанности, роль — это действующая в системе абстрактная сущность, с которой связан набор полномочий, необходимый для выполнения определенных функций. Один пользователь может быть авторизован на выполнение одной или нескольких ролей. Одна роль также может быть сопоставлена одному или нескольким пользователям.

При использовании ролевой модели управление доступом осуществляется в два этапа:

— для каждой роли указывается набор разрешений на доступ к различным объектам ИС;

— каждому пользователю назначается список доступных ролей.

Обозначим:

U — множество пользователей;

R — множество ролей;

P — множество разрешений на доступ к объектам ИС;

S — множество сеансов работы пользователя с системой;

$PA \subseteq P \times R$ — множество полномочий, установленных ролям (может быть представлено в виде матрицы доступа);

$UA \in U \times R$ — соответствие между пользователями и доступными им ролями.

Процесс определения прав доступа для пользователя, открывшего сеанс работы с системой, описывается с помощью следующих трех функций:

1) $user: S \to U$ — для каждого сеанса $s \in S$ эта функция определяет пользователя, который осуществляет этот сеанс работы с системой: $user(s) = u/u \in U$;

2) $role(s)$ — для каждого сеанса $s \in S$ данная функция определяет подмножество ролей, которые могут быть одновременно доступны пользователю в ходе данного сеанса: $role(s) = \{r_i/(user(s), r_i) \in UA\}$;

3) $permissions: S \to P$ — для каждого сеанса $s \in S$ эта функция задает набор доступных в нем полномочий, который определяется путем объединения полномочий всех ролей, задействованных в этом сеансе: $permissions\ (s) = U_{r \in roles(s)}\{p_i/(p_i, r) \in PA\}$.

В качестве критериев безопасности ролевой модели используется правило: система безопасна, если любой пользователь, работающий в сеансе $s \in S$ может осуществлять действия, требующие полномочий $p \in P$ только в том случае, если $p \in permissions\ (s)$.

Имеется несколько ролевых моделей управления доступом, различающихся видом функций user, roles, permissions, а также ограничениями, накладываемыми на множества PA и UA.

Например, роли могут образовывать иерархии, и каждая роль наследует полномочия подчиненных ей ролей. Могут быть определены взаимоисключающие роли, которые не разрешается одновременно назначать одному пользователю. Могут вводиться ограничения на одновременное использование ролей в рамках одной сессии, количественные ограничения при назначении ролей и полномочий, группировка ролей и полномочий и т. д.

5.5. Корректность и полнота реализации политики разграничения доступа

При внедрении сформированной политики разграничения доступа в КС необходимо оценить, насколько корректно эта политика реализована и насколько она полна.

Под *корректностью* понимается свойство механизма управления доступом полностью разделять ресурс между субъектами системы. Разграничение доступа должно быть реализовано так, чтобы различные пользователи имели доступ к непересекающимся элементам разделяемого ресурса, что исключит возможность несанкционированного обмена между ними информацией посредством данного ресурса.

Под полнотой понимается свойство системы защиты обеспечивать корректную реализацию разграничительной политики доступа ко всем ресурсам системы, с помощью которых возможен несанкционированный обмен информацией субъектов между собой.

В системах защиты компьютерной информации, владельцем информации которых не является пользователь, доверенным лицом владельца информации (государства, ведомства, предприятия) должен быть некий субъект внешний по отношению к обрабатываемой информации. Этот субъект обладает доверием со стороны владельца информации и наделяется специальными полномочиями. Таким субъектом является администратор безопасности.

Задачи настройки правил разграничения доступа, решаемые администратором безопасности, являются очень объемными. Он должен безошибочно задать полномочия множества субъектов по отношению к множеству объектов. Средства задания полномочий доступа ОС являются недостаточно прозрачными. Это делает контроль системы разграничения доступа с их помощью весьма затруднительным. Для контроля системы разграничения доступа целесообразно использовать дополнительные средства наглядного представления структуры объектов доступа и полномочий пользователей.

В качестве таких средств часто используется программа Ревизор XP. Эта программа предназначена для автоматической проверки соответствия прав пользователей по доступу к защищаемым ресурсам. Основные ее возможности:

— отображение всей информации, содержащейся в правилах разграничения доступа;

— сравнение структуры ресурсов КС, описанной в правилах разграничения доступа, с реальной структурой;

— построение плана тестирования КС;

— проверка реальных прав доступа пользователей к объектам системы;

— вывод результатов тестирования на экран или в текстовый файл с возможностью вывода на печать.

5.6. Создание замкнутой рабочей среды для пользователей

Важную роль в системе разграничения доступа играет создание для каждого пользователя ограниченной виртуальной среды, скрывающей запрещенные ресурсы и не предоставляющей средства доступа к этим ресурсам. С этой целью для рабочих станций достаточно создать замкнутое интерфейсное окружение, при котором пользователь будет иметь возможность доступа только к тем программам и элементам интерфейса, которые разрешены администратором. В этом случае можно заблокировать доступ к панели управления, системным дискам рабочих станций и установить список только разрешенных программ. Данные возможности на основе использования правил системной политики предоставляют встроенные средства ОС Microsoft Windows, начиная с Windows 98/NT и ряда других современных ОС.

Контрольные вопросы:

1. Назовите базовые функции подсистемы управления доступом.

2. Дайте определение «идентификация», «аутентификация» и «авторизация».

3. Какие существуют виды управления доступом пользователей к защищаемым ресурсам?

4. Перечислите модели доступа.

5. Что включает в себя корректность и полнота реализации политики разграничения доступа?

6. Как создается замкнутая рабочая среда для пользователей?

Лекция 6. Защита информации в сетях

Вопросы лекции:

6.1. Принципы адресации и передачи информации в сети «Интернет».

6.2. Межсетевые экраны.

6.3. Системы обнаружения вторжений.

6.4. Виртуальные частные сети.

В предыдущей лекции мы рассмотрели механизмы решения задачи защиты компьютерной сети за счет аутентификации, идентификации, авторизации и разграничения доступа. Эти механизмы предполагают, что субъекты и объекты информационного взаимодействия находятся внутри КС, и связаны между собой определенными разрешениями и запретами на доступ субъектов к объектам.

Для защиты от доступа внешних субъектов к объектам сети и внутренних субъектов сети к внешним объектам, вследствие неопределенно большого количества внешних субъектов и объектов, такие механизмы не подходят. Нужны иные — сетевые механизмы защиты. Основными из этих механизмов являются межсетевые экраны, системы обнаружения вторжений и виртуальные частные сети. В лекции, посвященной классификации программно-аппаратной защиты информации, мы кратко пояснили назначение этих механизмов. Теперь рассмотрим их более подробно. Но для того чтобы лучше уяснить излагаемый материал, начнем с принципов адресации и передачи информации в сети «Интернет».

6.1. Принципы адресации и передачи информации в сети «Интернет»

Каждый компьютер (узел, хост) в сети «Интернет» имеет уникальный IP-адрес (Internet Protocol Address), состоящий из четырех десятичных чисел (от 0 до 255), разделенных точкой, например: 195.34.32.116. Однако так как обмениваются информацией не компьютеры, а работающие на них приложения, знание IP-адреса недостаточно. Каждое приложение обменивается информацией через определенный порт [1], имеющий свой уникальный номер. Всего портов 2^{16}=65536. Комбинация IP-адреса компьютера и номера порта назы-

[1] Следует различать порты, через которые приложения обмениваются сообщениями и порты ввода/вывода применительно к архитектуре — разъемы, позволяющие подключать к компьютеру периферийные устройства, а также обслуживающие эти разъемы микросхемы.

вается сокет. Пример сокета: 195.34.32.116:53. Здесь первые четыре комбинации десятичных цифр IP-адрес компьютера, последняя пятая комбинация — номер порта. Большинство серверных приложений имеют стандартные фиксированные номера портов в диапазоне от 0 до 1024. Так почтовый сервис привязан к порту 25, Веб сервис — к порту 80, FTP — к порту 21 и т. д. Номера клиентских портов находятся в диапазоне от 1025 до 65536 и назначаются ОС динамически.

Человеку трудно запомнить цифровые IP-адреса. Поэтому в сети «Интернет» каждый IP-адрес связан с буквенно-цифровым доменным именем. Преобразованием доменного имени в цифровой IP-адрес занимается сервис доменных имен — DNS (Domain Name System).

Передача информации между компьютерами зависит от того, принадлежат они одной локальной сети или нет. Если принадлежат, то обмен происходит напрямую. Если нет, то обмен происходит через шлюзы (роутеры, маршрутизаторы), находящиеся на выходе каждой локальной сети. Для выяснения того, принадлежат обменивающиеся информацией компьютеры одной сети или нет, служит маска сети.

Информация, предаваемая между компьютерами разных локальных сетей, делится на пакеты. Каждый пакет содержит: адреса отправителя и получателя, передаваемые данные и служебную информацию. Взаимодействие между адресатами осуществляется по технологии «клиент — сервер». Клиент запрашивает информацию, сервер принимает и обрабатывает запрос, затем посылает ответ.

Передача информации по сети «Интернет» осуществляется в соответствии с правилами, описанными в стеке протоколов TCP/IP. Название свое этот стек получил по двум наиболее важным протоколам — TCP (Transmission Control Protocol) и IP (Internet Protocol). В стек входит несколько десятков протоколов, которые в настоящее время являются основными для сети «Интернет», а также для большинства корпоративных и локальных сетей.

Протоколы TCP/IP делятся на четыре уровня: прикладной, транспортный, сетевой и канальный. На каждом уровне передаваемая информация состоит из заголовка и данных. Заголовок и данные более высокого уровня инкапсулируется в данные более низкого уровня (рис. 6.1).

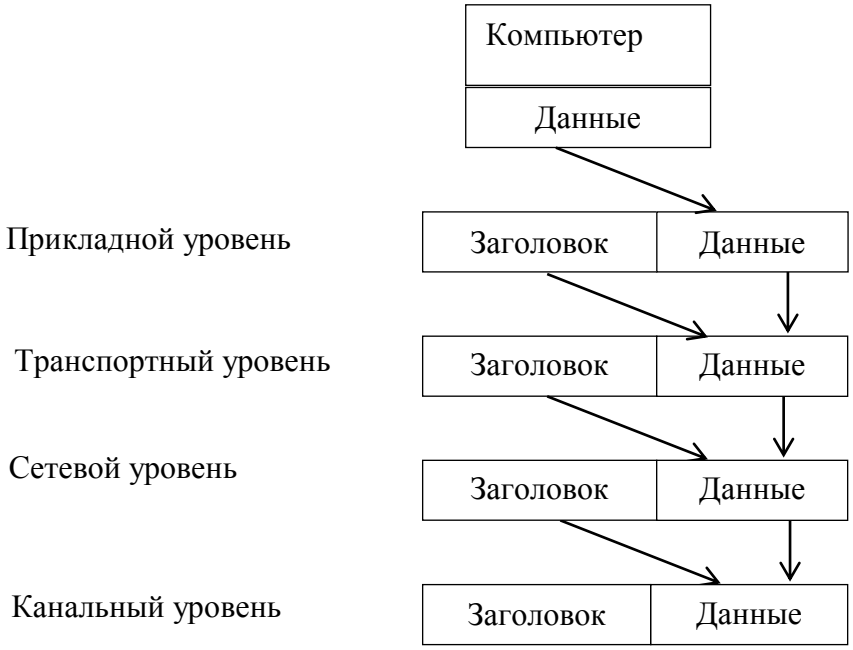

Рис. 6.1. Структура стека протоколов TCP/IP

Протоколы прикладного уровня это HTTP, FTP и т. д. Каждый протокол предназначен для обработки приложений своего типа.

На транспортном уровне данные прикладного уровня обрабатываются как единый блок. Полученная информация делится на сегменты, к ним добавляется заголовок и все это отправляется на сетевой уровень. К пакету добавляются порты отправителя и получателя.

На транспортном уровне используются протоколы TCP и UDP. TCP — это протокол с установлением соединения и с гарантированной доставкой пакетов. Вначале производится обмен специальными пакетами для установления соединения. Затем по этому соединению туда и обратно посылаются пакеты с проверкой того, дошел ли пакет до получателя. Если пакет не дошел, то он посылается повторно. UDP — это дайтаграммный протокол без установления соединения и с негарантированной доставкой пакетов.

Сетевой уровень из полученной информации формирует пакеты, добавляя заголовки. Сетевой уровень отвечает за: определение маршрутов доставки, передачу пакетов между сетями, присвоение уникальных адресов. На сетевом уровне используется протокол IP.

На канальном уровне определяется взаимосвязь между устройством и физической средой передачи, добавляется заголовок. Этот уровень отвечает за кодировку данных и подготовку их для передачи по физической среде. На этом уровне работают сетевые коммутаторы.

На приемном конце пакет будет обработан по той же модели, но в обратном порядке (рис. 6.2).

Рис. 6.2. Модель взаимодействия протоколов стека TCP/IP

6.2. Межсетевые экраны

Технология межсетевых экранов (МЭ) является одной из наиболее разработанных технологий сетевой защиты. Первое поколение МЭ появилось в 1983–1985 годах, второе поколение — в 1989–1990 годах. В 1991–1997 годах появились МЭ 3–5 поколений. Затем появились технологии экранирования МЭ и технология экранирования WEB приложений. Наконец, в 2008 году появилось новое поколение межсетевых экранов.

Единой, общепринятой классификации МЭ не существует. Однако в большинстве случаев основой классификации является уровень стека TCP/IP, на котором установлен межсетевой экран. По этому признаку различают:

— управляемые коммутаторы;
— пакетные фильтры;
— шлюзы сеансового уровня;
— посредники прикладного уровня;

— инспекторы состояния.

Управляемые коммутаторы работают на канальном уровне и разделяют трафик между компьютерами в локальной сети. Они не могут быть использованы для обработки трафика из внешних сетей. Поэтому они не являются МЭ в полном смысле этого термина.

Пакетные фильтры работают на сетевом уровне и контролируют прохождение трафика на основе информации в заголовке пакетов. Многие МЭ данного типа могут оперировать и с заголовками протоколов более высокого — транспортного уровня (например, TCP и UDP). Пакетные фильтры остаются самым распространенным типом МЭ. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах.

Шлюз сеансового уровня — это межсетевой экран, исключающий прямое взаимодействие между узлом локальной сети и внешним хостом. Этот МЭ выступает в качестве посредника (proxy), который реагирует на входящие пакеты, проверяет их допустимость на основании текущей фазы соединения. Шлюз гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению.

Посредники прикладного уровня осуществляют посреднические услуги по передаче данных и команд прикладного уровня между двумя компьютерами в сети. Посредничество заключается в том, что связь между двумя компьютерами физически осуществляется через систему-посредника и реально состоит из двух соединений прикладного уровня.

Инспекторы состояния используются для защиты корпоративных сетей. Позволяют контролировать: каждый передаваемый пакет на основе таблицы правил, каждую сессию на основе таблицы состояний, каждое приложение на основе разработанных посредников.

Каждый МЭ настраивается на определенные протоколы обмена информацией. Казалось бы, лучше делать его многопротокольным. Однако, доминирование протоколов TCP/IP столь велико, что поддержка других протоколов часто представляется лишней. Особенно, если учесть, что чем сложнее межсетевой экран, тем он более уязвим.

МЭ можно установить для фильтрации данных на любом из четырех уровнях стека TCP/IP. При этом он умеет работать только с протоколами «своего» уровня. Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях стека TCP/IP.

По состоянию на 2020 год наиболее распространенными являются два типа межсетевых экранов: МЭ (посредники) прикладного уровня и МЭ с пакетной фильтрацией (сетевые или пакетные фильтры).

Формально постановка задачи межсетевого экранирования заключается в следующем. Пусть имеются две компьютерные сети. МЭ — это средство разграничения доступа клиентов из одной сети к серверам другой сети. Для решения этой задачи МЭ контролирует информационные потоки между двумя сетями. Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

Экран можно представить, как последовательность фильтров. Каждый фильтр, проанализировав данные, может не пропустить их и возвратить отправителю, преобразовать данные и передать их следующему фильтру для продолжения анализа, а может и сразу «перебросить» их получателю (рис. 6.3).

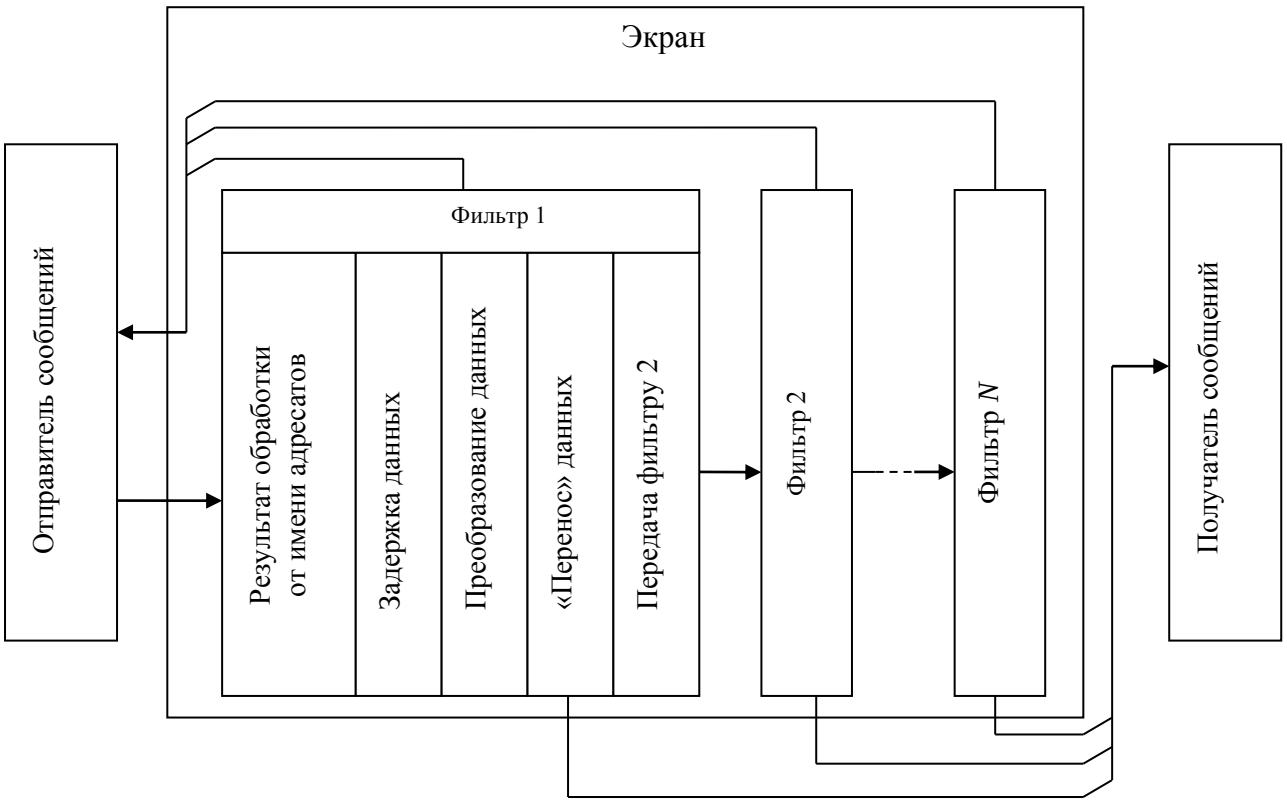

Рис. 6.3. Экран как последовательность фильтров

Кроме того, межсетевой экран протоколирует ход и результаты обмена данными.

МЭ может располагаться как между защищаемой внутренней сетью и внешними сетями, так и между различными сегментами одной

сети. В первом случае говорят о внешнем, а во втором — о внутреннем межсетевом экране.

Для защиты внутренней сети от внешних подключений обычно используется двухкомпонентное экранирование (рис. 6.4).

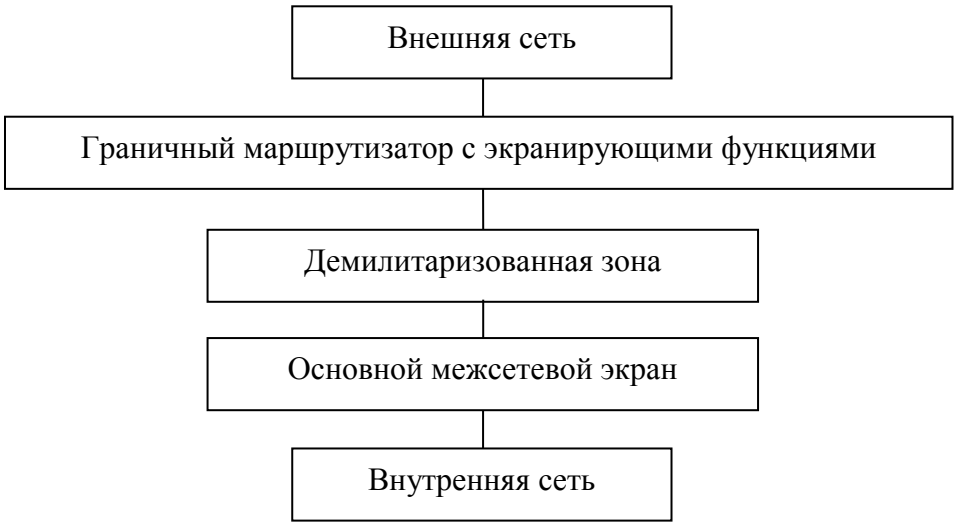

Рис. 6.4. Двухкомпонентное экранирование с демилитаризованной зоной

Двухкомпонентный экран включает:

1. Граничный маршрутизатор с экранирующими функциями. Этот маршрутизатор осуществляет первичную фильтрацию входящего трафика, например, фильтрацию пакетов с определенными IP-адресами, включенными в «черный список». За граничным маршрутизатором располагается так называемая демилитаризованная зона — сеть с умеренным доверием безопасности. В эту зону выносятся внешние информационные сервисы организации — Web, электронная почта, FTP и т. п.

2. Основной межсетевой экран, защищающий внутреннюю часть корпоративной сети.

Корпоративная сеть, как правило, состоит из нескольких территориально разнесенных сегментов. Каждый сегмент подключен к сети «Интернет». Поэтому каждый сегмент защищается своим внешним экраном. Корпоративный внешний МЭ является составным (распределенным), и требует решения задачи согласованного администрирования всех компонентов. Распределенные МЭ управляются централизованно с единой консоли. МЭ экраны, предназначенные для защиты отдельных компьютеров. Главное отличие персонального МЭ от распределенного заключается в том, что они управляются с того компь-

ютера, на котором они установлены. Это привело к тому, что некоторые производители стали выпускать свои решения в двух версиях — персональной (для домашних пользователей) и распределенной (для корпоративных пользователей).

МЭ пропускает или блокирует данные в зависимости от реализованного в нем набора правил фильтрации, являющихся выражением сетевых аспектов политики безопасности. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения: текущее время, количество активных соединений, порт, через который поступил сетевой запрос и т. д.

Существует два способа создания такого набора правил. Первый способ реализует принцип «запрещено все, что *не разрешено* в явном виде». Экран, в котором реализован этот способ, пропускает трафик, соответствующий разрешающим правилам и блокирует все остальное. Второй способ реализует противоположный принцип: «разрешено все, что *не запрещено* в явном виде». Экран, в котором реализован этот способ, пропускает весь трафик, за исключением трафика, соответствующего набору запрещающих правил. Экраны с набором запрещающих правил более безопасны, так как они существенно снижают риск пропуска нежелательного трафика. Существуют также МЭ, в которых реализованы оба способа.

Возможности МЭ непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Чем выше уровень стека протоколов TCP/IP, на котором установлен межсетевой экран, тем более содержательная информация ему доступна, тем тоньше и надежнее он может быть сконфигурирован.

Безопасность МЭ можно повысить с помощью сохранения состояний. МЭ с сохранением состояний запоминает информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток такого экрана заключается в его уязвимости для DoS атак (Denial of Service — отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что оптимально для реальных применений.

Как отмечено выше, в настоящее время наиболее распространенными являются два типа межсетевых экранов: МЭ с пакетной фильтрацией (сетевые или пакетные фильтры) и МЭ (посредники)

прикладного уровня. Ограничимся описанием именно этих двух типов МЭ. Начнем с описания технологии фильтрации пакетов.

Вначале технология фильтрации пакетов применялась только на сетевом уровне. Фильтрации подвергались IP-адреса источника и получателя пакетов. В настоящее время анализ сетевого трафика проводится и на более высоком транспортном уровне.

Каждый IP-пакет проверяется на соответствие правилам, которым должен отвечать заголовок сетевого и транспортного уровней модели TCP/IP, и направление движения пакетов. Фильтры пакетов контролируют:

— физический интерфейс, откуда пришел пакет;

— физический адрес отправителя ($IP_О$) и получателя ($IP_П$) пакета;

— тип протокола транспортного уровня (TCP, UDP, ICMP);

— транспортные порты отправителя и получателя пакета.

Архитектура фильтра пакетов приведена на рис. 6.5.

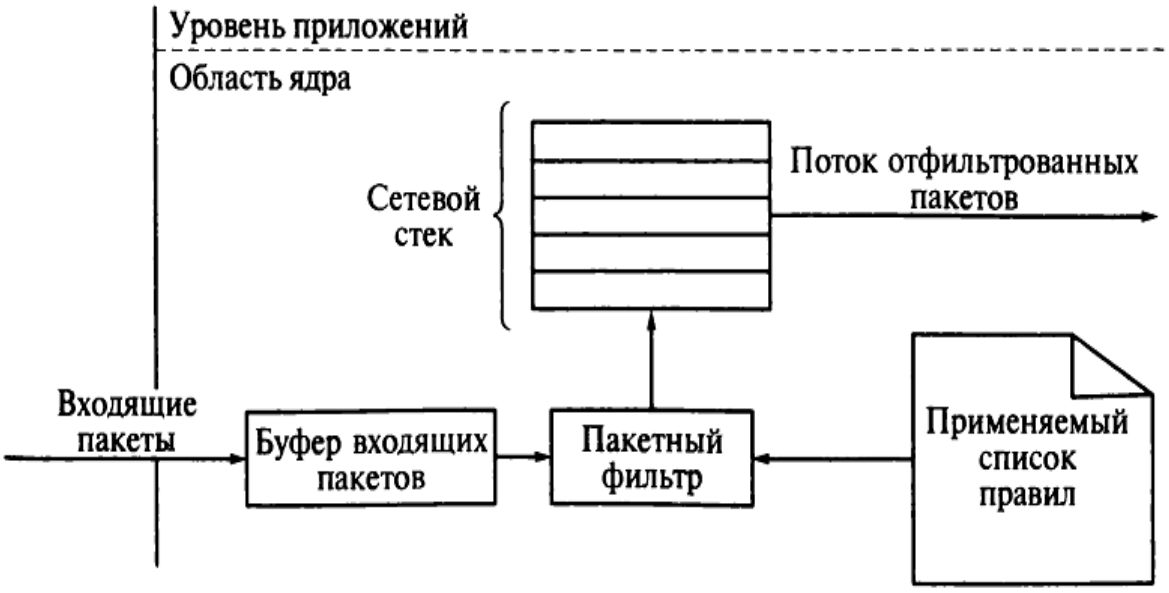

Рис. 6.5. Архитектура фильтра паке-

Трансляция сетевых адресов. МЭ, фильтрующий пакеты, часто переадресует сетевые пакеты так, что его выходной трафик имеет другие адреса. Это называется схемой трансляции адресов (Network Address Translation — NAT). Применение NAT позволяет спрятать топологию и схему адресации доверенной локальной сети и использовать внутри организации меньшее количество IP-адресов. Схема трансляции адресов приведена на рис. 6.6.

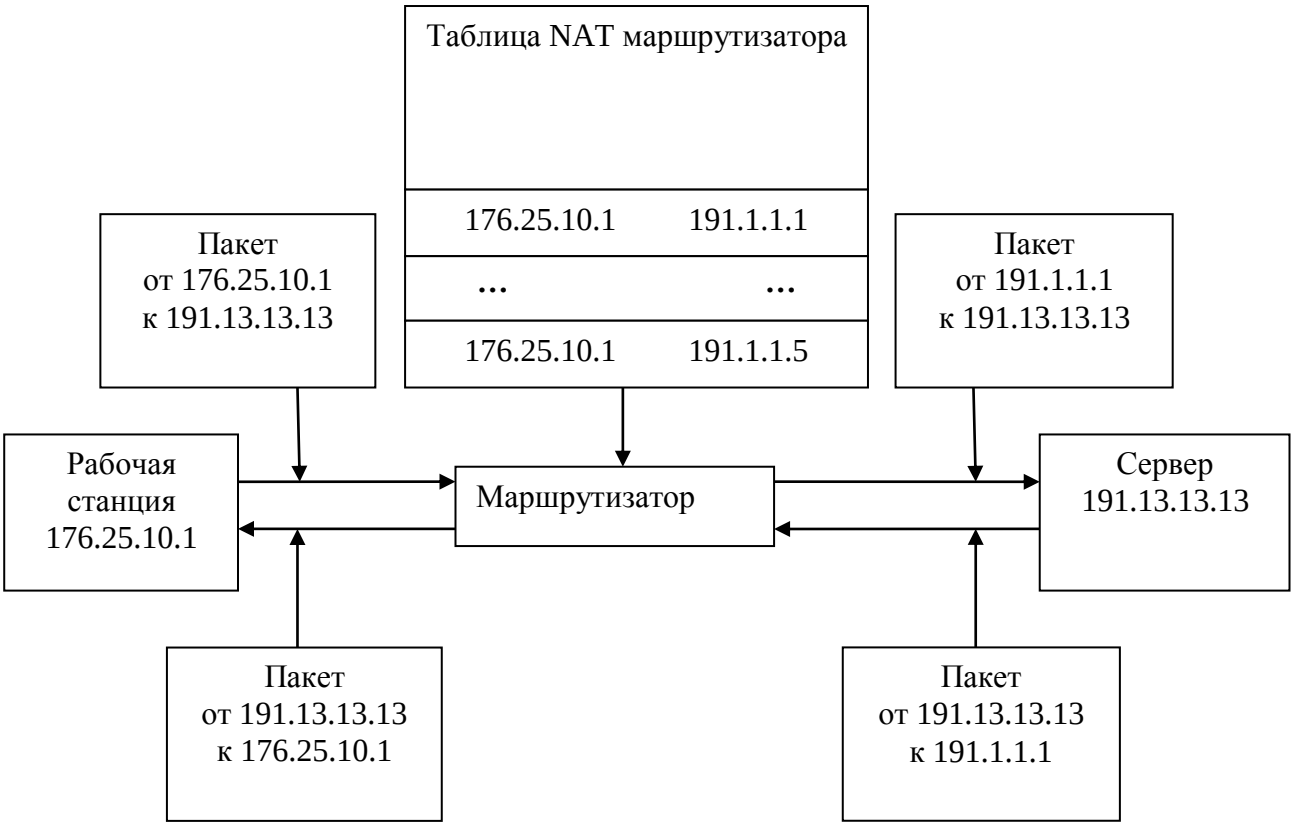

Рис. 6.6. Схема трансляции адресов

Различают статическую и динамическую трансляцию адресов. При статической трансляции используется блок внешних адресов, которые назначаются запросам хостов локальной сети. При динамической трансляции все запросы хостов локальной сети имеют один и тот же адрес. Для динамической трансляции используется форма NAT Overloading, которая ставит в соответствие множеству адресов локальной сети единственный IP-адрес, используя различные номера портов (Port Address Translation — PAT).

Трансляция адресов, кроме скрытия внутренних адресов локальной сети, выполняет еще одну важную функцию защиты: если атакующий направит пакет на хост внутренней сети, то он будет отброшен, так как для него нет соответствующей строки в таблице NAT.

Процесс фильтрации пакетов. Если пакет удовлетворяет правилам, то он, в зависимости от того направлен он к удаленному хосту или от него, перемещается по сетевому стеку для дальнейшей обработки или передачи. Все входные пакеты проверяются на соответствие заданным правилам фильтрации. Правила содержат два списка: список разрешений (permit) и список запрещений (deny). Сетевой пакет проходит проверку на оба списка. При этом:

— если правило разрешает, пакет допускается;

— если правило запрещает, пакет удаляется;

— если ни одно правило не сработало, пакет удаляется.

Для определения уровня защищенности, который МЭ обеспечивают при межсетевом взаимодействии АС, введены *показатели защищенности.*

Конкретные перечни показателей определяют классы защищенности МЭ, в зависимости от уровня контроля межсетевых информационных потоков. При этом дифференциация выбора функций защиты в МЭ определяется АС, для которой обеспечивается защищенность информации от НСД.

Требования к МЭ утверждены приказом ФСТЭК от 09.02.2016 г. № 9 и обязательны для межсетевых экранов, установленных после 1 декабря 2016 года МЭ, установленные до 1 декабря 2016 г., могут эксплуатироваться без проведения повторной сертификации на соответствие этим требованиям.

Данный приказ разработан в дополнение к рассмотренным выше РД Гостехкомиссии, посвященным показателям (критериям) защищенности СВТ и АС.

Документ содержит требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ[1], АС посредством управления межсетевыми потоками информации и реализованных в виде МЭ.

Для дифференциации требований к функциям безопасности МЭ выделяются шесть классов защиты межсетевых экранов. Самый низкий класс — шестой, самый высокий — первый (табл. 6.1).

[1] Под сетями ЭВМ (распределенными АС) понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

Таблица 6.1

Перечень показателей
и соответствующих классов защищенности МЭ

Показатели защищенности МЭ	Классы защищенности МЭ				
	5	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов	+	+	+	+	=
Идентификация и аутентификация	–	–	+	=	+
Регистрация	–	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	–	–	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Обозначения:

«–» — нет требований к данному классу;

«+» — новые или дополнительные требования;

«=» — требования к МЭ предыдущего класса.

Межсетевые экраны, соответствующие 6 классу защиты, применяются в государственных ИС 3 и 4 классов защищенности, в АСУ производственными и технологическими процессами 3 класса защищенности, в ИС персональных данных при необходимости обеспечения 3 и 4 уровней защищенности персональных данных.

Межсетевые экраны, соответствующие 5 классу защиты, применяются в государственных ИС 2 класса защищенности, в АСУ производственными и технологическими процессами 2 класса защищенности, в ИС персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Межсетевые экраны, соответствующие 4 классу защиты, применяются в государственных ИС 1 класса защищенности, в АСУ производственными и технологическими процессами 1 класса защищенности, в ИС персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в ИС общего пользования 2 класса.

Соотношение между классами защищенности МЭ и видами конфиденциальной информации отображено на рис. 6.7.

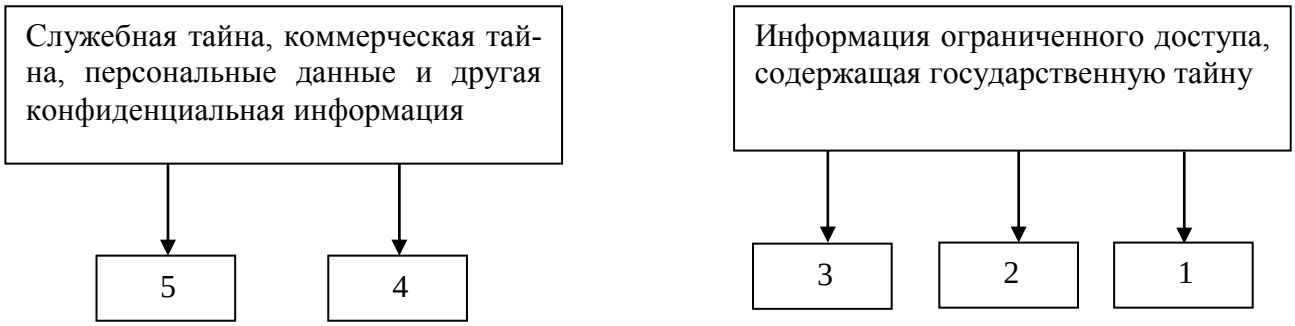

Рис. 6.7. Классификация МЭ по уровню защищенности от НСД

Класс защищенности АС, полученной при включении в ее состав МЭ не должен понижаться. В силу этого условия:

— для АС класса защищенности 3Б, 2Б необходимо применять МЭ не ниже 5 класса.

Для АС класса защищенности 3А, 2А, в зависимости от важности обрабатываемой информации, необходимо применять МЭ следующих классов:

— при обработке информации с грифом «секретно» — не ниже 3 класса;

— при обработке информации с грифом «совершено секретно» — не ниже 2 класса;

— при обработке информации с грифом «особой важности» — не ниже 1 класса.

6.3. Системы обнаружения вторжений

Система обнаружения вторжений (Intrusion Detection System — IDS) — программное или программно-аппаратное средство для выявления атак или иных вредоносных действий, успешно преодолевших МЭ. Типовая система обнаружения вторжений (СОВ) состоит из:

— детекторной (сенсорной) подсистемы, предназначенной для сбора информации о событиях, связанных с безопасностью;

— подсистемы анализа, предназначенной для выявления подозрительных действий на основе данных, получаемых от сенсорной подсистемы;

— хранилища, обеспечивающего накопление первичных событий и результатов анализа;

— консоли управления.

Работа системы обнаружения вторжений основывается на принципе обнаружения любых попыток проникновения внутрь периметра безопасности объекта. Периметр безопасности компьютерной сети представляет собой виртуальный периметр, внутри которого находятся КС. Этот периметр может определяться межсетевыми экранами, точками разделения соединений или настольными компьютерами с модемами. Данный периметр может быть расширен для содержания домашних компьютеров сотрудников, которым разрешено подключаться к сети и работать дома. С появлением в деловом взаимодействии беспроводных сетей периметр защиты организации расширяется до размера беспроводной сети.

Эффективность системы обнаружения вторжений решающим образом зависит от правильности определения этого периметра и перечня событий, которые являются нарушением периметра безопасности. Наиболее сложным вопросом, который необходимо принимать в расчет при развертывании системы обнаружения вторжений, является определение того, какие события являются нарушением периметра безопасности.

СОВ можно классифицировать по многим критериям. Мы остановимся на двух наиболее важных критериях: классификация по методам обнаружения вторжений и классификация по защищаемым объектам (рис. 6.8).

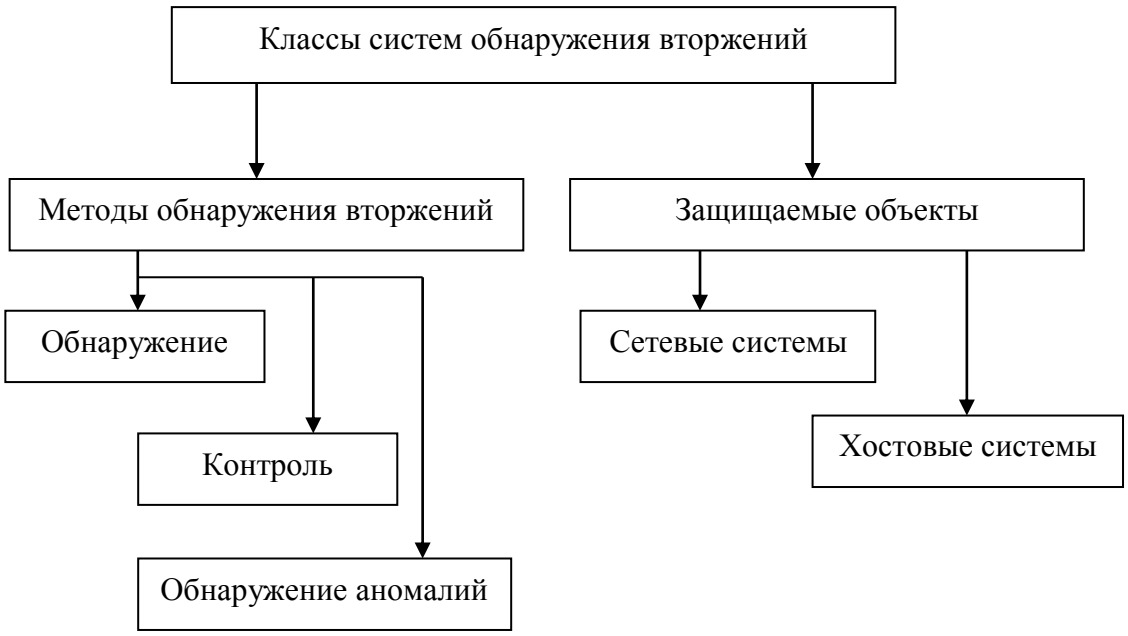

Рис. 6.8. Классификация СОВ

Классификация по методам обнаружения вторжений. Основной метод обнаружения вторжений заключается в том, что трафик сравнивается с базой данных известных шаблонов вредоносной активности, называемых сигнатурами. Этим системы обнаружения вторжений похожи на антивирусные программы. СОВ может обнаружить атаки на основе IP-адресов, номеров портов, информационного наполнения и прочих критериев.

Существует и иной способ обнаружения вторжений на системном уровне, состоящий в контроле целостности ключевых файлов. Контроль целостности чаще всего осуществляется с помощью электронной цифровой подписи.

Наряду с двумя вышеуказанными методами обнаружения вторжений, появляются и новые методы, которые сочетают концепции обнаружения вторжений и межсетевого экранирования или предпринимают дополнительные действия помимо простого обнаружения.

Последние годы на рынке начали появляться сетевые СОВ, базирующиеся на обнаружении аномалий с помощью методов искусственного интеллекта, таких как: Data Mining, экспертные системы, искусственные нейронные сети, иммунные системы и генетические алгоритмы. Эти системы осуществляют поиск аномалий в сетевом трафике для выявления атак. Например, если обнаружен всплеск трафика FTP, интеллектуальная система обнаружения вторжений предупредит об этом, как об обнаруженной атаке. Но такой всплеск может быть вызван и тем, что идет загрузка большого по объему файла. Поэтому сетевые СОВ на основе обнаружения аномалий отличаются большим количеством ложных срабатываний. Вероятно, что с развитием интеллектуальных методов выявления аномалий этот недостаток станет не столь значимым.

Классификация по защищаемым объектам. Существуют два основных типа систем обнаружения вторжений: узловые (HIDS) и сетевые (NIDS). Узловая СОВ располагается на отдельном узле и отслеживает признаки атак на данный узел. Среди узловых СОВ различают: СОВ на уровне ОС (обнаруживают атаки на ОС), СОВ на уровне СУБД (обнаруживают атаки на базы данных), СОВ на уровне приложений (обнаруживают атаки на приложения). Сетевая СОВ находится в отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети. Рассмотрим особенности узловых и сетевых систем обнаружения вторжений.

Узловые СОВ представляют собой систему датчиков (сенсоров), загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные типы событий и предпринимают определенные действия на сервере либо передают уведомления. Датчики отслеживают события, связанные с сервером, на котором они загружены. датчик позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой он установлен.

Различные типы датчиков позволяют выполнять различные типы задач по обнаружению вторжений. Не каждый тип датчиков может использоваться в организации, и даже для различных серверов внутри одной организации могут понадобиться разные датчики. Следует заметить, что узловая СОВ, как правило, стоит дороже, чем сетевая, так как в этом случае каждый сервер должен иметь лицензию на датчик (датчики дешевле для одного сервера, однако общая стоимость датчиков больше по сравнению со стоимостью использования сетевых СОВ).

Кроме того, работа датчиков может занимать от 5 до 15 % общего процессорного времени. Это отрицательно сказывается на производительности системы.

Существует пять основных типов датчиков узловых СОВ:

— анализаторы журналов;

— датчики признаков;

— анализаторы системных вызовов;

— анализаторы поведения приложений;

— контролеры целостности файлов.

Анализатор журнала представляет собой именно то, что отражает название датчика. Процесс выполняется на сервере и отслеживает соответствующие файлы журналов в системе. Если встречается запись журнала, соответствующая некоторому критерию в процессе датчика HIDS, предпринимается установленное действие.

Большая часть анализаторов журналов настроена на отслеживание записей журналов, которые могут означать событие, связанное с безопасностью системы. Администратор системы, как правило, может определить другие записи журнала, представляющие определенный интерес.

Анализаторы журналов по своей природе являются реактивными системами. Иными словами, они реагируют на событие уже после того, как оно произошло. Таким образом, журнал будет содержать сведения о том, что проникновение в систему выполнено. В большин-

стве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

Анализаторы журналов, в частности, хорошо адаптированы для отслеживания активности авторизованных пользователей на внутренних системах. Таким образом, если в организации уделяется внимание контролю за деятельностью системных администраторов или других пользователей системы, можно использовать анализатор журнала для отслеживания активности и перемещения записи об этой активности в область, недосягаемую для администратора или пользователя.

Датчики признаков представляют собой наборы определенных признаков событий безопасности, сопоставляемых с входящим трафиком или записями журнала. Различие между датчиками признаков и анализаторами журналов заключается в возможности анализа входящего трафика.

Системы, основанные на сопоставлении признаков, обеспечивают возможность отслеживания атак во время их выполнения в системе, поэтому они могут выдавать дополнительные уведомления о проведении злоумышленных действий. Тем не менее, атака будет успешно или безуспешно завершена перед вступлением в действие датчика HIDS, поэтому датчики этого типа считаются реактивными. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри ИС.

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и ОС для идентификации событий, связанных с безопасностью. Датчики HIDS данного типа размещают программную спайку между ОС и приложениями. Когда приложению требуется выполнить действие, его вызов ОС анализируется и сопоставляется с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора IDS.

Анализаторы системных вызовов отличаются от анализаторов журналов и датчиков признаков HIDS тем, что они могут предотвращать действия. Если приложение генерирует вызов, соответствующий, например, признаку атаки на переполнение буфера, датчик позволяет предотвратить этот вызов и сохранить систему в безопасности.

Необходимо обеспечивать правильную конфигурацию датчиков этого типа, так как их некорректная настройка может вызывать ошибки в приложениях либо отказы в их работе. Такие датчики, как правило, обеспечивают возможность функционирования в тестовом

режиме. Это означает, что датчик отслеживает события, но не предпринимает никаких блокирующих действий; этот режим можно использовать для тестирования конфигурации без блокировки работы легитимно используемых приложений.

Анализаторы поведения приложений аналогичны анализаторам системных вызовов в том, что они применяются в виде программной спайки между приложениями и ОС. В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять данное действие, вместо определения соответствия вызова признакам атак. Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места или открыть новые сетевые соединения, датчик обнаружит несоответствующее норме поведение сервера и заблокирует действие.

При конфигурировании таких датчиков необходимо создавать список действий, разрешенных для выполнения каждым приложением. Поставщики датчиков данного типа предоставляют шаблоны для наиболее широко используемых приложений. Любые «доморощенные» приложения должны анализироваться на предмет того, какие действия им разрешается выполнять, и выполнение этой задачи должно быть программным образом реализовано в датчике.

Контролеры целостности файлов отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла. Конечная цифровая подпись файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть атрибуты файла, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

При изначальной конфигурации датчика каждый файл, подлежащий мониторингу, подвергается обработке алгоритмом для создания начальной подписи. Полученное число сохраняется в безопасном месте. Периодически для каждого файла эта подпись пересчитывается и сопоставляется с оригиналом. Если подписи совпадают, это означает, что файл не был изменен. Если соответствия нет, значит, в файл были внесены изменения.

Работа датчика данного типа сильно зависит от качества контроля над конфигурацией. Если организация не осуществляет управление датчиком на должном уровне, то датчик, как правило, обнаруживает все типы изменений, вносимых в файл, которые, на самом деле, могут быть легитимными, но неизвестными датчику.

Контролер целостности файлов не осуществляет идентификацию атаки, а детализирует результаты проведенной атаки. Таким образом, в случае атаки на веб-сервер сама атака останется незамеченной, но будет обнаружено повреждение или изменение домашней страницы веб-сайта. То же самое относится и к другим типам проникновений в систему, так как в процессе многих из них осуществляется изменение системных файлов.

Одним из главных преимуществ сетевых СОВ является то, что они, в отличие от узловых СОВ, способны выявлять внутренние атаки и подозрительную активность пользователей. В силу этих причин сетевые СОВ часто используются в DLP-системах. Сетевая СОВ представляет собой программный процесс, работающий на специально выделенной системе. Она переключает сетевую карту в системе в неразборчивый режим работы, при котором сетевой адаптер пропускает весь сетевой трафик (а не только трафик, направленный на данную систему) в программное обеспечение СОВ. После этого происходит анализ трафика с использованием набора правил и признаков атак для определения того, представляет ли этот трафик какой-либо интерес. Если это так, то генерируется соответствующее событие.

Чаще всего при применении сетевых СОВ используются две сетевые карты. Одна карта используется для мониторинга сети. Эта карта работает в «скрытом» режиме, поэтому она не имеет IP-адреса и, следовательно, не отвечает на входящие соединения.

Вторая сетевая карта используется для соединения с системой управления IDS и для отправки сигналов тревоги. Эта карта присоединяется ко внутренней сети, невидимой для той сети, в отношении которой производится мониторинг.

Среди преимуществ использования сетевых СОВ можно выделить следующие моменты:

— сетевой СОВ можно полностью скрыть в сети так, что злоумышленник не будет знать о том, что за ним ведется наблюдение;

— одна сетевая СОВ может использоваться для мониторинга трафика с большим числом потенциальных систем-целей;

— сетевая СОВ может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков данной системы необходимо отметить:

— сетевая СОВ может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам;

— сетевая СОВ может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов;

— сетевая СОВ не может определить, была ли атака успешной;

— сетевая СОВ не может просматривать зашифрованный трафик.

Система обнаружения вторжений обеспечивает дополнительный уровень защиты КС и используется для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность КС. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к файлам, действия вредоносного ПО (вирусов, троянов, червей).

В 2012 году дополнительно к межсетевым экранам Информационным письмом ФСТЭК от 01.03.2012 г. № 240 «Об утверждении требований к системам обнаружения вторжений» установлены требования к системам обнаружения вторжений. Всего установлено шесть классов. На рис. 6.9 приведено соответствие классов защищенности СОВ уровням конфиденциальности.

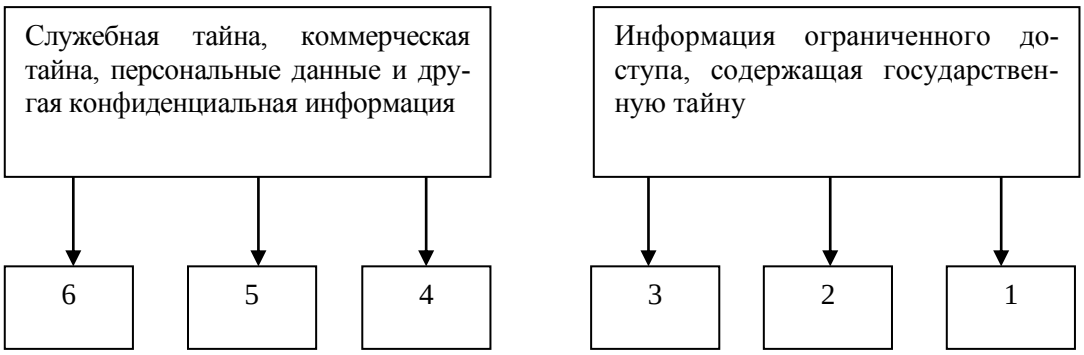

Рис. 6.9. Классификация СОВ по уровню защищенности от НСД

Спецификация профилей защиты систем обнаружения вторжений для каждого ее типа и класса приведена в таблице 6.2. Таким образом, с 15 марта 2012 года сертификация средств защиты информации, реализующих функции обнаружения вторжений, в системе сертификации ФСТЭК проводится на соответствие Требованиям к системам

обнаружения вторжений, утвержденным приказом ФСТЭК от 06.12.2011 г. № 638.

Таблица 6.2

Классификация профилей защиты систем обнаружения вторжений

Тип СОВ	Класс защиты					
	6	**5**	**4**	**3**	**2**	**1**
СОВ уровня сети	ИТ.СОВ. С6.ПЗ	ИТ.СОВ. С5.ПЗ	ИТ.СОВ. С4.ПЗ	ИТ.СОВ. С3.ПЗ	ИТ.СОВ. С2.ПЗ	ИТ.СОВ. С1.ПЗ
СОВ уровня узла	ИТ.СОВ. У6.ПЗ	ИТ.СОВ. У5.ПЗ	ИТ.СОВ. У4.ПЗ	ИТ.СОВ. У3.ПЗ	ИТ.СОВ. У2.ПЗ	ИТ.СОВ. У1.ПЗ

Примечание. Здесь в клетках на пересечении строки и столбца указаны: ИТ — информационная технология, СОВ — система обнаружения вторжений, СХ — класс Х сети, УХ — класс Х узла, ПЗ — профиль защиты.

Обеспечение федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций требованиями к СОВ, утвержденными приказом ФСТЭК от 06.12.2011 г. № 638, а также методическими документами ФСТЭК, содержащими профили защиты систем обнаружения вторжений 3, 2 и 1 классов защиты, производится в соответствии с Временным порядком обеспечения органов государственной власти Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК (www.fstec.ru).

Методические документы ФСТЭК, содержащие профили защиты СОВ 6, 5 и 4 классов защиты, размещены на официальном сайте ФСТЭК www.fstec.ru в разделе «Информационно-справочная система по документам в области технической защиты информации. Специальные нормативные документы».

6.4. Виртуальные частные сети

В современном мире весьма востребованной является услуга по обмену информацией между территориально удаленными абонентами. Если эта информация является конфиденциальной, то для обмена часто используются виртуальные частные сети (Virtual Private Network — VPN). Начальные сведения о виртуальных частных сетях приведены ранее. Здесь мы рассмотрим эти сети более подробно.

Основы организации VPN рассмотрим на следующем примере. Пусть у компании есть две локальных сети: сеть головного офиса (LAN1) и сеть филиала (LAN2). Обе сети объединены через Интернет (рис. 6.10). Сотрудники головного офиса и филиала по работе должны обмениваться между собой конфиденциальной информацией.

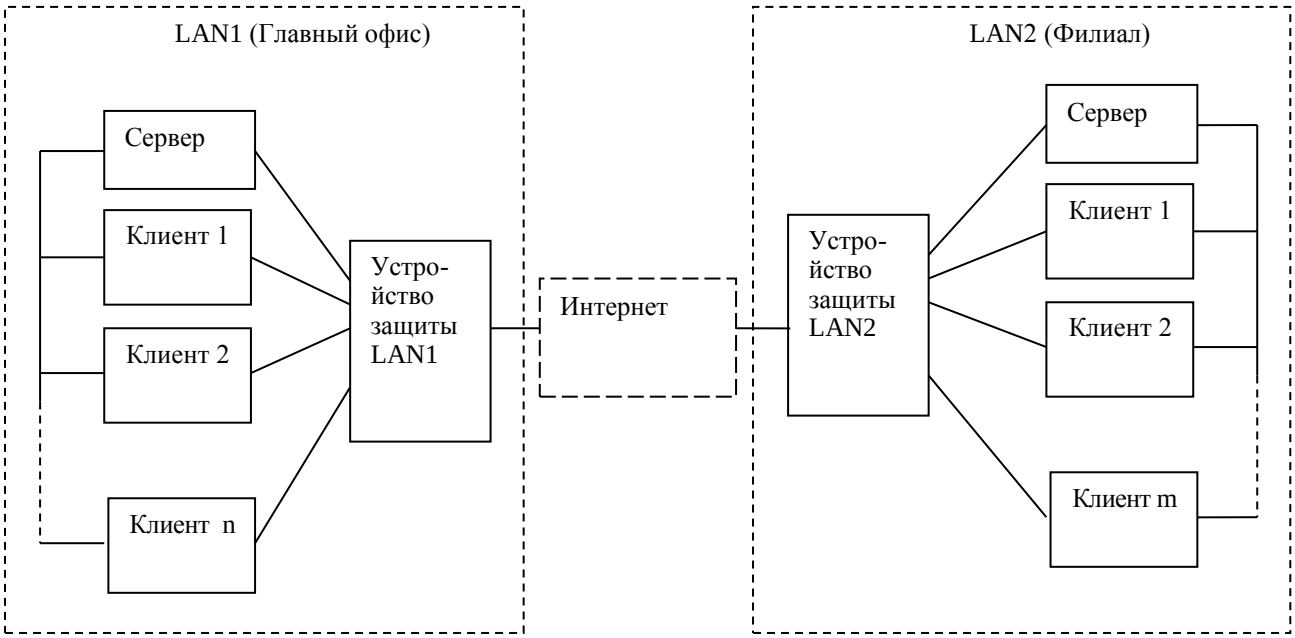

Рис. 6.10. Организация VPN

Обмен возможен между любыми компьютерами этих сетей. При этом:

— обмен между компьютерами, входящими в состав одной сети, идет напрямую;

— обмен между компьютерами головного офиса и филиала осуществляется через неких посредников, установленных на входе каждой сети. Эти посредники — пограничные VPN узлы с элементами межсетевого экранирования, реализуют функции защиты.

Задача пограничных узлов заключается в такой обработке трафика между сетями, чтобы злоумышленник не мог совершить с передаваемой информацией какие-либо действия, нарушающие ее конфиденциальность и целостность. То есть передаваемая информация, включая адреса отправителя и получателя должна быть, зашифрована и подписана электронной цифровой подписью. В этом случае злоумышленник видит в сети лишь зашифрованный обмен информацией между устройствами защиты.

Из выше изложенного следует, что виртуальная частная сеть ориентирована на решение следующих задач.

1. Обеспечение конфиденциальности, целостности и подлинности передаваемой по сетям информации. Данная задача решается применением криптографии.

2. Защита внутренних сегментов сети от НСД извне. Решение данной задачи возможно благодаря встроенным в пограничные узлы VPN-системы элементам межсетевого экранирования, а также криптографическим механизмам, запрещающим незашифрованный сетевой трафик.

3. Обеспечение идентификации и аутентификации пользователей. Данная задача возникает вследствие того, что в сети должны взаимодействовать лишь доверенные узлы, доверие к которым возможно после прохождения процедур идентификации и аутентификации.

Задачу обеспечения доступности информации технология VPN не решает.

Важнейшее достоинство VPN заключается в экономии финансовых ресурсов организации, поскольку здесь для обеспечения конфиденциальности связи с филиалами применяются не арендуемые дорогие выделенные защищенные каналы связи, а Интернет или иные сети общего пользования.

Для успешного решения этих задач программно-аппаратные комплексы, реализующие VPN, должны удовлетворять следующим требованиям:

— масштабируемость — возможность подключать новые локальные сети и компьютеры без необходимости изменения структуры, имеющейся VPN;

— интегрируемость — возможность внедрения VPN-системы в имеющуюся технологию обмена информацией;

— легальность и стойкость используемых криптографических алгоритмов — система должна иметь соответствующий сертификат, позволяющий использовать ее на территории Российской Федерации;

— высокая пропускная способность сети — система не должна существенно увеличивать объем передаваемого трафика и уменьшать скорость его передачи;

— унифицируемость — возможность устанавливать защищенные соединения с коллегами по бизнесу, у которых уже установлена иная VPN-система;

— общая совокупная стоимость — затраты на приобретение, развертывание и обслуживание системы не должны превосходить стои-

мость самой информации, особенно если речь идет о защите коммерческой тайны.

Важнейшим инструментом VPN является туннелирование. Туннелирование предполагает, что в пакетах, которые идут по открытой сети между территориально разнесенными абонентами, в качестве адресов фигурируют только адреса пограничных узлов VPN, стоящих на входе в туннель и выходе из туннеля. Кроме того, туннелирование предполагает, что внутри локальных сетей трафик передается в открытом виде, а его защита осуществляется только тогда, когда он попадает в «туннель».

Итак, пусть у отправителя сообщения имеется пакет, содержащий данные и IP-заголовок, которые подлежат защите (рис. 6.11).

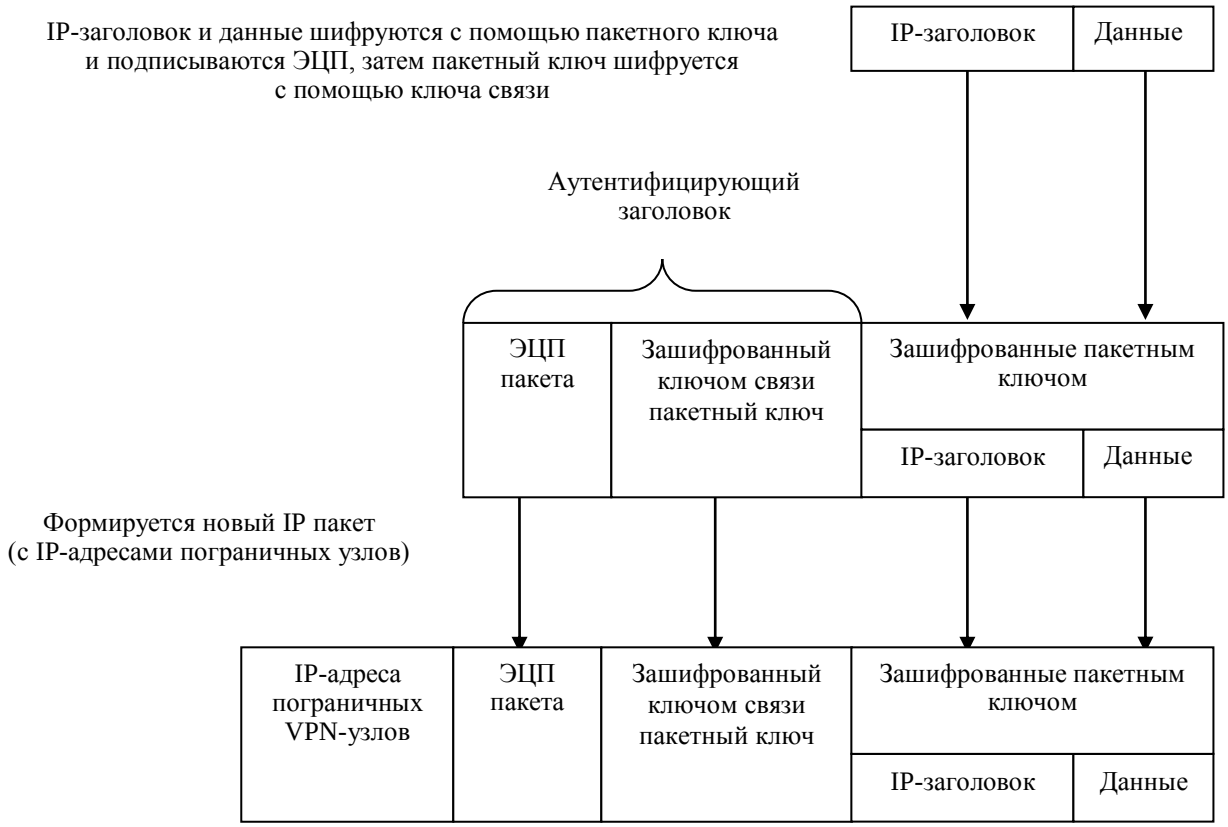

Рис. 6.11. Схема преобразования пакета, отправляемого через туннель

Для защиты применим криптографию и зашифруем и данные, и заголовок вместе. Так как необходимо обеспечить высокую скорость обработки пакета, то для его шифрования/расшифрования будем использовать симметричную криптографическую систему. Но тогда и мы (отправитель сообщения), и его получатель должны знать общий секретный ключ. Для остальных абонентов этот ключ должен держаться в секрете.

Этот ключ будет генерироваться отправителем сообщения случайным образом, например, в зависимости от характера движения мышки компьютера. Если ключ генерируется при передаче каждого пакета, то это пакетный ключ, если он является одинаковым для всех пакетов сеанса связи — то это сеансовый ключ. В дальнейшем будем говорить о пакетном ключе, подразумевая, что схемы использования и преобразования пакетного и сеансового ключей в принципе совпадают.

Зашифруем пакетный ключ, чтобы затем передать его получателю сообщения. Для шифрования воспользуемся выбранной нами асимметрической криптосистемой. Учитывая, что пакетный ключ имеет в длину не более нескольких сотен бит, его шифрование с помощью асимметрической криптосистемы не займет много времени. Шифровать пакетный ключ будем с помощью открытого ключа получателя сообщения, взятого нами из доверительного центра. Для шифрования пакетного ключа может быть применен и симметричный алгоритм. Однако тогда вновь возникает проблема распространения ключей. Ключ алгоритма шифрования пакетного ключа назовем ключом связи.

После этого, прикрепим зашифрованный пакетный ключ к зашифрованным данным и IP-адресам. Кроме того, для обеспечения целостности пакетов сгенерируем электронно-цифровую подпись (ЭЦП) пакета и прикрепим ее к формируемому пакету. Совокупность ЭЦП и зашифрованного пакетного ключа называют аутентифицирующим заголовком.

Для того чтобы отправить сгенерированный пакет, необходимо добавить к нему IP-адреса источника и приемника. В случае туннеля этими адресами будут адреса пограничных VPN-узлов. Если защищается трафик между двумя узлами без применения туннеля, то эти адреса совпадут с адресами в исходном пакете.

Таким образом, исходный пакет защищен. Осталось выяснить, что в VPN понимается под шифруемыми данными: только лишь данные прикладного уровня или также данные, относящиеся к транспортному или сетевому уровню, которые, как известно, включают и заголовки данных более высокого уровня.

Сети VPN строятся с использованием протоколов туннелирования данных, которые предусматривают шифрование данных и их сквозную передачу между пользователями. Эти протоколы распределены по уровням модели TCP/IP (табл. 6.3).

Таблица 6.3

Расположение протоколов VPN по уровням модели

Уровень TCP/IP	Основные протоколы
Прикладной (application)	PGP, S/MIME, SSH, Kerberos, RADIUS
Транспортный (Transport)	SSL,TSL,SOCS v5
Сетевой (internetworking)	IPSec (AH, ESP)
Канальный (datalink)	L2TP, PPTP, L2A, CHAP, PAP, MS-CHAP

Для каждого уровня возможность шифрования передаваемой информации различна. Так, на прикладном уровне можно скрыть данные. Однако факт передачи данных определенного типа скрыть невозможно. На транспортном уровне вместе с данными может быть скрыт и тип передаваемых данных, однако IP-адреса получателя и приемника остаются открытыми. На сетевом уровне уже появляется возможность скрыть и IP-адреса. Эта же возможность имеется и на канальном уровне. Чем ниже уровень, тем легче сделать систему, функционирование которой будет незаметно для приложений высокого уровня, и тем большую часть передаваемой информации можно скрыть.

Протоколы канального уровня. На канальном уровне есть два протокола для реализации VPN: протокол туннелирования типа точка-точка (Point to Point Tunneling Protokol — PPTP) и протокол туннелирования второго уровня (Layer Two Tunneling Protocol — L2TP).

Протокол PPTP есть развитие протокола PPP (Point to Point Protocol). PPP — протокол канального уровня, разработан для инкапсуляции данных и их доставки по соединениям типа точка-точка[1]. В основе протокола PPTP лежит следующий алгоритм: сначала производится инкапсуляция данных с помощью протокола PPP, затем протокол PPTP выполняет шифрование данных и инкапсуляцию. PPTP инкапсулирует PPP-кадр в пакет Generic Routing Encapsulation (протокол GRE). Схема инкапсуляции приведена на рис. 6.12.

IP-заголовок	GRE-заголовок	PPP-заголовок	IP-заголовок	TCP, UDP	Данные

Рис. 6.12. Инкапсуляция в протоколе PPTP

[1] Простейший вид компьютерной сети, при котором два компьютера соединяются напрямую через коммуникационное оборудование. Соединить таким образом можно только два компьютера.

К исходному отправляемому IP-пакету, состоящему из трех правых полей (рис. 6.12) последовательно добавляются PPP, GRE и IP-заголовки[1]. Получается новый IP-пакет. В этом новом пакете в качестве адресов указываются уже не адреса компьютеров, отправляющих данные, а адреса туннелирующих узлов.

В протоколе PPTP для аутентификации предусматриваются различные протоколы аутентификации: Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MSCHAP), Challenge Handshake Authentication Protocol (CHAP), Shiva Password Authentication Protocol (SPAP), Password Authentication Protocol (PAP). Наиболее стойким является протокол MSCHAP, требующий взаимную аутентификацию клиента и сервера. В протоколе MSCHAP могут быть использованы три различных варианта передачи пароля: клиент передает серверу пароль в открытом текстовом виде; клиент передает серверу хэш пароля; аутентификация сервера и клиента осуществляется с использованием вызова и ответа.

Протокол L2TP является гибридом двух протоколов туннелирования: протокола PPTP и протокола пересылки второго уровня Layer Two Forwarding (L2F). Этот протокол заменил протокол PPTP в ОС Windows, начиная с Windows 2000.

Этот протокол, как и PPTP, при аутентификации абонента использует возможности протокола PPP. Аналогично протоколу PPTP протокол L2TP использует для канала связи сообщения управления и сообщения туннеля для передачи данных. Первый байт заголовка протокола PPTP служит для опознания типов сообщений: «1» — для сообщений управления, «0» — для сообщений данных. Сообщениям управления придается более высокий приоритет.

Подключение канала управления устанавливается для туннеля, который затем сопровождается инициированием сеанса протокола L2PT. По завершении инициирования обоих подключений информация в виде кадров протокола PPP начинает передаваться по туннелю.

Протоколы сетевого уровня. На сетевом уровне в основном используется протокол IPSec (Internet Protocol Security), реализующий криптографическую защиту данных, фильтрацию входя-

[1] Напомним, что: PPP — двухточечный протокол канального уровня, GRE (Generic Routing Encapsulation) — протокол туннелирования сетевых пакетов фирмы Cisco, IP (Internet protocol) — маршрутизируемый протокол сетевого уровня.

щих/исходящих пакетов и аутентификацию абонентов. Стандарт IPSec выбран международным сообществом, группой IETF[1].

Способ взаимодействия лиц, использующих технологию IPSec, принято определять термином «защищенная ассоциация» — Security Association (SA). Защищенная ассоциация функционирует на основе соглашения, заключенного сторонами, которые пользуются средствами IPSec для защиты передаваемой друг другу информации. Это соглашение регулирует несколько параметров: IP-адреса отправителя и получателя, криптографический алгоритм, порядок обмена ключами, размеры ключей, срок службы ключей, алгоритм аутентификации.

IPSec — это согласованный набор открытых стандартов, имеющий ядро, которое может быть достаточно просто дополнено новыми функциями и протоколами. Ядро IPSec составляют три протокола:

1) AH или Authentication Header — заголовок аутентификации — гарантирует целостность и аутентичность данных. Основное назначение протокола AH: он позволяет приемной стороне убедиться, что:

— пакет был отправлен стороной, с которой установлена безопасная ассоциация;

— содержимое пакета не было искажено в процессе его передачи по сети; пакет не является дубликатом уже полученного пакета.

Две первые функции обязательны для протокола AH, а последняя выбирается при установлении ассоциации по желанию. Для выполнения этих функций протокол AH использует специальный заголовок.

Его структура рассматривается по следующей схеме:

1. В поле следующего заголовка (next header) указывается код протокола более высокого уровня, т. е. протокола, сообщение которого размещено в поле данных IP-пакета.

2. В поле длины полезной нагрузки (payload length) содержится длина заголовка AH.

3. Индекс параметров безопасности (Security Parameters Index, SPI) используется для связи пакета с предусмотренной для него безопасной ассоциацией.

4. Поле порядкового номера (Sequence Number, SN) указывает на порядковый номер пакета и применяется для защиты от его ложного воспроизведения (когда третья сторона пытается повторно использовать перехваченные защищенные пакеты, отправленные реально аутентифицированным отправителем).

[1] Internet Engineering Task Force — Инженерный совет Интернета.

5. Поле данных аутентификации (authentication data), которое содержит так называемое значение проверки целостности (Integrity Check Value, ICV), используется для аутентификации и проверки целостности пакета. Это значение, называемое также дайджестом, вычисляется с помощью одной из двух обязательно поддерживаемых протоколом AH вычислительно необратимых функций MD5 или SAH-1, но может использоваться и любая другая функция.

2) *ESP или Encapsulating Security Payload* — инкапсуляция зашифрованных данных — шифрует передаваемые данные, обеспечивая конфиденциальность, может также поддерживать аутентификацию и целостность данных. Протокол ESP решает две группы задач. К первой группе относятся задачи, аналогичные задачам протокола AH, — это обеспечение аутентификации и целостности данных на основе дайджеста. Ко второй — защита передаваемых данных путем их шифрования от несанкционированного просмотра.

Заголовок делится на две части, разделяемые полем данных. Первая часть, называемая собственно заголовком ESP, образуется двумя полями (SPI и SN), назначение которых аналогично одноименным полям протокола AH, и размещается перед полем данных. Остальные служебные поля протокола ESP, называемые концевиком ESP, расположены в конце пакета.

Два поля концевика — следующего заголовка и данных аутентификации – аналогичны полям заголовка AH. Поле данных аутентификации отсутствует, если при установлении безопасной ассоциации принято решение не использовать возможностей протокола ESP по обеспечению целостности. Помимо этих полей концевик содержит два дополнительных поля — заполнителя и длины заполнителя.

Протоколы AH и ESP могут защищать данные в двух режимах:

— в транспортном — передача ведется с оригинальными IP-заголовками;

— в туннельном — исходный пакет помещается в новый IP-пакет, и передача ведется с новыми заголовками.

Применение того или иного режима зависит от требований, предъявляемых к защите данных, а также от роли, которую играет в сети узел, завершающий защищенный канал. Так, узел может быть хостом (конечным узлом) или шлюзом (промежуточным узлом).

Соответственно, имеются три схемы применения протокола IPSec:

1. Хост-хост;
2. Шлюз-шлюз;

3. Хост-шлюз.

Возможности протоколов AH и ESP частично перекрываются: протокол AH отвечает только за обеспечение целостности и аутентификации данных, протокол ESP может шифровать данные и, кроме того, выполнять функции протокола AH (в урезанном виде). ESP может поддерживать функции шифрования и аутентификации / целостности в любых комбинациях, т. е. либо всю группу функций, либо только аутентификацию / целостность, либо только шифрование.

3) *IKE или Internet Key Exchange* — обмен ключами Интернета — решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

Протоколы транспортного уровня. На транспортном уровне используется протокол SSL/TLS или Secure Socket Layer/Transport Layer Security, реализующий шифрование и аутентификацию между транспортными уровнями приемника и передатчика. SSL/TLS может применяться для защиты трафика TCP, не может применяться для защиты трафика UDP. Для функционирования VPN на основе SSL/TLS нет необходимости в реализации специального программного обеспечения так как каждый браузер и почтовый клиент оснащены этими протоколами. В силу того, что SSL/TLS реализуется на транспортном уровне, защищенное соединение устанавливается «из-конца-вконец».

TLS-протокол основан на Netscape SSL-протоколе версии 3.0 и состоит из двух частей — TLS Record Protocol и TLS Handshake Protocol. Различие между SSL 3.0 и TLS 1.0 незначительные.

SSL/TLS включает в себя три основных фазы:

1. Диалог между сторонами, целью которого является выбор алгоритма шифрования;
2. Обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификатов;
3. Передача данных, шифруемых при помощи симметричных алгоритмов шифрования.

Протоколы прикладного уровня. На прикладном уровне для защиты электронной почты можно применять протокол S/MIME [1] (Secure Multipurpose Internet Mail Extension) либо систему PGP. Для

[1] S/MIME — Secure/Multipurpose Internet Mail Extension — многоцелевые расширения электронной почты — стандарт для шифрования и подписи в электронной почте с помощью асимметричной криптосистемы. Поддерживает большую часть почтовых программ.

защиты обмена по протоколу HTTP применяется протокол HTTPS[1] На данном уровне шифруется текст передаваемого почтового сообщения или содержимое HTML-док.

Контрольные вопросы:

1. Перечислите основные принципы адресации и передачи информации в сети «Интернет».
2. Что представляют собой МЭ?
3. Что включает в себя СОВ?
4. Как формируется виртуальная частная сеть?

[1] Безопасный протокол передачи гипертекста, поддерживающий шифрование посредством криптографических протоколов SSL и TLS. Является расширением протокола HTTP с надстройкой шифрования.

Лекция 7. Защита от вредоносного программного обеспечения

Вопросы лекции:

7.1. Разрушающие программные воздействия и защита от них.

7.2. Принципы и методы защиты от разрушающих программных воздействий.

7.1. Разрушающие программные воздействия и защита от них

В данном вопросе рассмотрены основные виды разрушающих программных воздействий (РПВ) (за исключением программных вирусов, которые будут рассмотрены позже), средства и методы защиты от них. Отличительной особенностью РПВ является лавинообразное увеличение их конкретных реализаций. Освоить все их невозможно. Однако знакомство с принципами построения и применения РПВ, принципов борьбы с ними поможет разобраться с практическими вопросами их выявления и ликвидации. Более детальную информацию можно найти в прилагаемой литературе, а также в сети «Интернет».

Сущность разрушающих программных воздействий

Как отмечено ранее, современные концепции построения защищенных КС предполагают использование в едином комплексе программных средств различного назначения. Важным моментом при работе этих средств является необходимость защиты программ и данных от НСД — от потенциального вмешательства иных, присутствующих в ПК прикладных и системных программ в процесс обработки информации.

Под НСД понимаются действия по использованию, изменению и уничтожению исполняемых модулей и массивов данных, производимых субъектом, не имеющим право на такие действия (злоумышленником). Это возможно, если:

— система имеет механизм различения злоумышленников и легальных пользователей;

— в системе есть пассивная и активная компоненты (исполняемые модули и данные), использование которых злоумышленником нежелательно;

— в системе есть механизм установления соответствия субъекта и информации, к которой он имеет доступ.

Считая, что злоумышленник в совершенстве владеет всем программным и аппаратным обеспечением, можно предполагать, что НСД может быть вызван следующими причинами:

— отключением или видоизменением защитных механизмов злоумышленником (доступ «мимо» средств контроля и пр.);

— входом злоумышленника в систему под именем и с полномочиями легального пользователя.

В первом случае злоумышленник должен изменить защитные механизмы системы, *во втором* — узнать идентификатор и пароль реального пользователя. В обоих случаях НСД можно представить моделью, в которой проникновение и работа внутри КС осуществляется на основе некоторого воздействия, произведенного предварительно внедренными в систему программами.

Программы, способные помочь злоумышленнику осуществить любой из этих двух случаев, называются программами с потенциально опасными воздействиями (Badware — «плохие» программы). Эти программы включают набор инструкций для какого-либо процессора, способных выполнить нижеперечисленные функции:

1. Скрыть признаки своего присутствия в ПК;
2. Реализовать самодублирование, ассоциирование себя с другими программами и/или перенос своих фрагментов в иные области ОП или внешней памяти;
3. Разрушить (исказить) код программ в оперативной памяти КС;
4. Перенести (сохранить) фрагменты информации из оперативной памяти в некоторые другие области ОП или внешней памяти прямого доступа;
5. Имеет потенциальную возможность исказить, заблокировать и/или подменить выводимый на внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ или уже находящийся в ВП, либо изменить его параметры.

Программы с потенциально опасными последствиями по функциональному признаку можно поделить на три класса (рис. 7.1):

1. Классические деструктивные программы — вирусы. Особенность данного класса заключается в ненаправленности их воздействия на конкретные данные, а также в том, что во главу угла ставится самодублирование вируса.

2. Программы типа «программный червь» или «троянский конь» и фрагменты программ типа «логический блок» Здесь имеет место обратная ситуация — самодублирование не всегда присуще,

но они обладают возможностью перехвата конфиденциальной информации, или извлечения информации из систем безопасности или разграничения доступа.

3. Программные закладки (руткиты — root — корень, kit — комплект), которые представляют собой группу небольших программ, позволяющих злоумышленнику получить доступ с правами root или админа — наиболее привилегированного пользователя. Это набор программ, обеспечивающих постоянное, устойчивое и неопределяемое присутствие на ПК. Наибольшая часть технологии и приемов, используемых руткитом, служит для скрытия кода и данных в системе. Руткиты позволяют получить полный контроль над ПК. При этом атакующий должен быть уверен, что только интересующие его компьютеры будут подвержены атаке. Иначе могут быть перекрыты границы операции. Руткиты требуют четкого управления, что делает использование вирусов в них невозможным.

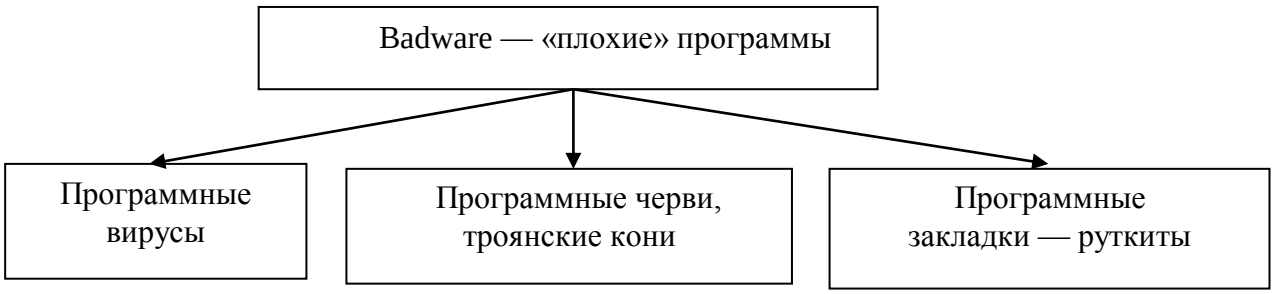

Рис. 7.1. Классификация вредоносных программ

Для всех этих трех классов программ обычно используют термин разрушающее программное воздействие (РПВ). РПВ это воздействие, оказываемое на КС разрушающими программными средствами (РПС) — программными средствами с потенциально опасными последствиями, которые реализуют хоть один из пяти перечисленных выше пунктов.

Модели взаимодействия прикладных программ и программы злоумышленника

Рассмотрим модели программных закладок, исходящие из образа мышления и возможностей злоумышленника — из модели злоумышленника (рис. 7.2).

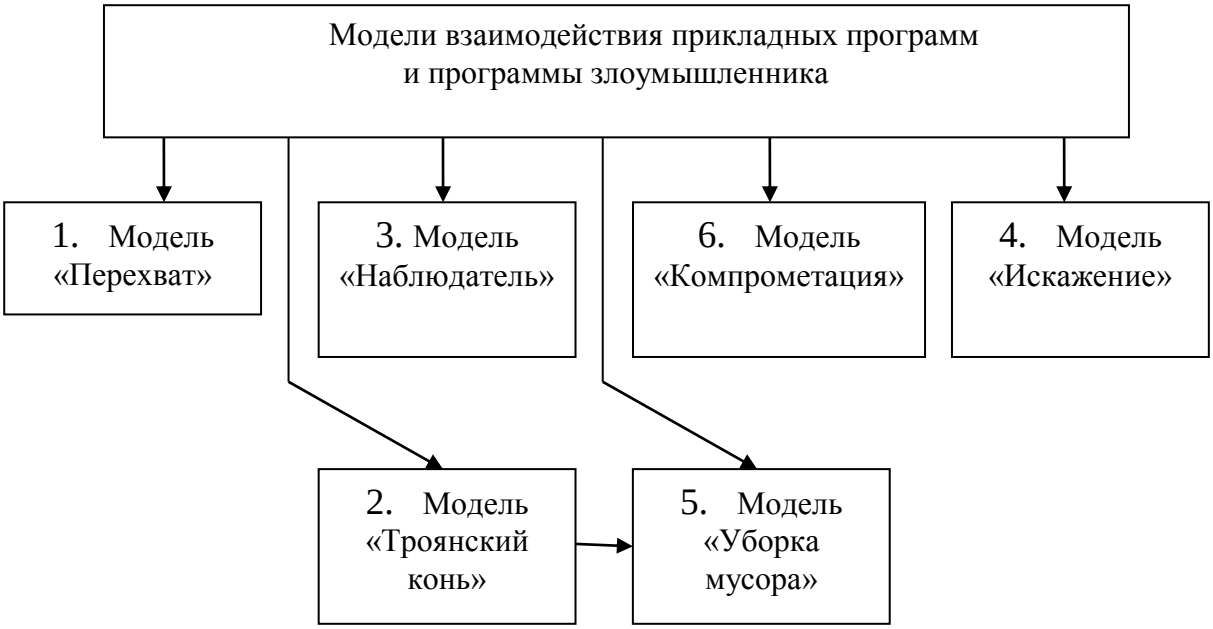

Рис. 7.2. Классификация моделей взаимодействия прикладных программ с программой злоумышленника

1) Модель «Перехват». Программная закладка встраивается в ПЗУ, ОС или прикладное ПО и сохраняет все или избранные фрагменты вводимой или выводимой информации в скрытой области локальной или удаленной памяти прямого доступа. Объектом сохранения может быть клавиатурный ввод (целиком или избранные последовательности), документы, выводимые на принтер, уничтожаемые файлы-документы.

Эта модель является двухэтапной: на первом этапе сохраняются только атрибутивные признаки (например, имена или начала файлов), затем накопленная информация снимается и злоумышленник принимает решение о конкретных объектах дальнейшей атаки. Здесь существенно наличие во внешней памяти места хранения информации, организованное так, чтобы обеспечить ее сохранность на протяжении заданного отрезка времени и возможность ее съема. Информация должна быть замаскирована от просмотра легальным пользователем.

2) Модель «Троянский конь». Закладка встраивается в постоянно используемое ПО и по некоторому активизирующему событию моделирует сбойную ситуацию на средствах хранения информации или оборудовании КС. При этом достигаются две цели: парализуется работа КС, а злоумышленник под видом ремонта может ознакомиться с имеющейся в системе информацией, накопленной по модели «перехват». Событием, активизирующим закладку, может быть заданный момент времени, сигнал по каналу модемной связи (явный или мас-

кированный), состояние некоторого счетчика (например, число запусков программы) и пр.

3) Модель «Наблюдатель». Закладка встраивается в сетевое ПО. Пользуясь тем, что данное ПО, как правило, всегда активно, закладка осуществляет контроль процесса обработки информации на компьютере, установку и удаление закладок, съем накопленной информации (первая модель «сохранение»). Закладка может инициировать события для ранее внедренных закладок, действующих по модели «троянский конь».

4) Модель «Искажение или инициатор ошибок». Закладка искажает входные потоки данных, либо выходные потоки, возникающие при работе прикладных программ, либо инициирует (или подавляет) ошибки, возникающие при работе последних.

5) Модель «Уборка мусора». Здесь прямого воздействия РПС может не быть. Изучаются «остатки» информации. В случае применения программной закладки навязывается такой порядок работы, который максимизирует количество остающихся фрагментов ценной информации. Злоумышленник получает либо данные фрагменты, используя закладки моделей 2 и 3, либо непосредственный доступ к компьютеру под видом ремонта или профилактики.

6) Модель «Компрометация». Закладка либо передает заданную злоумышленником информацию (например, клавиатурный ввод) в канал связи, либо сохраняет ее, не полагаясь на гарантированную возможность последующего приема или снятия.

У рассмотренных моделей имеется одна общая черта — наличие операции записи в оперативную или внешнюю память, производимой закладкой. Без такой операции негативное воздействие невозможно. Для направленного воздействия закладка должна также уметь читать. Без чтения невозможна модификация данных, а возможно только их разрушение. Операции чтения и записи могут быть не связаны с получением информации, так происходит, например, при считывании параметров устройств или его инициализации – закладка может использовать такие операции для инициирования сбойных ситуаций или для переназначения ввода/вывода.

Возможные комбинации несанкционированного чтения (НСЧ), несанкционированной записи (НСЗ) закладкой, санкционированного чтения (СЧ) и санкционированной записи (СЗ) прикладной программой или ОС приведены в таблице 7.1.

Таблица 7.1

Возможные комбинации несанкционированных и санкционированных действий

№ ситуации	НСЧ	НСЗ	Действия закладки	СЧ	СЗ
1	0	0	Нет	0	0
2	0	0	Нет	0	1
3	0	0	Нет	1	0
4	0	0	Нет	1	1
5	0	1	Изменение (разрушение) кода прикладной программы	0	0
6	0	1	Разрушение или сохранение данных, вводимых прикладной программой	0	1
7	0	1	Разрушение или сохранение данных, выводимых прикладной программой	1	0
8	0	1	Разрушение или сохранение вводимых или выводимых данных	1	1
9	1	0	Нет	0	0
10	1	0	Перенос данных, выводимых прикладной программой в ОП	0	1
11	1	0	Перенос данных, вводимых в прикладную программу в ОП	1	0
12	1	0	Перенос выводимы и вводимых данных в ОП	1	1
13	1	1	Процедуры типа «размножение вируса» (действия закладки независимо от операций прикладной программы)	0	0
14	1	1	Те же действия, что и в ситуациях 6–8	0	1
15	1	1		1	0
16	1	1		1	1

Ситуации 1–4 соответствуют нормальной работе прикладной программы — закладка не оказывает воздействия.

Ситуация 5 может быть связана либо с разрушением прикладной программы в ОП ЭВМ (прикладная программа не выполняет операции записи и чтения), либо с сохранением уже накопленной в ОП информации.

Ситуация 6 связана с разрушением или сохранением информации (искажение или сохранение выходного потока), записываемой прикладной программой.

Ситуация 7 связана с сохранением информации (сохранением входного потока), считываемой прикладной программой.

Ситуация 8 связана с сохранением информации закладкой при считывании или записи ее прикладной программой.

Ситуация 9 не связана с прямым негативным воздействием, так как прикладная программа не активна, а закладка производит только НСЧ (процесс «настройки»).

Ситуация 10 может быть связана с сохранением выводимой информации в ОП.

Ситуация 11 может быть связана с сохранением вводимой информации в ОП, либо с изменением параметров процесса сканированного чтения закладкой.

Ситуация 12 может быть связана с сохранением как вводимой, так и выводимой прикладной программой информации в ОП.

Ситуация 13 может быть связана с размножением закладки, сохранением накопленной в буферах ОП информации или с разрушением кода прикладной программы и данных в файлах, так как прикладная программа не активна.

Ситуации 14–16 могут быть связаны как с сохранением, так и с разрушением данных или кода программы и аналогичны ситуациям 6–8.

НСЗ закладкой может происходить:

— в массив данных, не совпадающий с пользовательской информацией — сохранение информации закладкой;

— в массив данных, совпадающий с пользовательской информацией или ее подмножеством — искажение, уничтожение или навязывание информации закладкой.

Таким образом, существуют три основные группы деструктивных функций, которые могут выполняться закладками:

1. Сохранение фрагмента информации, возникающей при работе пользователя, прикладной программы, вводе/выводе данных, во внешней памяти (локальной или удаленной) сети или выделенном компьютере, в том числе паролей, ключей и кодов доступа, конфиденциальных документов, либо безадресная компрометация фрагментов ценной информации (модели «перехват» и «компрометация»).

2. Изменение алгоритмов прикладных программ (целенаправленное воздействие во внешней или оперативной памяти), происходит изменение кодов программ (например, программа разграничения доступа начнет пропускать пользователей по любому паролю (модели «искажение» и «троянский конь»).

3. Навязывание некоторого режима работы (например, при уничтожении информации — блокирование записи на диск, при этом

информация не уничтожается), либо замена записываемой информации данными, навязываемыми закладкой.

Таким образом, можно выделит следующие компоненты программной среды, в которой существуют закладки: множество фрагментов кода прикладных программ, множество фрагментов кода закладок и множество событий, как последовательностей передачи управления от одного фрагмента кода к другому.

Классификация разрушающих программных средств и их воздействий

Выше мы привели классификацию разрушающих программных средств по функциональному признаку. Рассмотрим наиболее распространенную классификацию — классификацию по методу и месту их внедрения и применения (по способу «доставки» в КС). Эти признаки РПС делятся на:

— программы, ассоциированные с программно-аппаратной средой компьютера (основная или расширенная BIOS);

— программы, ассоциированные с программами первичной загрузки, находящиеся в Master Boot Record (MBR) или в BOOT секторах активных разделов — загрузочные закладки;

— программы, ассоциированные с загрузкой драйверов внешних устройств других ОС, командного интерпретатора, сетевых драйверов — т. е. с загрузкой операционной среды;

— программы, ассоциированные с прикладными программами общего назначения (встроенные в клавиатурные и экранные драйверы, в программы тестирования компьютеров, утилиты и файловые оболочки);

— исполняемые модули, содержащие только код закладки (как правило, внедряемые в файлы пакетной обработки типа *.BAT);

— модули-имитаторы, совпадающие по внешнему виду с некоторыми программами, требующими ввод конфиденциальной информации (характерны для UNIX-систем);

— программы, маскируемые под программные средства оптимизационного назначения (архиваторы, ускорители обмена с диском и пр.);

— программы, маскируемые под программные средства игрового и развлекательного назначения (как правило, используются для первичного внедрения закладок).

Кроме того, РПС имеют развитые средства борьбы с отладчиками и дизассемблерами.

Чтобы деструктивная программа могла выполнить какие-то действия по отношению к прикладной программе или данным, она должна получить управление, т. е. процессор должен начать ее выполнение. Это возможно только при наличии следующих двух условия:

1. РПС должно находиться в ОП до начала работы прикладной программы, которая является целью воздействия закладки, т. е. она должна быть загружена раньше или вместе с этой программой.

2. РПС должно активизироваться по некоторому общему, как для прикладной программы, так и для закладки активизирующему событию. То есть при выполнении ряда условий в программно-аппаратной среде управление должно быть передано закладке.

Выполнение этих условий достигается обычно путем анализа и обработки закладкой общих относительно закладки и прикладной программы воздействий (как правило, прерываний) либо событий (в зависимости от типа и архитектуры операционной среды). Прерывания должны сопровождать работу прикладной программы (например, прерывания ввода/вывода), либо всего компьютера (например, прерывания разделения времени). Эти два типа условий являются необходимыми, но не достаточными.

Возможен случай, когда при запуске прикладной программы (активирующим событием является запуск программы) закладка разрушает некоторую часть кода программы, уже загруженной в ОП, и систему контроля целостности кода или контроля иных событий, и на этом заканчивает работу. Этот случай не противоречит необходимым условиям.

При условии, что закладка может быть загружена в ОП раньше, чем цель ее воздействий, выделим закладки двух типов:

1. Закладки резидентного типа, находящиеся в ОП постоянно с некоторого момента времени до окончания сеанса работы на компьютере, его перезагрузки или выключения. Закладка может быть загружена при начальной загрузке компьютера или запуске некоторой программы (носителе закладки) или самостоятельно.

2. Закладка нерезидентного типа начинает работу, как и резидентные, но заканчивают самостоятельно, через некоторый промежуток времени или по некоторому событию, выгружаясь из ОП.

Для атак на КС часто используются РПС, *превышающие полномочия пользователей*. Эти закладки применяются для преодоления тех систем защиты, в которых реализовано разграничение доступа пользователей к объектам системы (в основном они используются

против ОС). Они позволяют злоумышленнику получить доступ к тем объектам, доступ к которым ему запрещен согласно текущей политике безопасности. В большинстве систем с разграничением доступа существуют администраторы, которые имеют право доступа ко всем (или почти всем) объектам системы. Если РПС наделяет злоумышленника такими правами, то он имеет практически неограниченный доступ к ресурсам системы.

Средства и методы, используемые такими закладками, в значительной степени определяются архитектурой атакуемой системы. Чаще всего эти закладки используют ошибки в программном обеспечении.

Широкое распространение получили и *перехватчики паролей*, которые перехватывают логины и пароли, вводимые пользователем. В простейшем случае перехваченные логины и пароли сохраняются в текстовом файле, более сложные закладки пересылают их по сети на компьютер злоумышленника. Существуют три основных архитектуры перехватчиков паролей:

1. Перехватчики первого рода. Злоумышленник запускает программу, которая имитирует приглашение пользователя для входа в систему и ждет ввода. Пользователь вводит логин и пароль, закладка сохраняет их в доступном злоумышленнику месте, завершает работу и осуществляет выход из системы злоумышленника (в большинстве ОС выход можно осуществить программно). По окончании работы закладки на экране ПК вновь появляется приглашение для входа пользователя в систему. Пользователь повторно вводит логин и пароль и начинает работу. Некоторые закладки по окончании своей работы выводят на экран сообщение об ошибке типа: «Пароль введен неверно. Попробуйте еще раз».

2. Перехватчики второго рода (сниферы) перехватывают все данные, вводимые пользователем с клавиатуры. Простейшие перехватчики просто сбрасывают все вводимые данные на жесткий диск ПК или в любое другое доступное злоумышленнику место. Более совершенные — анализируют перехваченные данные и отсеивают информацию, не имеющую отношения к паролям. Эти закладки являются резидентными, перехватывающими прерывания, используемые при работе с клавиатурой.

3. Перехватчики третьего рода — программы-закладки, полностью или частично подменяющие собой подсистему аутентификации защищенной системы. Задача создания такой закладки намного сложнее, чем задачи создания перехватчиков первого и второго ро-

да. Случаи применение таких перехватчиков в открытой литературе не публиковались.

Следующий вид РПС — *логические бомбы*. Это программные закладки, при определенных условиях оказывающие разрушающие воздействия на атакованную систему и обычно нацеленные на полное выведение ее из строя. В отличие от вирусов, логические бомбы не размножаются или размножаются ограниченно. Они всегда предназначены для конкретной КС. После завершения разрушающего воздействия логическая бомба уничтожается. Иногда выделяют особый класс логических бомб — временные бомбы, для которых условием срабатывания является достижение определенного момента времени. Характерным свойством логических бомб является то, что их воздействия носят исключительно разрушающий характер.

Еще один распространенный вид РПС – *мониторы*. Монитор — это программная закладка, перехватывающая те или иные потоки данных, протекающие в атакуемой системе. Целевое назначение мониторов может быть самым разным. Они могут быть предназначены для того, чтобы:

— полностью или частично сохранять перехваченную информацию в доступном злоумышленнику месте;

— искажать поток данных;

— помещать в поток данных навязываемую информацию;

— полностью или частично блокировать поток данных;

— использовать мониторинг потока данных для сбора информации об атакованной системе.

Мониторы позволяют перехватывать самые разные потоки атакуемой системы, однако наиболее часто перехватываются:

— потоки данных, связанные с чтением, записью и другими операциями над файлами;

— потоки данных, связанные с удалением информации с дисков или из ОП.

В отдельную категорию целесообразно выделить «злые шутки» (hoax). К ним относятся программы, которые не причиняют компьютеру вреда, однако выводят сообщения о том, какой вред уже нанесен, либо будет нанесен при определенных условиях. Это, например, программы, которые пугают пользователя сообщениями о форматировании диска (хотя на самом деле форматирования не происходит), детектируют вирусы в незараженных файлах (это делает, например, широко из-

вестная в прошлом программа Antitime), выводят странные вирусоподобные сообщения и т. д., в зависимости от юмора автора программы.

Методы внедрения разрушающих программных средств

Метод первый. Маскировка закладки под безобидное ПО. Закладка внедряется в систему под видом полезной программы. Это может быть текстовый или графический редактор, системная утилита, компьютерная игра, хранитель экрана и т. д. После внедрения такую закладку можно не маскировать, даже если администратор ее заметит, он не придаст этому значения.

При внедрении в многозадачную или многопользовательскую программную среду ее возможности сильно ограничены. В таких средах программы выполняются изолированно друг от друга, и закладка не может оказывать негативные воздействия на другие программные среды. Поэтому при внедрении такой закладки в многозадачную или многопользовательскую программную среду такой метод целесообразно применять только для внедрения инсталлирующей части составной программной закладки.

Метод второй. Маскировка закладки под безобидный модуль расширения программной среды. Многие программные среды допускают свое расширение дополнительными программными модулями. Например, для ОС Microsoft Windows модулями расширения могут выступать динамически подгружаемые библиотеки (DLL) и драйверы устройств. В качестве одного или нескольких модулей расширения в систему может быть внедрена программная закладка.

Этот метод фактически является частным случаем первого метода, но при внедрении закладки в многопользовательскую программную среду, поддерживающую разграничение доступа к объектам он более эффективен, поскольку модули расширения могут загружаться не только пользовательскими, но и системными процессами программной среды. В этом случае модуль расширения получает значительные возможности. С другой стороны, для внедрения такой закладки в многопользовательскую среду злоумышленник должен обладать большими полномочиями, которые при соблюдении адекватной политики безопасности предоставляются только системным администраторам.

Третий метод. Подмена закладкой одного или нескольких модулей атакуемой программной среды. В атакуемой среде выбирается один или несколько программных модулей, подмена которых фрагментами закладки позволяет оказывать на среду требуемые негатив-

ные воздействия. Закладка должна быть способна полностью реализовать все функции подменяемых модулей.

Основная, возникающая при этом, проблема заключается в том, что злоумышленник никогда не может быть уверен, что созданная им закладка точно реализует все функции подменяемого программного модуля. Если подменяемый модуль велик по объему или недостаточно полно задокументирован, точно запрограммировать все его функции практически невозможно.

Любая многозадачная программная среда обеспечивает корректность совместного доступа к программам и данным. Корректность подразумевает, что программа не может открыть для записи объект, уже открытый другой программой. Чтобы подмена могла произойти, необходимо либо завершить работу подменяемого модуля и перезапустить его после подмены, либо изменить конфигурацию системы так, чтобы после ее перезагрузки вместо подменяемого модуля была загружена закладка.

Если в многопользовательской среде реализовано разграничение доступа к объектам, то каждая программа запускается от имени того пользователя, который ее запустил. Чтобы закладка могла оказать серьезное воздействие на систему, она должна быть запущена либо от имени пользователя, обладающего достаточно большими правами, либо как системный процесс.

Четвертый метод. Прямое ассоциирование. Заключается в ассоциировании закладки с исполняемыми файлами одной или нескольких легальных программ. Сложность внедрения такой закладки зависит от того, является атакуемая среда одно или многозадачной, одно или многопользовательской. Для однозадачных однопользовательских систем эта задача решается достаточно просто. Для многопользовательских многозадачных систем эта задача достаточно сложна.

Прямое ассоциирование закладки с программным модулем предусматривает открытие закладкой для записи исполняемого файла программы, с которой происходит ассоциирование. Если в момент внедрения закладки программа выполняется или если атакуемая среда поддерживает разграничение доступа к своим объектам, при применении данного метода возникают те же проблемы, что и при применении третьего метода.

Так как при прямом ассоциировании закладки с атакуемой программой нарушается целостность исполняемого файла этой программы, закладка легко может быть выявлена с помощью контроля це-

лостности. При разработке закладки по методу прямого ассоциирования перед злоумышленником не стоит задача реализации всех функций программного модуля атакуемой среды, в который должна быть внедрена закладка. Поэтому данный метод в большинстве случаев более эффективен, чем метод подмены.

Пятый метод — косвенное ассоциирование — заключается в ассоциации закладки с кодом программного модуля загруженного в ОП. При косвенном ассоциировании исполняемый файл программного модуля остается неизменным, что затрудняет выявление закладки. Чтобы косвенное ассоциирование стало возможным, необходимо, чтобы инсталлирующая часть закладки уже присутствовала в системе. То есть закладка должна быть составной. При реализации косвенного ассоциирования в многозадачной среде инсталлирующая часть закладки должна получить доступ к коду или данным атакуемой программы. Так как в многозадачных средах программы выполняются изолированно друг от друга, косвенное ассоциирование возможно только в отдельных случаях. Так в ОС Microsoft Windows программная закладка может быть косвенно ассоциирована только с ядром системы, Hall.dll, или одним из Boot-драйверов. При этом инсталлирующая часть закладки должна выполняться в привилегированном режиме (kernel mode). Это сильно ограничивает применение данного метода.

Так как при косвенном ассоциировании закладки с одной из программ целостность кода последней не нарушается, выявить такую закладку сложно. Основным фактором, демаскирующим такую закладку, является наличие в системе инсталлирующей части закладки.

Существуют и другие методы. Так известна программа Teav Wiev — для удаленного входа в компьютер. При ее запуске на компьютере «жертвы» выдается логин и пароль. Если их передать удаленному пользователю, то он с помощью этой программы может работать на ПК «жертвы».

Наибольшая опасность при внедрении РПВ заключается в особой изобретательности их разработчиков. Так, чтобы в обход антивирусных средств осуществить закладку в программно-аппаратную среду с использованием модуля Computrace, реализуется схема, основанная на использовании соединения через AN/Ethernet, когда код модуля для запуска/инсталляции тех или иных устройств хранится в Flash-ROM BIOS. Bios агент (модуль) Computrace встраивается в BIOS как PCI-ROM. То есть используется обычный стандарт, который нужен

для загрузочных PCI устройств в системе: сетевая карта с ее Boot-ROM, SCSI, SATA контроллер и т. д.[1]

В процессе работы POST сканируется Option ROM — область памяти, где располагаются модули PCI-ROM, подсчитывается контрольная сумма CRC, и BIOS передает им управление для установки нужных их работе ресурсов. Таким образом, подобная методика предполагает изначальное нахождение данного модуля в исходном BIOS системы.

Получив управление, PCI-ROM модуль Computrace резервирует в свободной памяти блок объемом 64 кБ, куда расшифровывает/распаковывает свой код. При отсутствии свободной памяти используется фрагмент видеопамяти. В расшифрованном/распакованном коде содержится процедура поиска на жестком диске каталога Windows и запускных exe файлов. Стартовый файл для установки агента замещает собой autochk.exe в Windows/System32, переименовывая первоначальный файл в autochk.bak.

При старте Windows поддельный autochk.exe, получив управление, извлекает из своего тела файл rpc.net и прописывает его в реестр для работы/ автозагрузки в качестве сервиса. После получения управления от Windows уже в качестве сервиса, он (rpc.net) при наличии доступа в Интернет, соединяется с одним из управляющих серверов 209.53.113.xxx. С него скачивается полная версия, которая устанавливается на жесткий диск в качестве обычного файла (rpcnetp.dll) и в дальнейшем выполняет основную работу. Компьютер начинает управляться удаленно — принимает на исполнение как внутренние команды, так и через API-интерфейс, позволяет удаленно вызывать стандартные Windows процедуры (уровня application). Сервис обеспечивает периодический сигнал (раз в 4 часа) к серверу на запрос управления им. Установив удаленное управление, сервер может выполнять различные команды, например, удалять файлы с жесткого диска.

---

[1] Примечание: Опция Computrace — определяет поведение встроенных программных систем защиты от хищения устройств — в данном случае службы Computrace(R) от компании Absolute(R) Software. Это поле позволяет активировать или отключить модуль BIOS Computrace (R) опциональной службы в ОС от Absolute(R) Software. Computrace (R) агент от Absolute(R) Software является сервисом, предназначенным для отслеживания устройств и предоставления услуги по установлению их места расположения, в случае если компьютер будет потерян или украден. Computrace (R) агент общается с программным обеспечением сервера мониторинга Absolute(R) Software на запрограммированных интервалов для предоставления услуг слежения.

В качестве еще одного примера приведем новые способы внедрения РПВ на компьютер обычного пользователя. В последнее время широкую популярность в торговле, логистике приобрели матричные двумерные штрих коды — QR-коды, которые, по сравнению с обычными штрихкодами обеспечивают возможность хранения большего количества информации, а также доступны для скачивания любым средством вычислительной техники (СВТ) с камерой (рис. 7.3).

Рис. 7.3. Образец QR-кода

С помощью QR-кода можно заставить владельца СВТ выполнить необходимую злоумышленнику USSD команду (отображение IMEI, MAC WLAN и т. д.

Дополнительно к этому некоторое время назад в ряде СВТ под управлением ОС Android была найдена уязвимость, позволяющая использовать протокол tel://. Официально она предназначалась для того, чтобы прямо из браузера по ссылке на каком-то сайте можно было быстро позвонить туда. Однако вместе со ссылкой можно подставить и USSD команду, в том числе и автоматически — просто заставить браузер открыть tel://USSD .

Все это делает задачу защиты от РПВ весьма нетривиальной, предполагая от пользователя наличие обширных и постоянно обновляемых знаний в данной области.

С продвижением x64 на рынке ОС Microsoft Windows появились новые технологии защиты от РПВ. Одна из них — PatchGuard, отслеживающая изменение критических областей ядра ОС, таких как:

— таблица глобальных дескрипторов — GDT;

— таблица дескрипторов прерываний — IDT;

— таблица дескрипторов системных сервисов — SSDT;

— некоторые системные файлы, например, NTOSKRNL.EXE, NDIS.SYS, HAL.DLL;

— служебные MSR-регистры STAR/LSTAR/CSTAR/SFMASK.

При загрузке, в рамках функционирования PatchGuard, ОС подсчитывает контрольные суммы для вышеуказанных объектов, сохраняет их и периодически проверяет соответствие текущих значений с сохраненными значениями. Обнаружив несовпадение ОС завершает работу с вызовом BSOD («синий экран смерти»). Существует и еще один защитный механизм — запрет загрузки драйверов, не имеющих валидной электронной подписи (Driver Signing Policy).

Механизмы PatchGuard и Driver Signing Policy значительно усложнили жизнь разработчиков РПВ, работающих в режиме ядра. Это вынудило злоумышленников искать обходные пути и привело к возникновению нового класса РПВ — bootkit (сочетание слов boot и rookit). Наиболее известными из буткитов последнего поколения является Gapz. Он даже содержит модуль режима ядра, включающий собственную реализацию стека протоколов TCP/IP, что позволяет обойти проверку локальных IPS/IDS при взаимодействии с сетью. Кроме того, особенностью вредоносного кода режима ядра является отсутствие структуры исполняемого файла, обусловленное его разбиением на несколько блоков, имеющих собственные заголовки. При загрузке Gapz анализирует заголовок каждого блока и вызывает функцию инициализации, которая, в свою очередь, выделяет память и заполняет их указателями на функции блока, а также различными структурами данных. Блоки модулей могут размещаться в секторах или до первого, или после последнего раздела, причем само хранилище выполнено в виде файла с зашифрованным содержимым (шифр AES-256) и хранящимися в каталоге System Volume Information системного диска с именем из случайных кэш значений.

Буткит Gapz имеет несколько версий, различающихся методами загрузки. Так он использует реализацию VBR тома NTFS, который содержит в себе структуру данных BPB (BIOS Parameter Blcok), указывающую на параметры тома. Наличие в BPB 4-хбайтного поля HiddenSectors, определяющего начало IPL (Initial Program Loader) — кода, которому передается управление после VBR, позволяет производить поиск загрузчика в файловой системе NTFS и его запуск. За счет

изменения данного поля буткит Gapz добивается передачи управления кода VBR не на IPL, а на свой код (рис. 7.4).

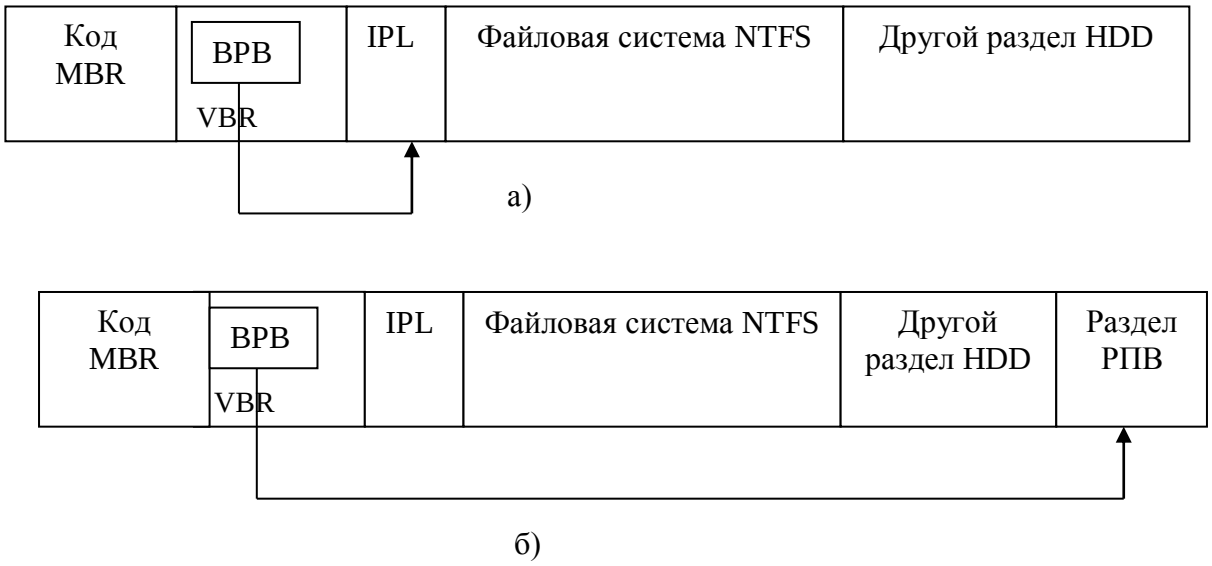

Рис. 7.4. Буткит Gapz получает управление, изменив 4 байта BPB

7.2. Принципы и методы защиты от разрушающих программных воздействий

Задача защиты от РПВ может ставиться в нескольких различных вариантах.

Первый вариант: выявление и уничтожение (лечение). Он берет начало в задачах выявления и ликвидации вирусов. Ослабленная разновидность этого варианта — выявление РПВ. Алгоритмы нахождения и лечения отличаются определенной ненадежностью: возможен пропуск РПВ в ходе проверки при условии, что он есть (ошибка первого рода); возможно обнаружение РПВ там, где его нет (ошибка второго рода — ложная тревога). Для серьезной системы защиты необходимо полностью исключить наличие РПВ (или допустить его присутствие с некоторой заданной малой вероятностью). Следовательно, задача борьбы с РПВ начинается со следующих исходных условий:

— априорно неизвестно наличие в каком-либо множестве программ фрагментов РПВ. Ставится задача определения факта их наличия или отсутствия. При этом программы не выполняются (статическая задача).

В условиях п. 1 прикладные программы используются по назначению. Ставится задача выявления закладки по результатам работы прикладных программ (динамическая задача).

Происходит обмен программным продуктом (либо в пространстве — передача по каналу связи или пересылка на магнитном носителе; либо во времени – хранение), априорно свободным от потенциально опасных действий. Программа не исполняется. Задача защиты ставится в трех вариантах: не допустить внедрение закладки; выявить внедренную закладку; удалить закладку.

В условиях п. 3 решается динамическая задача — защита от воздействия закладки в ходе работы программы.

При условии потенциальной возможности воздействия закладок решается задача борьбы с их итоговым влиянием. Закладка присутствует в системе, но либо неактивна при выполнении критических действий прикладных программ, либо результат их воздействия не конструктивен.

Методы борьбы с закладками можно разделить на классы и увязать с общей проблемой защиты ПО от несанкционированного доступа:

Общие методы защиты ПО, решающие задачи борьбы со случайными сбоями оборудования и НСД.

А) Контроль целостности системных областей, запускаемых прикладных программ и используемых данных (решение задачи 3).

Б) Контроль критических для безопасности системы событий (решение задачи 2).

Данные методы действенны лишь тогда, когда контрольные элементы не подвержены воздействию закладок и разрушающее воздействие либо инициирующее его событие входит в контролируемый класс. Так система контроля за вызовом прерываний не будет отслеживать обращение к устройствам на уровне портов. С другой стороны, контроль событий может быть обойден путем:

— навязывания конечного результата проверок;

— влияния на процесс считывания информации;

— изменения контрольных элементов (хэш-функций), хранящихся в общедоступных файлах или в оперативной памяти.

Важно, что контроль должен быть выполнен до начала влияния закладки, либо контроль должен осуществляться полностью аппаратными средствами с программным управлением, содержащимися в ПЗУ.

В) Создание безопасной и изолированной операционной среды (решение задачи 4).

Г) Предотвращение результирующего воздействия вируса или закладки (например, запись на диск только в зашифрованном виде на уровне контроллера — тем самым локальное сохранение информации

закладкой не имеет смысла — или запрет записи на диск на аппаратном уровне (решение задачи 5).

2. Специальные методы выявления программ с потенциально опасными последствиями.

А) Поиск фрагментов кода по характерным последовательностям (сигнатурам), свойственным закладкам, либо наоборот — разрешение на выполнение или внедрение в цепочку прерываний только программам с известными сигнатурами (решение задач 1 и 2).

Б) Поиск критических участков кода (с точки зрения безопасности КС) методом семантического анализа. Анализ фрагментов кода на выполнение ими функции, например, выполнение несанкционированной записи, часто сопряжен с дизассемблированием или эмуляцией решения (задачи 1 и 2).

Рассмотрим процесс создания защищенного фрагмента КС в применении к проблеме защиты от РПВ.

Шаг 1. Первоначально нужно убедиться, что в ПО ПЗУ системы (например, в BIOS ПЭВМ) нет РПВ. Эта задача может решаться в статическом (задача 1) или в динамическом (задача 2) вариантах. С точки зрения экономико-временных параметров целесообразнее решение задачи 1, т. к. в противном случае требуется длительная работа в аппаратной среде в различных режимах. На практике желательно комплексно решать 1 и 2 задачи.

Далее следует определить состав программных средств базовой вычислительной среды, т. е. определить конкретную ОС, дополнительные программные средства сервиса (например, программные оболочки или средства телекоммуникации) и программные средства поддержки дополнительного оборудования (программы управления принтером и т. п.).

Шаг 2. Убедиться в отсутствии РПВ в описанном наборе базовых ПС. При этом в составе ПО базовой вычислительной среды не должно быть целого класса возможностей — назовем их инструментальными. Это возможность вмешательства оператора в содержимое ОП, возможность инициирования и прекращения выполнения процессов нестандартным образом (помимо механизмов ОС).

Обобщенно достаточные условия к базовому набору ПО можно сформулировать так: в ПО, которое может быть инициировано в системе, не должно быть функций порождения и прекращения выполнения процессов, кроме заранее определенных, не должно быть

возможностей влияния на среду выполнения уже активных процессов и на сами процессы.

Шаг 3. Проектирование и разработка программных или программно-аппаратных средств защиты КС и их тестирование.

Шаг 4. Объединение всего комплекса ПО, включая и средства защиты, в изолированную программную среду. В этой среде программное обеспечение, полученное на шагах 1–3, остается неизменным. При пустом множестве активизирующих событий для закладки потенциально опасные действия с ее стороны невозможны.

Пусть в ПЗУ (BIOS) и в ОС закладки отсутствуют. Пользователь работает с программой, процесс написания и отладки которой полностью контролируются (исключено наличие закладок или каких-либо скрытых возможностей — проверенная программа).

Проанализируем откуда могут исходить потенциальные угрозы для такой системы.

1) Проверенные программы будут использованы на другом компьютере с другой BIOS, которая содержит закладки.

2) Проверенные программы будут использованы в аналогичной, но не проверенной операционной среде, в которой содержатся закладки.

3) Проверенные программы используются на проверенном компьютере, в проверенной программной среде, но вместе с ними запускаются и непроверенные программы, несущие в себе закладки.

Таким образом, деструктивные действия закладок невозможны, если:

1) На компьютере с проверенной BIOS установлена проверенная операционная среда.

2) Установлена неизменность операционной среды и BIOS для данного сеанса работы.

3) В данной программной среде запускаются только проверенные программы.

4) Запуск проверенных программ вне проверенной среды исключен.

5) При выполнении перечисленных условий программная среда называется изолированной.

Таким образом, основными элементами поддержания изолированной среды являются контроль целостности и контроль активности процессов. Для контроля целостности важно выполнение следующих двух условий: надежный алгоритм контроля и контроль реальных данных.

Контроль целостности всегда сопряжен с чтением данных (по секторам, по файлам и т. д.). Например, закладка в BIOS может навя-

зать при чтении вместо одного сектора другой или редактировать непосредственно буфер. С другой стороны, контроль BIOS может происходить «под наблюдением» какой-то другой аппаратуры и не показать изменение его содержимого. Аналогичные эффекты могут возникнуть и при обработке файла. Поэтому необходима модель «безопасной загрузки» или ступенчатого контроля. Эта модель заключается в постепенном установлении неизменности компонент программно-аппаратной среды: сначала проверяется BIOS. При положительном исходе этой проверки, через проверенную BIOS считываются загрузочный сектор и драйверы ОС (по секторам). Их неизменность проверяется через доверенные функции ОС.

При анализе проблемы защищенности информации в ходе ее обработки в КС необходимо обращать внимание на наличие скрытых возможностей в базовом ПО. Скрытые возможности сами по себе или в сочетании с другими программами базового ПО могут привести к опосредованному НСД. Для обеспечения безопасности обрабатываемой информации и всего информационного процесса в базовом ПО необходимо предусмотреть невозможность:

1) запуска иных программ, кроме программ базового ПО;

2) влияния на среду функционирования и сами программы, уже выполняемые в КС;

3) изменения любых программ базового ПО.

Данные три условия наиболее просто было бы выполнить в тех случаях, когда базовое ПО находится в ПЗУ, в котором нет иных программ. Инициирование программ происходит при включении питания. Однако это существенно ограничивает возможности компьютера, поэтому такой подход рационально использовать только в специальных вычислительных машинах и комплексах.

На практике в КС работает несколько человек, каждый из которых использует свое подмножество программ базового ПО, причем некоторыми программами базового ПО могут пользоваться сразу несколько человек. Практически на любом компьютере есть возможность влиять на среду функционирования. Например, текстовый редактор может использоваться для коррекции кода программы. Если не поставить соответствующих ограничений, всегда есть возможность использования программ-отладчиков, например, DEBUG.

При этом выполнить условия 1–3 становится практически невозможным. *Пример.* Текстовый редактор является неотъемлемой частью любой прикладной программной системы. Из любого редактора

возможен запуск программы либо напрямую, через операционную среду, либо косвенно, минуя ее.

Даже если администратор системы исключит из состава ПО все программы, которые кажутся ему подозрительными, пользователь все равно будет иметь возможность выхода в операционную среду (и выполнения ее команд, в том числе — уничтожение информации) и потенциальной активизации принесенных на различных носителях программных средств (в том числе, загружая собственную операционную среду). Если принять во внимание еще и скрытые возможности ПО, то говорить о защищенности информации в системе невозможно.

Рассмотрим функционирование программ в изолированной программной среде. В этом случае требования к базовому ПО значительно ослабляются. В самом деле, изолированная программная среда контролирует активизацию процессов через операционную среду, контролирует целостность исполняемых модулей перед их запуском и разрешает инициирование процесса только при одновременном выполнении двух условий: принадлежности программы к множеству разрешенных программ и неизменности программы. В таком случае от базового ПО требуется:

1) невозможность запуска программ в обход контролируемых изолированной программной средой событий;

2) отсутствие возможностей влиять на среду функционирования уже запущенных программ (невозможность редактирования ОП).

Все иные действия, являющиеся нарушением условий 1–3, в оставшейся их части, будут выявляться и блокироваться. Таким образом, изолированная программная среда значительно снижает трудозатраты на анализ наличия скрытых возможностей в ПО.

При включении компьютера происходит тестирование ОП, инициализация таблицы прерываний и поиск расширений BIOS. При наличии расширений, управление передается им. После обработки расширений BIOS в память считывается первый сектор магнитного носителя информации (МНИ) и управление передается ему, код загрузчика считывает драйверы, далее выполняются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска.

При реализации изолированной программной среды на нее должны быть возложены функции контроля запуска программ и контроля целостности. Выше, при описании методологии создания изолированной программной среды упоминалась проблема контроля реальных данных. Суть этой проблемы состоит в том, что контролируемая

на целостность информация может представляться по-разному на разных уровнях. Если программный модуль, обслуживающий процесс чтения данных, не содержал РПВ и целостность его зафиксирована, то при его последующей неизменности чтение с использованием его будет чтением реальных данных. Из этого утверждения логически вытекает способ ступенчатого контроля.

При запуске изолированной программной среды таким же образом и в той же последовательности происходит контроль целостности. Самым же первым этапом является контроль целостности программ в ПЗУ.

Контрольные вопросы:

1. Каковы модели разрушающих программных воздействий?
2. В чем состоит сущность разрушающих программных воздействий?
3. Расскажите о методах внедрения разрушающих программных средств.
4. Каковы принципы и методы защиты разрушающих программных воздействий?

Лекция 8. Добавочные средства защиты информации (на примере СЗКИ Dallas Lock)

Вопросы лекции:

8.1. Общие сведения о системе защиты компьютерной информации Dallas Lock.

8.2. Установка и администрирование Dallas Lock.

8.3. Работа в СКЗИ Dallas Lock.

8.1. Общие сведения о системе защиты компьютерной информации Dallas Lock

Типичным представителем специализированных (добавочных) средств защиты компьютерной информации является СЗКИ Dallas Lock. СЗКИ Dallas Lock может устанавливаться на компьютеры с ОС Windows или Linux. Мы опишем вариант работы в среде Windows ЗКИ Dallas Lock 8.0 — последней по времени версии (2020).

СЗКИ «Dallas Lock» (разработчик ООО «Конфидент») представляет собой программно-аппаратный комплекс, добавляющий к системе безопасности Windows следующие функциональные возможности:

— организация доверенной загрузки с возможностью идентификации и аутентификации при помощи электронных идентификаторов Touch Memory;

— создание замкнутой программной среды для пользователей путем разрешения запуска ограниченного количества прикладных программ и динамических библиотек;

— реализация мандатной или дискреционной (по выбору) модели разграничения доступа;

— контроль потоков защищаемой информации;

— очистка секторов, занимаемых защищаемыми файлами при их удалении, а также очистка памяти, выделяемой прикладным программам;

— контроль целостности указанных администратором файлов и системных областей диска;

— аудит доступа к защищаемым ресурсам;

— защита данных путем криптографического преобразования информации на диске.

8.2. Установка и администрирование СЗКИ Dallas Lock

Установка системы защиты «Dallas Lock» производится стандартным образом с вводом кода активации, получаемого в сервисном центре фирмы «Конфидент». После запуска образа системы и отработки процедуры POST BIOS происходит инициализация системы защиты «Dallas Lock» из MBR активного раздела. При этом запрашиваются идентификатор и пароль пользователя.

После предъявления правильного пароля и идентификатора выполняется процедура контроля целостности, при удачном завершении которой стандартным образом загружается ОС Windows.

Создание пользователей в СЗИ осуществляется с использованием программы «Администратор DL 8.0», которая вызывается командой ***Пуск ⇒ Программы ⇒ Dallas Lock 8.0 ⇒ Администратор DL 8.0***. Для создания учетных записей необходимо выполнить команду меню ***Пользователи ⇒ Создать***. Открывающееся окно «Новый пользователь» имеет четыре вкладки: «Общие», «Идентификация», «Расписание», «Группы».

Вкладка «Общие» позволяет установить для каждого из создаваемых пользователей следующие рекомендуемые параметры: «Потребовать смену пароля при следующем входе» (после первой регистрации каждый из пользователей должен будет изменить свой пароль), «Разрешена загрузка компьютера» (все пользователи могут включать защищаемый компьютер), «Блокировать клавиатуру», «Блокировать при нарушении целостности», «Запретить прерывать преобразование диска».

Вкладка «Идентификация» позволяет установить для каждого из пользователей электронный идентификатор Touch Memory. С помощью Вкладки «Расписание» указываются разрешенные дни недели и время работы пользователей, а вкладка «Группы» предназначена для включения учетной записи в одну или несколько рабочих групп. После задания необходимых параметров для каждой учетной записи вводится пароль.

Реализация мандатной модели разграничения доступа. Мандатная модель разграничения доступа в СЗИ «Dallas Lock» реализована посредством назначения защищаемым ресурсам и каждому пользователю системы меток конфиденциальности и сравнения их при запросах на доступ. В качестве меток конфиденциальности выступают:

— для защищаемых ресурсов — классификационная метка мандатного доступа;

— для пользователей — уровень допуска.

В СЗКИ «Dallas Lock» используются следующие наименования меток конфиденциальности в порядке повышения: «Открытые данные», «Конфиденциально» (соответствует «ДСП») и «Строго конфиденциально» (соответствует «Секретно»).

Наличие уровня допуска определяется значениями параметров «Уровень доступа: Конфиденциально» и «Уровень доступа: Строго конфиденциально», входящих в группу параметров безопасности «Права пользователей» программы «Администратор DL 8.0». Значением этих параметров является список учетных записей пользователей и групп, которым назначается соответствующий допуск. По умолчанию значением параметра «Уровень доступа: Конфиденциально» является группа «Конфиденциально», а значением параметра «Уровень доступа: Строго конфиденциально» — группа «Строго конфиденциально».

Применение такого подхода к назначению уровней допуска позволяет воспользоваться идеологией рабочих групп: для назначения пользователю допуска следует включить его учетную запись в состав одной из групп — «Конфиденциально» или «Строго конфиденциально». Если пользователь не включен в одну из этих групп, он допускается только к открытым данным. По умолчанию для каждого создаваемого пользователя устанавливается доступ к открытым данным.

Для защищаемых ресурсов (диски, каталоги, файлы) должны быть установлены классификационные метки мандатного доступа. По умолчанию все объекты относятся к категории «Открытые данные», доступ к которым могут получать пользователи с любым уровнем допуска.

Для изменения уровня конфиденциальности следует вызвать в контекстном меню объекта пункт «Dallas Lock 8.0», перейти к вкладке «Мандатный доступ» и, отключив параметр «По умолчанию», установить требуемый уровень.

Первая регистрация пользователя в системе связана с созданием профиля пользователя, т. е. набора каталогов и файлов в каталоге «Documents and Settings», имеющем гриф секретности «Открытые данные». Создание каталогов и файлов с грифом «Открытые данные» возможно только в том случае, когда текущий уровень допуска не превышает «Открытые данные». Таким образом, первая регистрация пользователя в системе должна быть осуществлена с текущим уровнем допуска «Открытые данные».

Реализация дискреционной модели разграничения доступа. Дискреционная модель разграничения доступа реализуется в СЗИ

«Dallas Lock» посредством стандартных списков доступа. Для просмотра или редактирования списков доступа необходимо из контекстного меню объекта выбрать пункт «Dallas Lock 8.0», в появившемся окне — вкладку «Доступ».

Основным отличием данного СЗКИ является то, что списки доступа выполнены не средствами ОС Windows (не средствами файловой системы NTFS), а собственным механизмом. Следствием этого является, во-первых, то, что списки доступа можно реализовать на разделах с файловой системой FAT (а не только NTFS). Во-вторых, вводится собственный, отличный от принятого в ОС Windows, алгоритм определения права доступа пользователя к ресурсу.

При попытке текущего пользователя совершить с объектом любую операцию система защиты анализирует в первую очередь локальные параметры данного объекта. Для этого она проверяет:

1. К какому разряду по отношению к объекту защиты принадлежит пользователь. Если это индивидуальный пользователь и ему назначены локальные параметры по отношению к данному объекту, то право на совершение запрошенной операции устанавливается исходя из этих параметров. Если параметру, контролирующему данную операцию, присвоено значение «Разрешить», то операция выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

2. Если текущий пользователь не относится к разряду индивидуальных пользователей или значение контролирующего данную операцию параметра явно не указано, то система защиты проверяет, входит ли текущий пользователь в какую-либо из групп пользователей, для которой назначены локальные параметры по отношению к данному ресурсу. Если это так, то право пользователя на совершение запрошенной операции устанавливается исходя из параметров этой группы. Если группе пользователей предоставлено право на совершение операции (контролирующему параметру присвоено значение «Разрешить»), то операция выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

3. Если текущий пользователь не принадлежит ни к одному из указанных выше разрядов или значение контролирующего параметра явно не указано, то анализируются локальные параметры, установленные для разряда «Все» по отношению к этому ресурсу. Если разряду «Все» предоставлено право на совершение операции (контролирующему параметру присвоено значение «Разрешить»), то операция

выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

4. Если значение контролирующего параметра для разряда «Все» явно не указано или для данного разряда не установлены локальные параметры, то система защиты проверяет, входит ли данный объект в состав другого объекта. При положительном результате повторяются действия пунктов 1–3, при отрицательном система защиты переходит к проверке глобальных параметров. Анализ глобальных параметров осуществляется по той же самой схеме, что и локальных.

Обеспечение замкнутости программной среды. Механизм замкнутой программной среды реализуется в СЗИ «Dallas Lock» путем установки для пользователей глобального запрета на запуск программ и разрешения запуска лишь определенных исполняемых файлов.

Стратегия может быть следующей:

1. Определить, какие исполняемые файлы должны запускаться для нормальной работы ОС;

2. Решить, какие файлы разрешается запускать пользователям для работы;

3. Запретить запуск всех исполняемых файлов для сменных дисков;

4. Запретить запуск всех исполняемых файлов для каждого из фиксированных логических дисков, доступных ОС;

5. Установить разрешение на исполнение выбранных файлов для конкретных пользователей или групп пользователей.

Очевидно, что пользователю должно быть запрещено изменение файлов, которые он имеет право запускать на выполнение.

Для установки глобального запрета на запуск программ на сменных носителях необходимо в программе «Администратор DL 8.0» в группе параметров безопасности «Параметры ресурсов» выбрать «Параметры сменных дисков по умолчанию». В диалоговом окне необходимо установить запрет на выполнение для группы пользователей «Все», а также разрешить выполнение для группы «Администраторы». В результате все пользователи, за исключением администраторов, не смогут запускать исполняемые файлы, находящиеся на сменных носителях (CD-ROM, дискеты).

Установка запрета на запуск файлов, находящихся на фиксированных носителях, производится через контекстное меню объекта (пункт меню Dallas Lock 8.0»). Запрет запуска при помощи «Администратора DL 8.0» (как в случае со сменными носителями) недопустим, так как он не вступает в силу. Чтобы обеспечить возможность нормальной загрузки и работы ОС, необходимо разрешить выполне-

ние файлов, находящихся в каталоге «*%SystemRoot%\system32*», а также файла «*%SystemRoot%\explorer.exe*».

8.3. Работа в СЗКИ Dallas Lock 8.0

Проверка целостности. СЗИ «Dallas Lock 8.0» включает в свой состав подсистему проверки целостности. Она запускается до загрузки ОС и обеспечивает проверку целостности BIOS, CMOS и MBR жесткого диска, а также проверку дисков, каталогов и файлов в случае установки соответствующих параметров.

Включение контроля целостности BIOS, CMOS, MBR и загрузочного сектора производится с использованием программы «Администратор DL 8.0» (группа настроек ***Параметры безопасности*** ⇒ ***Контроль целостности ПЭВМ***). Чтобы включить контроль целостности для файла или каталога, необходимо в контекстном меню выбрать пункт «Dallas Lock 8.0», и в открывшемся диалоговом окне открыть вкладку «Контроль целостности».

Для расчета контрольной суммы могут использоваться следующие алгоритмы: CRC32, хэш по ГОСТ Р 34.11-94 или хэш MD5. Если для объекта файловой системы задан контроль целостности, то система не позволит изменить этот объект, и он будет доступен только для чтения и выполнения.

Проверка целостности осуществляется при загрузке компьютера до начала загрузки ОС. При нарушении целостности хотя бы одного файла, загрузка компьютера блокируется для всех пользователей, кроме администратора безопасности (пользователя Администратор). Возможно возникновение ситуации, когда файл, для которого был установлен контроль целостности, удаляется администратором безопасности (остальные пользователи изменить этот файл не смогут). При попытке сверить контрольную сумму этого файла с эталонной будет принято решение о нарушении целостности, так как файла вообще не будет найдено. В результате загрузка всех пользователей, кроме администратора безопасности, будет заблокирована.

Ситуация является ошибочной, так как администратор не сможет отключить контроль целостности несуществующего файла. Чтобы обойти подобную ситуацию в СЗИ «Dallas Lock» предусмотрена функция пересчета списка дескрипторов. Активизация этой функции производится в программе «Администратор DL 8.0» командой меню ***Файл ⇒ Перестроить список дескрипторов***.

Регистрация событий. СЗИ Dallas Lock 8.0 включает средства аудита, автоматически ведущие запись в пять системных журналов:

«журнал входов», «журнал доступа к ресурсам», «журнал управления политиками безопасности», «журнал печати» и «журнал управления учетными записями». В «журнале входов» фиксируются события, связанные с загрузкой компьютера и регистрацией пользователя в ОС. «Журнал доступа к ресурсам» предназначен для отслеживания обращений пользователя к защищаемым ресурсам. «Журнал управления политиками безопасности» содержит информацию о действиях пользователя по настройке параметров системы защиты. В «журнале печати» отображаются все попытки печати. «Журнал управления учетными записями» предназначен для учета действий по изменению прав пользователей.

Включение регистрации указанных категорий событий производится в программе «Администратор DL 8.0» в разделе «Политика аудита».

Назначение аудита доступа к ресурсам производится отдельно для каждого ресурса. Чтобы включить регистрацию событий, связанных с конкретным ресурсом, необходимо в контекстном меню ресурса выбрать пункт «Dallas Lock 8.0», затем выбрать вкладку «Аудит» в открывшемся диалоговом окне и снять отметку «По умолчанию». Существует возможность фиксировать все типы событий доступа, которые могут контролироваться средствами СЗИ (обзор папки, создание файлов, выполнение и т. д.).

При просмотре содержимого журналов можно использовать средства фильтрации записей. Для включения фильтра необходимо зайти в любой из журналов, и в контекстном меню записи выбрать пункт «Настроить фильтр».

Правила фильтрации действуют на все журналы одновременно. Включение и выключение фильтра делается командой «Фильтрация» упомянутого контекстного меню.

Печать штампа. СЗИ «Dallas Lock» позволяет создавать штамп на документах, отправляемых на печать. Настройка печати штампа производится с использованием программы «Администратор DL 8.0» в разделе ***Параметры безопасности ⇒ Политика аудита***. Включение печати штампа для конфиденциальных и строго конфиденциальных документов, а также настройка информации, выводимой на штампе, производится в диалоговом окне «Штамп», которое открывается двойным щелчком на пункте «Печатать штамп». В этом диалоговом окне можно настроить положение штампа на странице (он печатается в верхней ее части), шрифт, которым он будет напечатан, а также содержимое штампа. Сам штамп представляет собой текстовый блок, который может содержать как неизменяемый текст, так

и служебные метаданные. Чтобы вставить в штамп служебную информацию, необходимо в контекстном меню поля ввода текста выбрать, какая именно информация должна быть добавлена.

Как уже было сказано, по умолчанию штамп печатается только на конфиденциальных и строго конфиденциальных документах. Чтобы печатать штамп на всех документах, нужно в «Администраторе DL» активизировать параметр «Печатать штамп на всех документах».

В силу особенностей программной реализации расположение штампа может незначительно меняться в зависимости от программы, из которой осуществляется печать. Так, при печати из программы WordPad требуется добавлять в штамп несколько пустых строк перед текстом, иначе верхняя строка надписи не будет видна. Поэтому рекомендуется проверять корректность вывода штампа из каждого используемого приложения, делая, при необходимости, соответствующие изменения в настройках внешнего вида штампа.

Гарантированное удаление данных. СЗИ «Dallas Lock 8.0» включает подсистему очистки остаточной информации, которая позволяет:

1. Заполнять очищаемое в результате удаления и изменения размеров файлов пространство жесткого диска маскирующей последовательностью;

2. Очищать (таким же образом) файл подкачки Windows при завершении работы;

3. Обнулять оперативную память при ее выделении;

4. Очищать все каталоги, помеченные как временные, при старте системы, завершении работы и завершении сеанса работы пользователя.

Включение указанных функций производится в программе «Администратор DL» в разделе «Очистка остаточной информации». Существует возможность задать от одного до пяти циклов затирания.

Реализация запрета загрузки в обход Dallas Lock. Запрет загрузки компьютера в обход защитных механизмов реализуется в СЗИ «Dallas Lock» путем внедрения процедур аутентификации пользователей и контроля целостности данных в программу, загрузка которой производится через MBR жесткого диска. Таким образом, загрузить ОС, например, в режиме защиты от сбоев становится невозможно.

Запрет загрузки со съемных носителей, а также противодействие анализу защищаемых данных при подключении жесткого диска к иному компьютеру осуществляется в СЗИ «Dallas Lock» путем включения режима прозрачного преобразования дисков. Алгоритм преобразования жесткого диска выбирается при установке СЗИ. Преобразованию может быть подвергнут весь диск либо его часть. Пре-

образование выполняется с использованием программы «Администратор DL 8.0», для чего необходимо в параметрах безопасности выбрать «Преобразование дисков» и указать область преобразования. Основным достигаемым результатом является невозможность обращения к диску в обход системы защиты.

Преобразование жесткого диска не является криптографической защитой данных — это лишь некое «кодирование» с использованием алгоритма, известного только разработчикам СЗИ. Вместе с тем даже такое кодирование является существенной преградой для злоумышленников.

При очередной загрузке компьютера начнется процесс преобразования указанной области. После преобразования получение доступа к данным, обрабатываемым на диске, в обход СЗИ становится невозможным. Таким образом, преобразование диска является важнейшим элементом для предотвращения несанкционированного доступа к данным и выполнения п. 2 Требований к защите АС от НСД. Для гарантированного блокирования возможности НСД при загрузке с внешних носителей необходимо осуществлять преобразование всего диска. Дополнительной мерой защиты является установка запрета загрузки с внешних носителей в настройках BIOS Setup, подкрепляемая паролем.

В данной лекции мы рассмотрели принципы работы с системой Dallas Lock. При этом мы особенно не вдавались в описание механизмов работы различных компонент СКЗИ, поскольку эти механизмы были рассмотрены нами ранее, в предыдущих лекциях.

Контрольные вопросы:

1. Расскажите о возможностях системы защиты компьютерной информации Dallas Lock.
2. Расскажите последовательность установки и администрирование Dallas Lock.
3. В чем состоит особенность работы в СКЗИ Dallas Lock?

Лекция 9. DLP-системы (на примере Falcongaze Secure Tower)

Вопросы лекции:

9.1. Функциональные требования, основные функции и способы перехвата информации Falcongaze Secure Tower.

9.2. Архитектурные решения Falcongaze Secure Tower 6.0.

9.3. Сертификация и соответствие требованиям регуляторов.

9.4. Методика реализации функциональных возможностей.

9.1. Функциональные требования, основные функции и способы перехвата информации Falcongaze Secure Tower

DLP — Data Loss Prevention — предотвращение утечек данных. Система DLP предназначена для активного противодействия утечкам информации из организации. Для реализации своего назначения эта система применяет блокировки сообщений и запрет определенных действий сотрудников компании. DLP — одна из важных компонент в системе обеспечения информационной безопасности организации.

Применение DLP-систем является наиболее актуальным для тех организаций, где количество конфиденциальной информации велико, а возможные финансовые и репутационные потери вследствие утечки могут привести к полному разорению организации или нанести существенный вред ее заказчикам, партнерам и клиентам.

Современные DLP-системы используются в государственном секторе, в банковской сфере, в энергетике, в промышленных компаниях, в научно-исследовательских центрах и др. Они решают задачи контроля конфиденциальной информации и задачи экономической безопасности, способствуют расследованию инцидентов, используются для оценки эффективности работы персонала.

Анализ рынка DLP-систем в России показывает, что в условиях импортозамещения российские системы вырвались на лидирующие позиции и вытеснили с него импортные аналоги. Российские системы ничем не уступают зарубежным функционально, в некоторых случаях даже превосходят их, а по цене — значительно ниже. Наиболее известными игроками отечественного рынка DLP-систем являются: группа компаний InfoWatch (до 30–50 % рынка), компания Solar Security, компания Searchinform, компания Zecurion, компания DeviceLock, компания Falcongaze и др. (рис. 9.1).

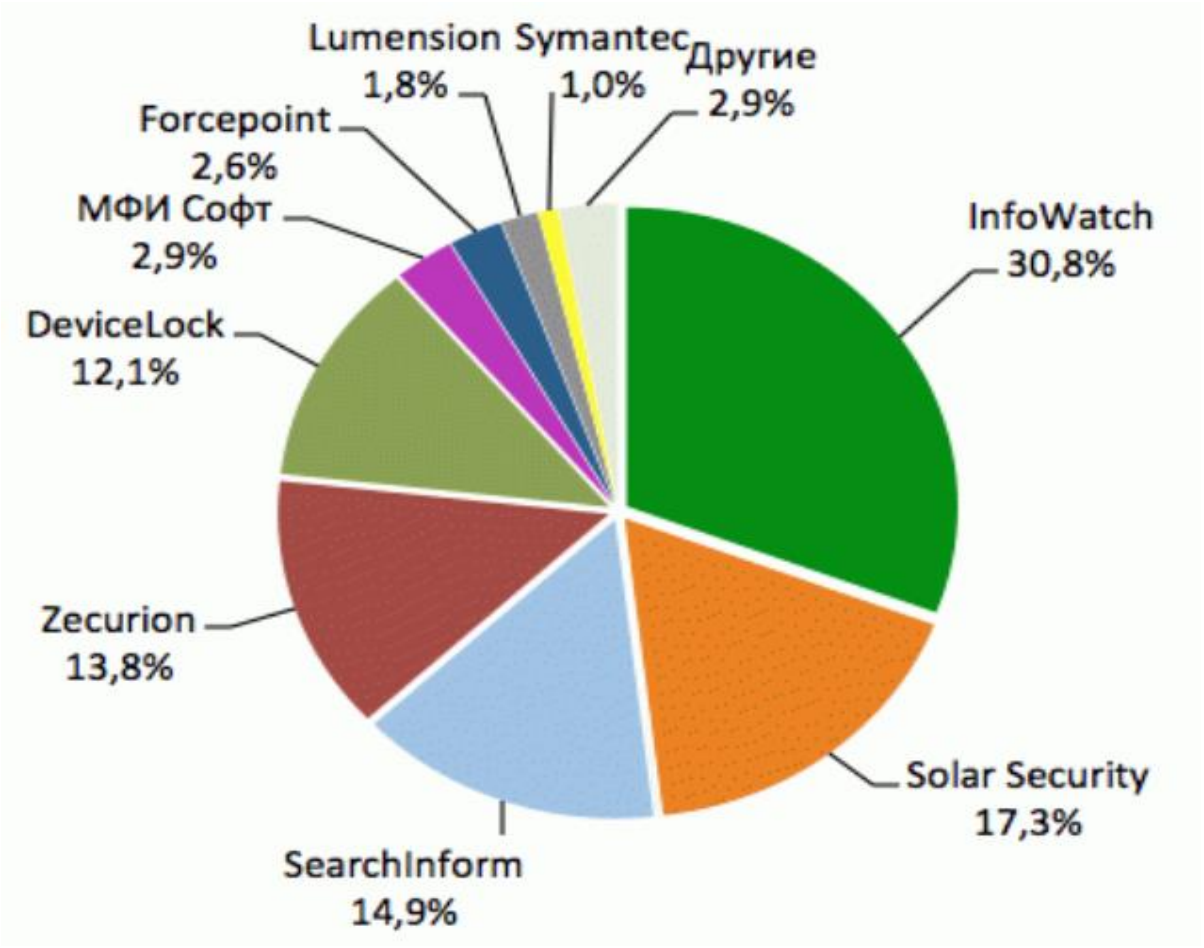

Рис. 9.1. Отечественные компании-производители DLP-систем

Мы в нашей лекции будем говорить о DLP SecureTower 6.0 компании Falcongaze, как о типичном представителе систем этого класса. Заметим, что сама компания Falcongaze существует с 2007 года и заняла достойное место среди компаний, разрабатывающих DLP-системы. Область этой и ей подобных DLP-систем вышла за границы только лишь предотвращения утечки данных.

SecureTower 6.0 позволяет осуществлять мониторинг множества каналов передачи данных (электронная почта, мессенджеры, социальные сети, облачные хранилища), перехватывать или блокировать передачу информации на периферийные устройства (USB, принтеры и другие), контролировать мобильные компьютеры, смартфоны и планшеты, осуществляя сбор информации о работе сотрудников и т. д.

SecureTower помогает не только оперативно расследовать инциденты по горячим следам, но и своевременно предотвращать их.

Выше мы определили назначение DLP-систем. Опишем основные функции, которым соответствует DLP-система, отвечающая этому назначению, на примере SecureTower 6.0. К числу основных функций относятся:

— *полный контроль документооборота и перехват данных в информационных каналах*. Система осуществляет перехват всех отправляемых и получаемых сообщений, выявление отправки конфиденциальных документов, контроль принтеров и подключаемых устройств (например, USB-устройств), контроль почтовых серверов, контроль мессенджеров, контроль использования облачных хранилищ. Гибкая система создания правил безопасности и многое другое;

— *контроль действий персонала*. В системе предусмотрен граф-анализатор, в котором для каждого сотрудника система создает профайл, который умеет импортировать данные как из Active Directory, так и формировать автоматически из перехваченной информации. В этом профайле отображаются коммуникации сотрудника с другими людьми, адреса электронной почты работника, имена в мессенджерах, аккаунты в социальных сетях и на других сайтах. Кроме того, ведется постоянный веб-контроль за посещенными сайтами и за активностью в социальных сетях. Есть возможность получать профайлы и полную историю коммуникации работников;

— *выявление передачи конфиденциальной информации с помощью различных методов анализа*. Метод контроля по цифровым отпечаткам позволяет выявлять в информационном потоке совпадения (даже фрагментарные) с конфиденциальными документами. Также SecureTower позволяет выявлять в документах и переписке регулярные выражения (такие как номера кредитных карт, ИНН, паспортные данные и др.) и осуществлять анализ по тематическим словарям. Во время анализа система учитывает морфологические особенности русского языка, распознает транслитерацию, определяет «замаскированный» формат файлов, а также анализирует текст, распознанный на изображениях;

— *сбор данных для расследования инцидентов*. Помимо предотвращения инцидентов безопасности, система используется и как средство для расследования причин и обстоятельств утечки данных. В SecureTower 6.0 предусмотрены все необходимые инструменты для расследования инцидентов по горячим следам. За счет того, что система хранит в архиве все коммуникации и действия сотрудников, это позволяет в кратчайшие сроки выявить виновного в утечке, определить наличие умысла, а также определить дальнейшие действия руководства. Собранные системой данные могут приниматься судами в качестве доказательной базы;

— *контроль мобильных рабочих станций*. В SecureTower 6.0 реализован метод удаленного контроля рабочих станций. Агент в автономном режиме снимает те же данные, что и в стационарных компьютерах, а после подключения устройства к корпоративной сети отправляет собранный архив на сервер;

— *гибкая система формирования отчетности*. Для сотрудников службы безопасности и руководителей структурных подразделений доступны полностью настраиваемые отчеты по инцидентам безопасности и ежедневной работе сотрудников. Можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту.

SecureTower 6.0 позволяет осуществлять автоматическую репликацию данных из филиалов на центральный сервер в головном офисе, что упрощает большим организациям с распределенной структурой обработку и хранение перехватываемой информации.

Для организаций, занимающихся проектной и производственной деятельностью (например, научно-исследовательские центры), критичным требованием к DLP-системам является поддержка анализа чертежной документации. SecureTower 6.0 умеет перехватывать и анализировать на предмет передачи конфиденциальных данных файлы САПР-программ в формате DWG и DXF, с которыми работают инженеры и проектировщики.

Система SecureTower 6.0 поддерживает несколько способов организации перехвата трафика в сети организации. Перехват на базе системы SecureTower может быть реализован как одним из приведенных ниже способов в отдельности, так и их комбинацией:

— перехват агентами, установленными на рабочие станции пользователей (80 % перехватов);

— централизованный перехват сетевого трафика путем его зеркалирования на SPAN-порт[1] сетевого коммутатора;

— перехват электронной почты, передаваемой через почтовые серверы;

— перехват HTTP(S)-трафика, передаваемого через прокси-серверы.

При выборе способа перехвата необходимо учитывать, что централизованно может перехватываться только трафик, передаваемый по нешифрованным протоколам, в то время, как агенты, установленные на рабочих станциях, могут перехватывать весь трафик, как не-

[1] SPAN — Switch Port Analyzer (порт анализа).

шифрованный, так и шифрованный. Перехват осуществляется по протоколам, использующим SSL-шифрование: HTTPS, FTPS, SMTPS, POP3S, IMAP4S, протоколы мессенджеров Skype, Telegram, Microsoft Lync, Viber, Google Hangouts, WhatsApp, а также SIP. Также агенты перехватывают данные, передаваемые на внешние устройства (USB-накопители, съемные жесткие диски, карты памяти и т. д.), локальные и сетевые принтеры, содержимое буфера обмена, кейлоггеры.

С помощью агентов также осуществляется перехват данных, отправляемых во все браузерные версии облачных хранилищ, перехват данных, передаваемых с помощью приложений в облачные хранилища Dropbox, OneDrive и Яндекс.Диск, iCloud, Google Drive и Облако Mail.ru.

В SecureTower 6.0 к уже имеющимся методам выявления передачи конфиденциальных документов (лингвистический анализ документов, атрибутивный анализ, контроль по цифровым отпечаткам и другие) добавилась возможность распознавать печати на изображениях. Это обеспечивает всестороннюю защиту от утечки таких данных как договоры, соглашения, проектная документация и т. д.

SecureTower 6.0 обладает большим набором функций контроля работников организации. Помимо функций, позволяющих контролировать и перехватывать передачу конфиденциальной информации, система позволяет осуществлять контроль активности сотрудников:

— мониторинг активности пользователя (во сколько была включена/выключена рабочая станция пользователя, время активности и время простоя рабочей станции);

— мониторинг аудио- и видеопотоков с рабочих станций;

— мониторинг файловых систем;

— мониторинг посещения веб-ресурсов;

— съемка скриншотов с заданной периодичностью;

— сбор статистики по используемым приложениям;

— сбор данных кейлоггера.

Таким образом, в условиях оптимизации кадровых ресурсов руководству организации намного проще будет вычислить слабое звено — человека, который бездельничает на работе.

9.2. Архитектурные решения DLP Falcongaze SecureTower 6.0

DLP-система Falcongaze SecureTower 6.0 имеет клиентскую и серверную части. Клиентская часть содержит Консоль администратора и консоль пользователя (офицера службы безопасности) и служит в качестве графического интерфейса пользователя. Серверные компоненты могут устанавливаться на один сервер или разноситься по разным, чтобы обеспечить масштабируемость, например, при одновременном контроле большого количества сотрудников (нескольких тысяч и более). Не обязательно устанавливать все компоненты, можно установить лишь те, которые требуются для выполнения поставленных задач.

Состав серверной части

Серверная часть SecureTower 6.0 включает следующие компоненты (сервисы/модули):

— центральный сервер;
— сервер индексирования;
— сервер пользователей;
— сервер контроля агентов;
— сервер обработки почты;
— сервер сетевого трафика;
— сервер ICAP;
— сервер распознавания;
— сервер безопасности и отчетности;
— сервер журналирования событий.

На рис. 9.2 представлена схема взаимодействия компонентов SecureTower 6.0, при условии их полной установки. Поясним кратко назначение каждой из вышеперечисленных компонент.

Рис. 9.2. Схема взаимодействия компонентов DLP-системы Falcongaze SecureTower 6.0

Центральный сервер отвечает за решение целого ряда задач: авторизацию и выделение лицензий компонентам программы, обработку и сохранение перехваченных данных, работу с цифровыми отпечатками документов, словарями и хэшами файлов, обработку поисковых запросов и результатов поиска и многое другое. На нем происходит сбор и сохранение всех перехваченных данных, поступивших от других серверов системы, в настроенные базы данных.

Сервер индексирования отвечает за извлечение информации из сложных форматов данных и обработку документов с целью преобразовать их в формат, удобный для дальнейшего поиска. Сервер индексирования также выполняет функции поиска по перехваченным данным, поиск по банкам цифровых отпечатков и словарям. Поисковые запросы, обработанные Центральным сервером, поступают Серверу индексирования, который осуществляет поисковые операции по файлам поискового индекса и возвращает результаты поиска Центральному серверу.

Сервер пользователей позволяет управлять данными о пользователях локальной сети, создавать карточки пользователей (имя и фамилия, должность, адреса электронной почты, UIN для ICQ, учетные записи в коммуникационных программах, IP-адреса и т. д.), объединять пользователей по определенным группам, а также отвечает за аутентификацию пользователей при доступе в систему.

Сервер контроля агентов позволяет централизовано осуществлять установку и управлять агентами. Сервер проверяет наличие рабочих станций в сети и, в зависимости от выбранной стратегии установки, производит удаленную установку агентов на компьютеры локальной сети незаметно для их пользователей. Информация, перехваченная агентами, перенаправляется на Центральный сервер для сохранения в базу данных.

Сами агенты контроля рабочих станций — независимые программные модули. Они предназначены для перехвата данных, передаваемых через Skype, Viber, Microsoft Lync, SIP или отправляемых по SSL-протоколу, и дальнейшей их передачи серверу для обработки.

Одной из интересных функций агентов является контроль активности пользователей, с ним можно осуществлять периодическое снятие скриншотов, сбор статистики по активности приложений, мониторинг файловых систем и аудио- и видеопотоков и т. д. Говоря простыми словами, агенты позволяют следить, чем занимается пользователь на своем рабочем месте.

Сервер обработки почты обеспечивает перехват почты, отправляемой через почтовые серверы, развернутые на базе MS Exchange Server, Postfix, Lotus и другого программного обеспечения. Интеграция с почтовыми серверами может осуществляться по протоколам POP3 или SMTP.

Сервер сетевого трафика обеспечивает перехват и анализ трафика сетевых портов, специально выделенных для этой цели (так называемых SPAN-портов, или портов зеркалирования). Все перехва-

ченные данные (электронные письма, файлы, сообщения и т. д.) передаются Центральному серверу для сохранения.

Сервер ICAP позволяет настроить параметры интеграции SecureTower с прокси-сервером для перехвата и блокирования данных, переданных по протоколам HTTP и HTTPs.

Сервер распознавания выполняет распознавание и анализ текстовой составляющей на изображении (сканированные копии документов в любом из графических форматов, DjVu и PDF-документы, изображения с текстовыми полями) и применяет к перехваченным данным настроенные политики безопасности. При обнаружении файлов сканированных копий документов, которые содержат изображения печатей, внесенных в банк эталонов Центрального сервера, также будут применены соответствующие политики безопасности.

Сервер безопасности и отчетности состоит из двух компонентов — Центр безопасности и Центр отчетности.

Центр безопасности отвечает за обработку правил безопасности. При обнаружении каких-либо данных, отвечающих требованиям правил безопасности, Центр безопасности автоматически отправляет уведомления на указанный адрес электронной почты и отображает информацию об обнаружении в Консоли пользователя.

Центр отчетности отвечает за создание статистических отчетов по широкому спектру параметров перехваченных данных. Все отчеты доступны для настройки и просмотра в Консоли пользователя. Отчеты представляются в графическом виде и обладают высокой степенью интерактивности.

Сервер журналирования событий позволяет контролировать состояние системы в режиме реального времени. При этом все события серверных компонентов фиксируются в журнале серверных событий SecureTower. Также обеспечивается запись сведений обо всех наиболее существенных событиях в работе серверных компонентов SecureTower в журнал ОС рабочей станции, на которой они установлены.

Консоль администратора предназначена для настройки работы всех подсистем SecureTower 6.0. С помощью нее настраиваются все компоненты, устанавливаются агенты системы, настраивается фильтрация данных при перехвате, устанавливается периодичность индексирования данных, просматривается статистика перехвата трафика в режиме реального времени, а также решаются задачи, которые необходимо выполнять администратору DLP-системы.

Консоль пользователя — основное графическое приложение, предназначенное для работы офицера службы безопасности. Здесь

осуществляется непосредственно работа с перехваченной информацией. Консоль позволяет анализировать трафик конкретных пользователей, осуществлять полнотекстовый поиск, по ключевым словам, и просматривать перехваченные данные в удобном виде. В консоли производится настройка работы Центра безопасности и просмотра результатов его работы, а также настройка отправки уведомлений о нарушении политики информационной безопасности. Кроме того, с помощью консоли обеспечивается доступ к Центру отчетности для автоматического построения отчетов по различным критериям, доступ к прослушиванию аудио- и видеопотока, и видеоизображения рабочего стола в режиме реального времени.

Особенность организации перехвата сетевого трафика в SecureTower 6.0

Схемы внедрения системы перехвата на базе «Сервера сетевого трафика» в SecureTower 6.0 могут быть различными и все зависит от топологии сети организации. Рекомендуемая схема внедрения системы перехвата на базе «Сервера сетевого трафика» в существующую сеть приведена на рис. 9.3.

Рис. 9.3. Рекомендуемая схема внедрения системы перехвата на базе Сервера сетевого трафика SecureTower 6.0

При использовании такой схемы перехватываться будет весь внешний сетевой трафик. Данная схема обеспечивает оптимальное распределение функций всех подсистем SecureTower 6.0 по сети, а также позволяет избежать дополнительной нагрузки на Сервер сетевого трафика.

Перехват между сегментами сети. Масштабирование системы

Одной из новых особенностей SecureTower 6.0 является масштабирование (рис. 9.3).

Возможность масштабирования системы перехвата позволяет избежать перегрузки системы при мониторинге сетей со сложной топологией и большим числом рабочих станций. Нагрузка по перехвату и обработке трафика распределяется по нескольким Серверам сетевого трафика, что позволит контролировать трафик, передаваемый между локальными рабочими станциями большой сети, и в целом повышать надежность и производительность системы перехвата.

DLP-система может быть развернута, как в крупных организациях с территориально распределенной структурой, так и в небольших организациях. Все компоненты SecureTower 6.0 могут быть установлены на один сервер или разнесены по разным, чтобы обеспечить нужную масштабируемость при одновременном контроле большого количества сотрудников (нескольких тысяч и более).

Системные требования для серверных компонентов Falcongaze SecureTower 6.0

Общим требованием для установки всех серверных компонентов является поддержка ОС Microsoft Windows Server 2008/2012/2016 (x64). Серверные компоненты Falcongaze SecureTower начиная с версии 6.0 не могут быть установлены на рабочие станции под управлением 32-разрядных ОС.

SecureTower 6.0 поддерживает работу с наиболее популярными СУБД. Среди поддерживаемых систем как платные продукты Microsoft SQL и Oracle SQL, так и open-source: PostgreSQL (9.3 и выше), MySQL, SQLite.

В комплект поставки включена СУБД SQLite. А рекомендуемой СУБД является PostgreSQL, которую следует размещать на том же физическом сервере, где расположен Сервер индексирования. Однако при использовании других СУБД или контроле более чем 1,5 тысяч пользователей и сроках хранения информации более полугода необходимо использовать высокопроизводительные системы хранения данных. Минимальные системные требования для серверных компо-

нентов Falcongaze SecureTower 6.0 для контроля 25 пользователей приведены в таблице 9.1.

Таблица 9.1

Системные требования для серверных компонентов SecureTower 6.0

Компонент	Минимальные системные требования	Рекомендации по установке
Серверное оборудование	CPU: 2,2 ГГц и выше (4 ядра и более); Сетевой адаптер: 1 Гбит (2 адаптера при централизованном перехвате); RAM: 6 ГБ и более; HDD: 100 ГБ раздел для ОС и файлов SecureTower (RAID1/RAID10); раздел для хранения перехваченных данных (на RAID1/RAID10) из расчета: 1,5 ГБ данных от каждого контролируемого пользователя за месяц, плюс 3 % от объема перехваченных данных для файлов поисковых индексов; Предустановленные компоненты: Windows.Net Framework 4.6 и выше, Microsoft Visual C++ Redistributable 2008/2010/2013 и 2015 (x86/x64); ОС: Microsoft Windows Server 2008/2012/2016 (x64)	Центральный сервер и Сервер индексирования рекомендуется установить на отдельные серверы. Сервер контроля агентов может работать вне зависимости от наличия остальных компонентов системы. Для его работы достаточно настроить подключение к базе данных. Сервер сетевого трафика устанавливается с помощью отдельного мастера установки. Основной рекомендацией является выделение отдельного сервера (или нескольких серверов) для его установки
Агент контроля рабочих станций	ОС: Microsoft Windows XP SP3/Vista/7/8/10/Server 2003/2008/2012/2016 (x86/x64)	–

Системные требования для клиентских компонентов Falcongaze SecureTower 6.0

Клиентские компоненты SecureTower 6.0 (Консоль администратора и Консоль пользователя) могут быть установлены на любых рабочих станциях сети, которые удовлетворяют системным требованиям, приведенным в таблице 9.2.

Таблица 9.2

Системные требования для клиентских компонентов Falcongaze SecureTower 6.0

Компонент	Минимальные системные требования	Рекомендации по установке
Консоль администратора и Консоль пользователя	CPU: 2 ГГц и выше; Сетевой адаптер: 100 Мбит/1 Гбит; RAM: не менее 4 ГБ; HDD: не менее 300 МБ; Windows .Net Framework: 4.6 и выше; Microsoft Visual C++ Redistributable 2008/2010/2013/ 2015 (x86/x64); Видеокарта: поддержка DirectX 7.0 и выше (разрешение экрана: 1024 x 768); ОС: Microsoft Windows Vista/7/8/10/2008/2012/2016 (x86/x64)	Клиентские компоненты могут быть установлены на любых рабочих станциях сети (стационарные или мобильные рабочие станции)

9.3. Сертификация и соответствие требованиям регуляторов

DLP-система SecureTower сертифицирована ФСТЭК (Сертификат ФСТЭК № 3421 от 25.06.2015). SecureTower является программным средством защиты от неправомерной передачи информации из ИС и соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Соответствует четвертому уровню контроля отсутствия недекларированных возможностей.

Применение DLP-системы SecureTower 6.0 позволяет компаниям соответствовать требованиям нормативных правовых актов Российской Федерации и отраслевых стандартов в области обеспечения информационной безопасности, таких как:

— Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

— Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

— Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

— Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»;

— Положение Банка России от 9 июня 2012 г. № 382-П «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;

— Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;

— ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

9.4. Методика реализации функциональных возможностей

Работа с DLP-системой SecureTower 6.0 интуитивно понятна и не требует специальных дополнительных знаний. Системному администратору и администратору информационной безопасности организации не составит труда установить и настроить систему, как им необходимо. Рассмотрим ряд наиболее востребованных функций.

Аудио- и видеомониторинг

Одним из нововведений является осуществление не только аудио-, но и видеомониторинга. Теперь можно не только мониторить аудиосигнал с рабочей станции, но и удаленно просматривать видеоизображение происходящего на экране монитора пользователя или видеоизображение, поступающее с подключенной к компьютеру веб-камеры. При этом перехватывается видеопоток с экранов всех мониторов, подключенных к контролируемой рабочей станции.

Воспроизведение результатов записи доступно напрямую из Консоли пользователя SecureTower 6.0 в окне модуля «Аудио- и видеомониторинг» (рис. 9.4).

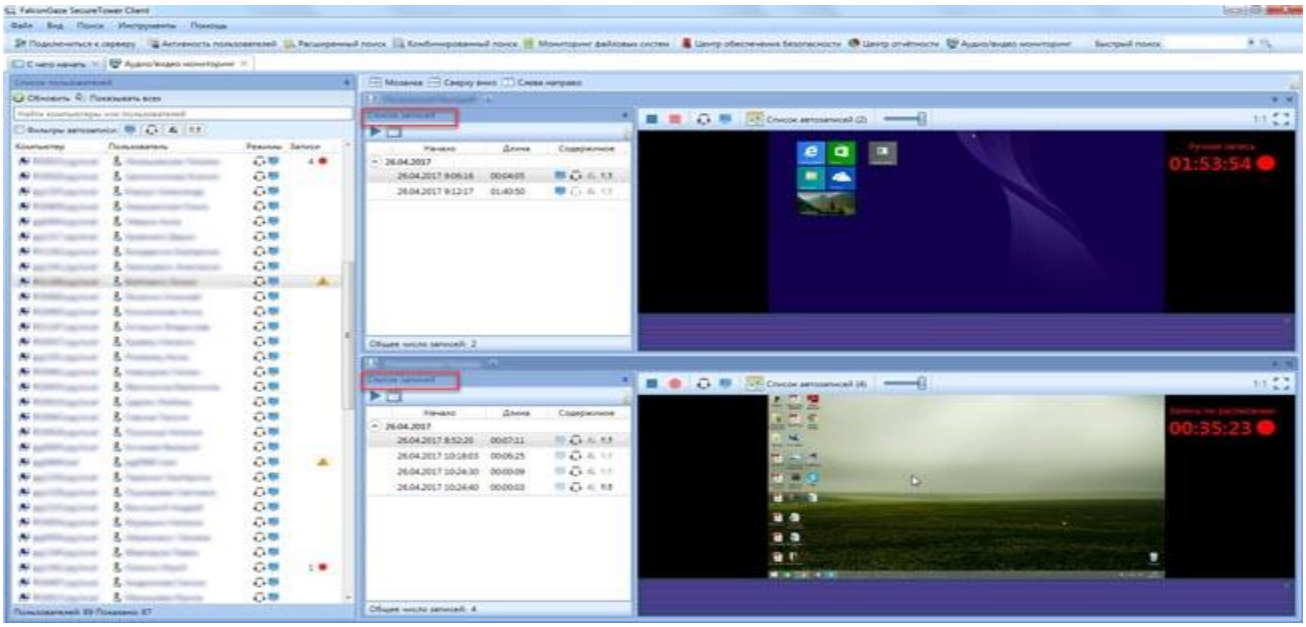

Рис. 9.4. Просмотр результатов аудио- и видеомониторинга в SecureTower 6.0

При этом можно настраивать автоматическую запись по расписанию (рис. 9.5).

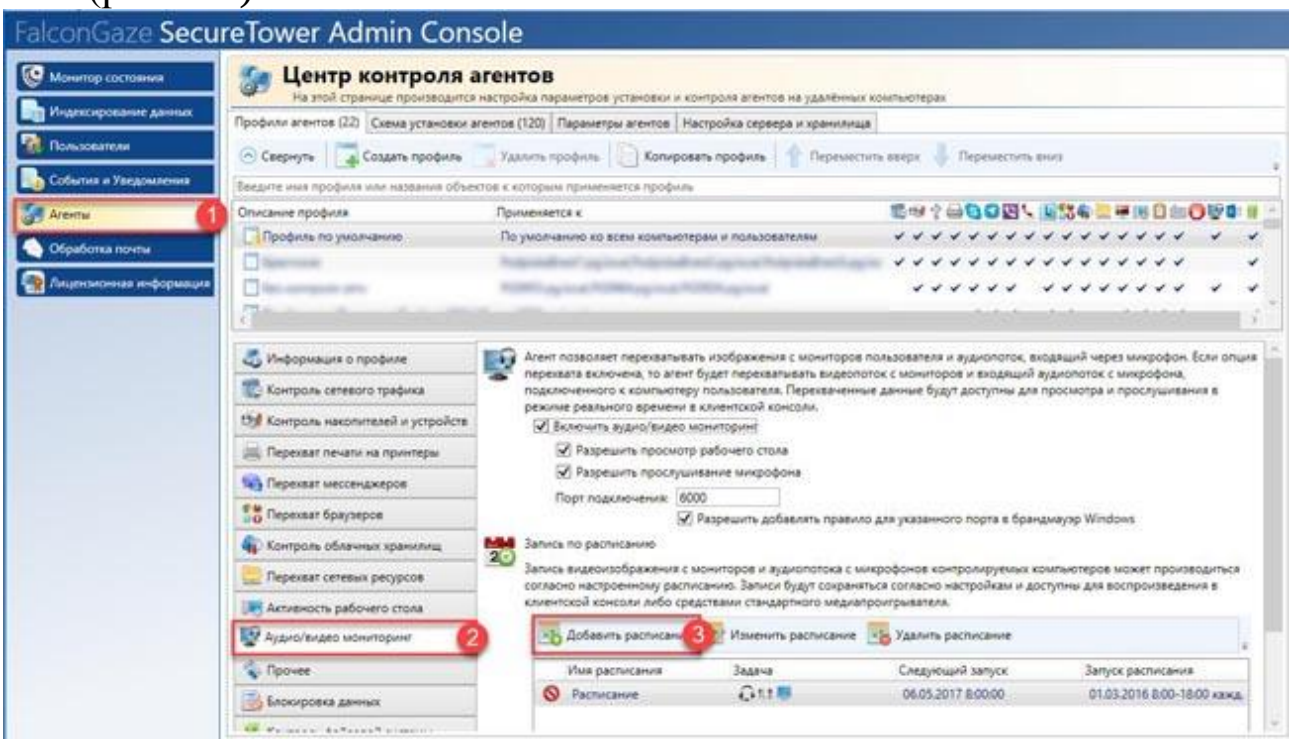

Рис. 9.5. Настройка автоматической записи результатов мониторинга аудио и видео в SecureTower 6.0

Функция аудио- и видеомониторинга позволяет просматривать, чем сотрудник занимается на своем рабочем месте, о чем и с кем ведет переговоры. В современных условиях перехват данных через такой канал связи широко используется в большинстве организаций (например, через такие приложения, как Skype, Viber, WhatsApp и др.) при общении с клиентами и заказчиками, т. к. позволяет в кратчайшие сроки уточнить информацию, сформировать заказ и т. д.

Например, сотрудник организации в разговоре с клиентом может договориться об откате. Рассмотрим еще такую ситуацию: сотрудник знает о том, что он не может скопировать и переслать конфиденциальный документ, при этом он осуществляет видеозвонок заинтересованным лицам и показывает в видеотрансляции снимок экрана своего монитора, на котором открыт такой документ. Теперь система SecureTower 6.0 позволяет отслеживать и такую возможность утечки конфиденциальной информации.

Возможность распознавания печатей на изображениях

Новая версия системы SecureTower 6.0 помимо распознавания текста на изображениях позволяет отслеживать передачу файлов, содержащих отсканированные копии документов с печатями установленного образца, и отправлять уведомление уполномоченному лицу о факте перехвата такого документа. Такая функция помогает отследить и перехватить неправомерную передачу, например, договоров, конструкторской документации, документов с пометкой «Для служебного пользования» и других завизированных печатью документов.

Настройка распознавания печатей на изображениях и добавление эталонных образцов печатей выполняется в Консоли администратора на вкладке Распознавание (рис. 9.6). Для работы данной функции необходимо добавить образцы печатей, которые недопустимы для передачи. Система поддерживает перехват печатей в том числе в документах XPS-формата.

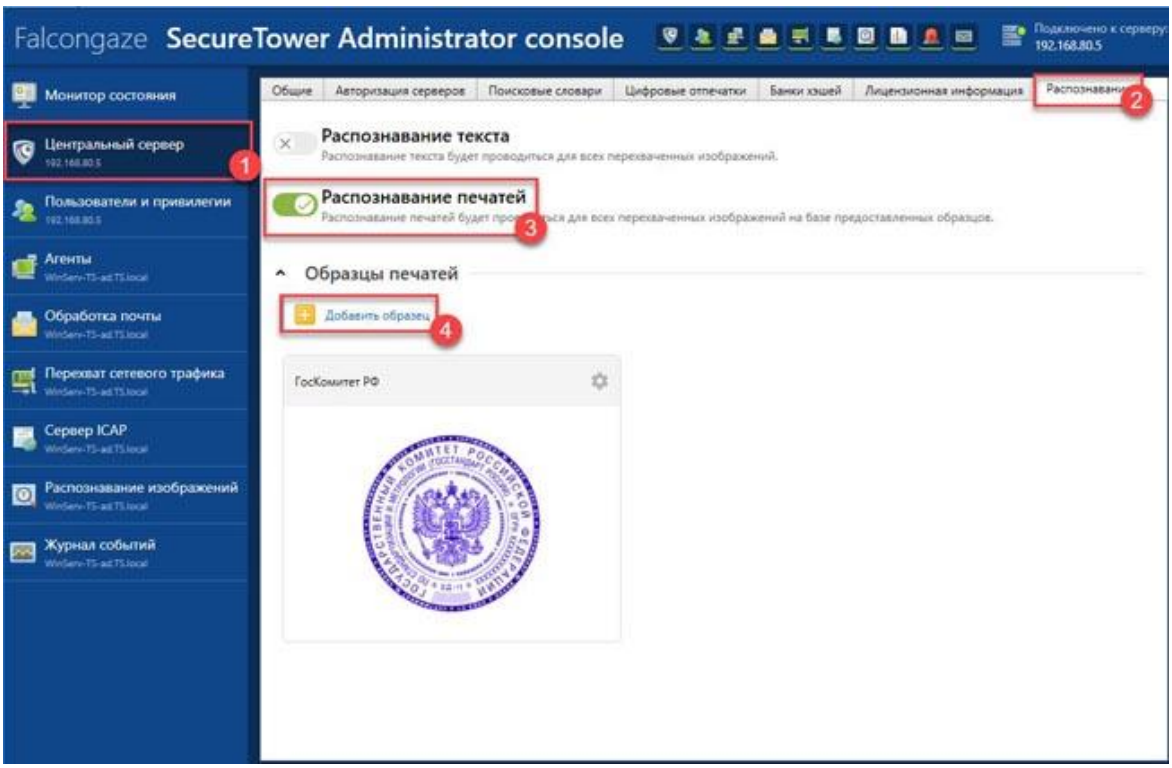

Рис. 9.6. Настройка функции Распознавание печатей в SecureTower 6.0

Можно также настроить правило безопасности, в рамках которого осуществлялись бы автоматические уведомления уполномоченных лиц о случаях обнаружения документов с печатями в Центре обеспечения безопасности Консоли пользователя. Настройка уведомления приведена на рис. 9.7.

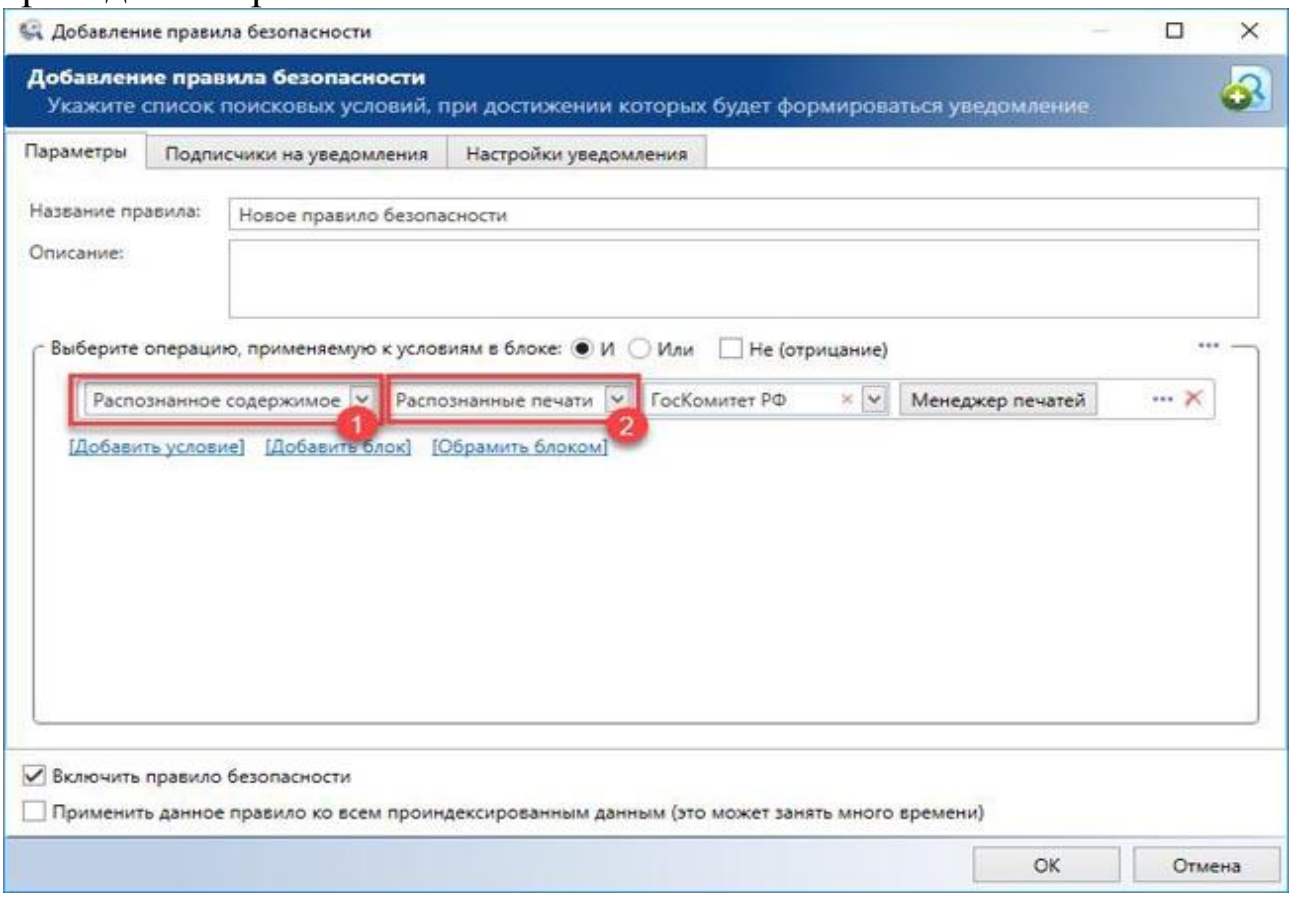

Рис. 9.7. Настройка автоматического уведомления о случаях обнаружения документов с печатями в SecureTower 6.0

Может потребоваться отследить, кому передаются те или иные документы. В этом случае мы настраиваем правило отслеживать документы с теми или иными печатями, но не запрещаем их передачу. Для отслеживания, кому и кто передавал такие документы, поиск документов с распознанными печатями осуществляется в Консоли пользователя с помощью модуля Комбинированного поиска (настройки поиска см. рис. 9.8).

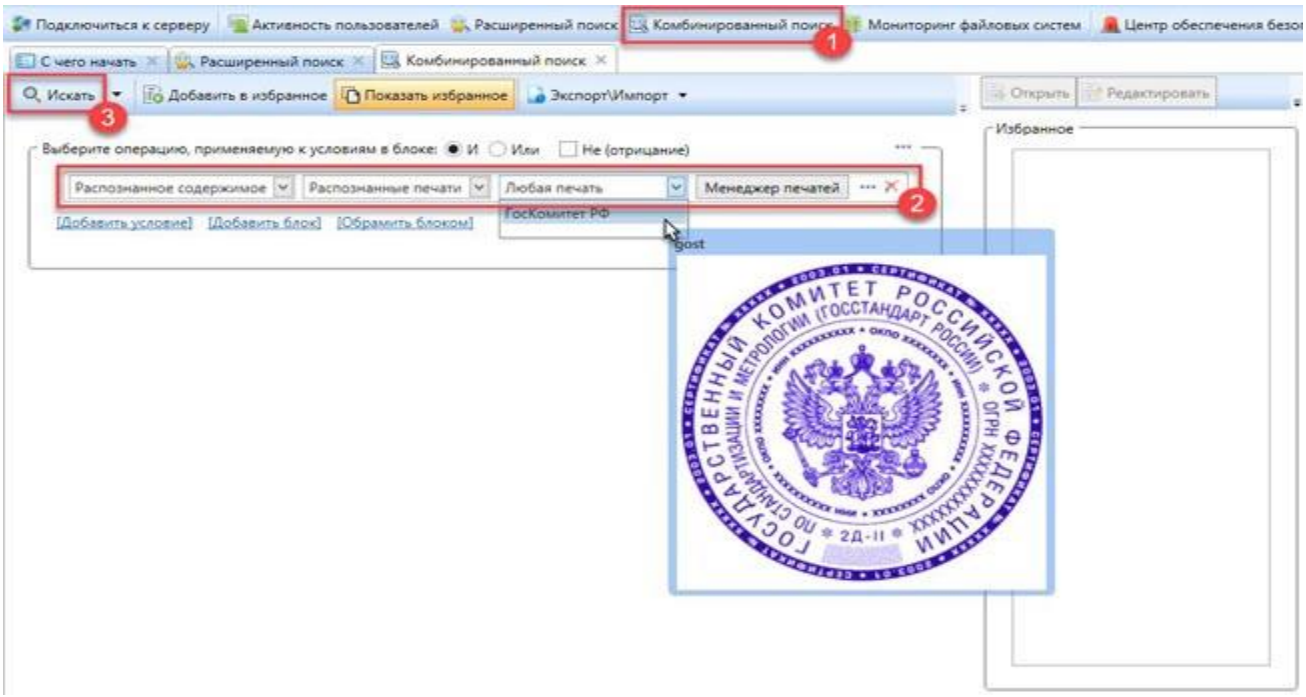

Рис. 9.8. Настройка поиска документов с распознанными печатями в SecureTower 6.0

Контроль облачных хранилищ

В настоящее время широко распространена возможность использования облачных хранилищ. Раньше, чтобы скопировать документ (по сути, украсть), необходимо было записать его на оптический диск или USB-носитель. Такая возможность в большинстве организаций была запрещена с помощью систем предотвращения утечки информации через периферийные устройства или системы защиты от несанкционированного доступа, имеющих функцию запрета использования периферийных устройств. Теперь пользователю достаточно иметь доступ в интернет и к облачному хранилищу.

Система SecureTower позволяет пресечь и эту возможность, при этом список контролируемых облачных хранилищ постоянно растет. Мы уже говорили, что в SecureTower 6.0 добавилась возможность контролировать еще и Google Drive, Apple iCloud, Облако Mail.Ru. При этом доступ к облачным хранилищам можно настраивать, т. е. можно запретить совсем, разрешить или оставить доступ только на чтение (рис. 9.9).

Рис. 9.9. Настройка доступа к облачным хранилищам в SecureTower 6.0

Настройка контроля облачных хранилищ осуществляется в Консоли администратора в профиле настроек агента на вкладке Контроль облачных хранилищ (рис. 9.10).

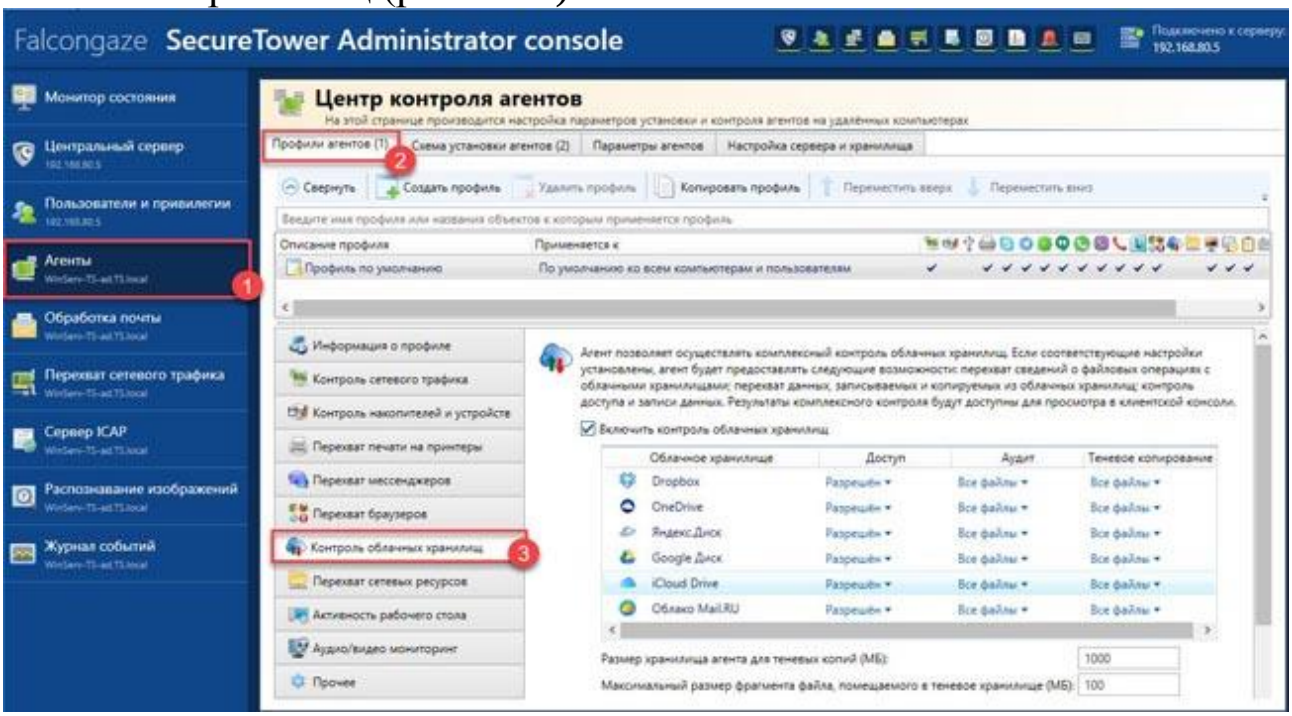

Рис. 9.10. Настройка контроля облачных хранилищ в SecureTower 6.0

Перехват информации осуществляется путем теневого копирования данных, передаваемых в облачные хранилища. В дальнейшем можно будет просмотреть информацию о дате и времени перехвата данных, имени и размере файла, имени локального пользователя, произведшего запись файла в облачное хранилище, путь к переданному файлу в локальной папке облачного хранилища и т. д.

Таким образом, система SecureTower 6.0 позволяет контролировать доступ и осуществлять перехват информации, передаваемой в самые распространенные облачные хранилища.

Контроль мессенджеров

Количество появляющихся на рынке и используемых в современном мире мессенджеров постоянно растет. И зачастую очень сложно

отследить информацию, передаваемую через них. SecureTower 6.0 позволяет осуществлять перехват данных в наиболее популярных мессенджерах (Skype, WhatsApp, Google Hangouts, Telegram, Viber и др.). Для этого в Консоли администратора в профиле настроек агента на вкладке Перехват мессенджеров можно установить, по каким мессенджерам требуется перехватывать информацию (рис. 9.11).

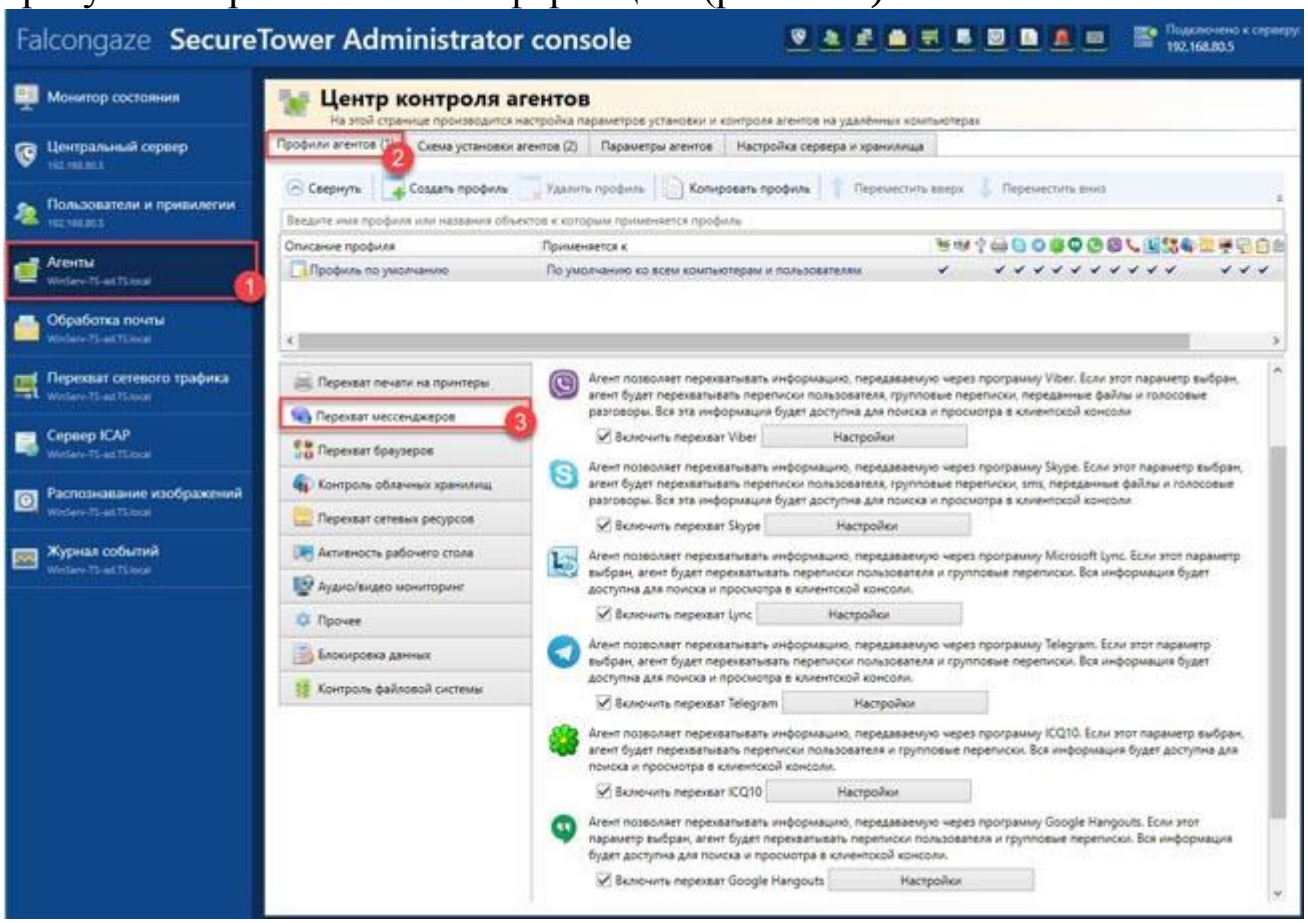

Рис. 9.11. Настройка контроля мессенджеров в SecureTower 6.0

SecureTower 6.0 позволяет осуществлять перехват (как переписки, так и передаваемых файлов) для следующих мессенджеров: ICQ (протокол OSCAR), Skype, WhatsApp, Google Hangouts, Telegram, SIP, Viber, Microsoft Lync, XMPP (Jabber), Mail.Ru Агент, Yahoo.

Мы познакомились с предпоследней по времени версией DLP-системы Falcongaze SecureTower (в 2019 году вышла обновленная версия DLP-версия 6.2. Однако по функциональности она лишь незначительно отличается от версии 6.0. А поскольку в большинстве организаций действующей остается версия 6.0, то целесообразно было ознакомиться именно с этой версией). По заявлениям разработчиков, это не просто обновление, а совершенно новый продукт. И это действительно так, ведь Falcongaze в SecureTower 6.0 кардинально переработали архитектуру системы. Компания Falcongaze динамично

развивает и совершенствует свою систему, что является немаловажным фактором при выборе.

Для превентивного устранения утечек и вредоносной инсайдерской активности в SecureTower 6.0 реализован перехват максимально возможного количества каналов связи: электронная почта, веб-активность, USB-носители, принтеры, а также мессенджеры и облачные сервисы. Возможности перехвата постоянно увеличиваются разработчиками, ориентированными на требования рынка. SecureTower 6.0 позволяет не только предотвращать инциденты, но и оперативно их расследовать.

В SecureTower 6.0 применяются две схемы перехвата — на шлюзе и с помощью агентов. В первом случае решение анализирует трафик на сервере, во втором перехват происходит непосредственно на рабочих компьютерах. Второй способ перехвата позволяет значительно расширить количество перехватываемых каналов, в том числе большинство мессенджеров и интернет-трафик по протоколу HTTPs. В зависимости от нужд организации способы перехвата могут комбинироваться, либо вообще использоваться только определенные модули системы. Также возможны работа системы на корпоративном почтовом сервере и интеграция с корпоративным Proxy-сервером.

Анализ перехваченных данных происходит на основе заранее заданных правил безопасности. При этом в SecureTower 6.0 предусмотрена возможность достаточно гибкой настройки правил. Например, можно создать правила — уведомлять о передаче большого числа файлов на печать сотрудниками определенного отдела или блокировать передачу по электронной почте документа, содержащего данные из базы данных конфиденциальных документов. Все уведомления о событиях отправляются ответственному лицу.

Система SecureTower 6.0 имеет так много достоинств, что может сложиться мнение, что у нее нет недостатков. Но недостатки есть. В частности, SecureTower 6.0 работает на серверах и компьютерах только под управлением ОС Windows. Конечно, большая часть организаций использует именно эту ОС, но разработчикам есть куда стремиться для расширения рынка. Еще одним недостатком является отсутствие функции агентского контроля мобильных устройств под управлением Android, iOS и мобильной версии Windows, востребованность которого вызывает сомнения, однако встречается все чаще.

Достоинства SecureTower 6.0:

— система отечественного производителя, который динамично развивает ее функциональность;

— внедрение SecureTower 6.0 занимает считанные часы, а установка и настройка производится из одной консоли. Для внедрения не требуется дорогостоящий консалтинг и покупка специального оборудования;

— масштабируемость и модульность системы;

— высокая скорость анализа данных при перехвате;

— возможность контроля облачного хранилища;

— возможность контроля мессенджеров Skype, Telegram, Microsoft Lync, Viber, Google Hangouts, WhatsApp, ICQ с включенным шифрованием протокола;

— поддержка файлов проектных данных САПР-программ (DWG и DXF) (контроль бинарных документов);

— распознавание текста и печатей на изображениях;

— полный контроль документооборота и перехват данных в информационных каналах;

— контроль за действиями персонала;

— осуществление аудио- и видеомониторинга;

— построение подробных отчетов о действиях и коммуникациях пользователей. В том числе формирование отчетов в графическом виде, а также построение граф-анализаторов действий пользователя;

— выявления передачи конфиденциальной информации по цифровым отпечаткам;

— контроль мобильных рабочих станций;

— интуитивно понятный интерфейс и гибкие настройки системы;

— собираемый объем данных позволяет оперативно осуществлять расследование инцидентов.

Недостатки SecureTower 6.0:

— поддержка только ОС на базе Windows;

— отсутствие агентов для мобильных устройств (смартфоны, планшеты);

— отсутствие готовой (из коробки) интеграции с другими продуктами по обеспечению информационной безопасности.

Контрольные вопросы:

1. Расскажите об основных функциях и способах перехвата информации Falcongaze Secure Tower.
2. На чем основывается архитектурное решение Falcongaze Secure Tower 6.0?
3. Сертификация и соответствие требованиям регуляторов.
4. Методика реализации функциональных возможностей.

Лекция 10. Методология экспертного оценивания программ и данных

Вопросы лекции:

10.1. Общая методология компьютерно-технической экспертизы.

10.2. Типичные правовые ошибки при выполнении компьютерно-технической экспертизы.

10.3. Особенности экспертизы программного обеспечения.

10.4. Примеры проявления недокументированных функций программного обеспечения.

Любое экспертное исследование компьютера преследует определенную цель и для ее достижения решает определенные задачи. Большинство задач касается ответов на вопросы о программном обеспечении компьютера и данных, которые в нем находятся. На эти вопросы обычно отвечает компьютерно-техническая экспертиза. Эта экспертиза, как правило, проводится с изъятыми компьютерами в экспертных учреждениях. В данной лекции приведена методология изъятия компьютера на объекте и экспертного оценивания программ и данных в экспертном учреждении.

10.1. Общая методология компьютерно-технической экспертизы

Известно множество программ, которое может помочь в проведении компьютерно-технической экспертизы. Отметим среди них набор утилит Windows Sysinternals (http://go.microsoft.com/?linkId=6013253), используемых для исследования компьютеров на базе ОС Windows. Большую пользу могут также принести внутренние команды и инструментальные средства Windows. Аналогичные по назначению программы существуют и для экспертизы компьютеров с другими ОС, например, с ОС Linux. Кроме того, для исследования программ широкое применение находят отладчики программ и дизассемблеры, переводящие исполняемые файлы программ в программы на языке высокого уровня.

Методология изъятия компьютера на объекте

Все компьютерные средства, обнаруженные в ходе следственного действия и имеющие значение для дела, должны быть изъяты в соответствии с требованиями закона (ст.ст. 164, 165, 177, 182, 183 УПК РФ), чтобы впоследствии они могли быть признаны доказательствами.

Типичными изымаемыми объектами являются системные блоки и все обнаруженные носители компьютерной информации. Однако

специалист в каждом конкретном случае, исходя из сложившихся обстоятельств, должен помочь определить перечень изымаемых объектов, в т. ч. периферийных устройств (мониторы, принтеры, факс-модемы и пр.), устройств для доступа к обнаруженным носителям, сетевого оборудования, кабелей и пр. Данный выбор должен быть сделан с позиций всестороннего обеспечения производства судебной экспертизы, которая будет впоследствии назначена следователем.

В протоколе следственного действия описываются место и время изъятия компьютерных средств, основные физические характеристики изымаемых устройств, их видимые индивидуальные признаки, конфигурация компьютерных средств (их комплектация); номера моделей и серийные номера каждого из устройств; инвентарные номера, присваиваемые бухгалтерией при постановке средства на баланс организации; иную информацию, имеющуюся на фабричных ярлыках фирмы-изготовителя.

Все изъятые системные блоки компьютеров и другие устройства (в т. ч. носители) должны быть упакованы и опечатаны. Причем, это должно быть выполнено таким образом, чтобы исключить возможность их повреждения, включения в сеть и разборки. Например, системные блоки компьютеров должны быть пронумерованы, а все их разъемы опечатаны. Следует пронумеровать и все носители информации, пакеты, в которые они запакованы, проставить опознавательные знаки на бумажных аналогах информации (при наличии таковых). Изымаемые жесткие диски упаковываются в металлизированную упаковку, исключающую влияние полей. Все действия должны быть зафиксированы в протоколе.

В необходимых случаях изъятие компьютерной техники осуществляется в присутствии эксперта, который будет проводить экспертизу. Эксперт может помочь в правильной организации процессуального действия, чтобы упростить дальнейшие свои задачи и не потерять доказательную силу будущих выводов. Для этого в процессе изъятия по возможности нужно придерживаться следующего:

— записать данные лиц, находящихся в помещении на момент появления группы, независимо от объяснения причин их пребывания;

— составить список всех сотрудников организации, имеющих доступ к компьютерной технике либо часто пребывающих в помещении, где находятся ЭВМ;

— осмотреть документацию, обращая внимание на рабочие записи, часто именно в записях неопытных пользователей можно обнаружить коды, пароли и другую полезную информацию;

— составить список всех внештатных и временных работников с целью выявления программистов и других специалистов в области информационных технологий, работающих в учреждении. По возможности, установить их паспортные данные, адреса и места постоянной работы;

— принять меры по установлению пароля доступа к защищенным программам;

— в случае необходимости консультаций персонала организации, получать их следует у разных лиц путем опрашивания или допроса. Подобный метод позволит получить максимально правдивую информацию и избежать умышленного вреда;

— не допускать к исследуемому компьютеру владельца для оказания помощи в его эксплуатации. Известны случаи из практики США (и не только), когда подозреваемые на допросах допускались к работе на изъятом компьютере и при этом шифровали критическую информацию.

При активном вмешательстве сотрудников учреждения, стремящихся противодействовать работе группы, отключить электропитание всех компьютеров на объекте, опечатать их и изъять вместе с магнитными носителями для исследования информации в лабораторных условиях. При этом составляется соответствующий протокол.

Перед выключением компьютера по возможности закрыть все используемые на компьютере программы. Следует помнить о том, что некорректный выход из некоторых программ может вызвать уничтожение информации или испортить саму программу.

Методология исследования

Для того чтобы найденная информация могла в дальнейшем иметь доказательную силу, она не может быть подвергнута изменениям. Это один из главнейших принципов любой экспертизы.

Не всегда существенная информация доступна в виде файлов. Иногда она может быть удалена. Однако если для удаления не были использованы специальные программы типа *Wipe File*, содержимое файлов остается в свободном пространстве диска до тех пор, пока не будет перекрыто какой-либо другой информацией.

Кроме этого, некоторые программы при работе с информацией создают временные файлы, в которые эта информация может попадать.

Наконец, все действия с информацией возможны, только если она загружена в оперативную память, которая при некоторых условиях выгружается в специальные файлы на диске.

Отсюда самая первая рекомендация при исследовании компьютера — найти и сделать копии временных файлов, временных файлов сети «Интернет», а также файлов обмена с памятью (*swap*), в том числе используемых для спящего режима. В последние сохраняется образ всей используемой оперативной памяти. При загрузке с ОС исследуемого компьютера доступ к некоторым системным файлам будет ограничен даже для копирования, поэтому — если есть возможность — нужно загрузить компьютер со специально подготовленного носителя.

10.2. Типичные правовые ошибки при выполнении компьютерно-технической экспертизы

В соответствии со ст. 57 УПК РФ эксперт не вправе… проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств.

Большинство экспертов нарушают требования этой статьи немедленно в самом начале исследования — как только включают исследуемый компьютер. Применительно к компьютерной технике, эксперт обязан обеспечить неизменность содержимого жестких дисков и иных носителей информации в исследуемых компьютерах. Только при соблюдении этого условия выводы эксперта могут быть проверены при необходимости повторной экспертизой.

Большинство современных ОС, в частности *Windows Linux, MacOS* и пр. в процессе работы осуществляют запись программ и данных на жесткий диск — как минимум в файл подкачки. Если речь идет о компьютерах, используемых в криминальных целях, то на них вообще может быть установлена специальная программа для экстренного уничтожения информации в случае необходимости. При включении такого «заминированного» компьютера без особых предосторожностей содержимое его жесткого диска может измениться до такой степени, что не будет представлять уже никакой ценности для следствия и суда.

Поэтому эксперт обязан позаботиться о сохранении всех исследуемых носителей информации в неизменяемом состоянии. Эта цель может быть достигнута как технологически, так и физическими методами. Основной технологический прием — загрузка на исследуемом компьютере с внешнего носителя т. н. доверенной ОС, которая заве-

домо не производит несанкционированной записи на жесткий диск. Характерным примером такой системы могут служить, например, некоторые специальные версии *UNIX,* а также *Live-CD* — специальные загружаемые *CD*, которые размещают ОС в оперативной памяти и позволяют, например, исправить ошибки ОС диска, удалить вредоносные программы, а также исследовать диск ОС. Однако самым надежным методом является изъятие жесткого диска из исследуемого компьютера и подключение его к собственному компьютеру с загруженной там доверенной ОС.

Физически жесткий диск исследуемого компьютера может быть защищён от записи путём подключения его через специальное устройство, например, через устройство HDD&DATA. В такой (и только в такой) конфигурации допустимо загружать исследуемый компьютер в штатном режиме.

В любом случае невозможность записи на жесткий диск исследуемого компьютера существенно затрудняет процесс поиска нужной информации. Оказывается, невозможным, к примеру, восстановить стертые файлы, работать с текстовыми процессорами и СУБД, даже просто осуществлять расширенный поиск информации. Поэтому для того, чтобы произвести экспертизу за приемлемое время, эксперт должен создать файл-образ исследуемого жёсткого диска на своём компьютере либо попросту скопировать исследуемый жёсткий диск на другой. При этом недопустимо стандартное копирование файлов, поскольку не меньший интерес для эксперта представляет пространство диска, считающееся свободным. Следует использовать специальное программное обеспечение, например, *Symantec Ghost*[1], которое осуществляет посекторное копирование носителей информации.

Слабым местом такого подхода является финансирование. Для того чтобы создать на своем компьютере (или компьютерах) образ или копию исследуемого жесткого диска, эксперт должен располагать носителем информации как минимум такой же емкости. А если на экспертизу направлено несколько компьютеров, да еще сервер с *RAID*-массивом… Вот тут-то государственный эксперт и вспоминает, что проверить его заключение сможет разве что коллега из соседней комнаты. И 57-я статья приносится в жертву целесообразности. Раз такого объема свободного места просто нет, эксперт начинает работать непосредственно с жестким диском исследуемого компьютера.

[1] Программа клонирования дисков.

При этом могут быть восстановлены файлы, распакованы архивы, снят пароль с подвернувшейся базы данных… Словом, в ходе исследования происходит то самое «изменение внешнего вида или основных свойств» исследуемого объекта. Аналогичные ошибки зачастую допускают и «независимые» эксперты, приглашенные сторонами процесса либо правоохранительными органами.

Если подсудимый смог воспользоваться услугами высокооплачиваемого адвоката и выводы эксперта ставятся под сомнение, то при повторной экспертизе могут возникнуть существенные трудности.

10.3. Особенности экспертизы программного обеспечения

Экспертиза программного обеспечения может быть связана с вопросами детализации некоторых функций и возможностей, входящих в него программ. Функции — это то, что программы делают, а возможности относятся к каждой функции и уточняют их некоторые особенности и отдельные случаи.

Является ли программа вредоносной, т. е. включает ли она такие функции, которые могут причинить вред пользователю? Очевидно, что эти функции являются недокументированными и напрямую неизвестны.

Насколько правильно работает программа? Как принципиально можно обнаружить несоответствующее объявленным возможностям поведение программы? Видимо, это возможно в случае, когда результаты обработки оказываются не такими, какими они ожидаются. Вполне возможно это объяснить и неправильными ожиданиями. Если ранее эта программа давала результаты в соответствии с ожиданиями, возможно, что она неустойчива по отношению к входным данным или к каким-либо настройкам, которые изменились.

Некоторые алгоритмы, которые используются в программах, должны соответствовать каким-либо правовым нормам, хотя, и не обязаны давать детерминированные результаты. Например, программа игрового аппарата должна в среднем обеспечивать призовой фонд в размере не менее 75 % от суммы сбора. Делает ли это она, можно выяснить, если есть доступ к тексту программы, если есть возможность отладить ее или изучая статистику ее работы.

Вопросы, связанные с конкретной программой, правильнее всего задать ее автору. Однако в некоторых ситуациях это может представляться невозможным. Автор неизвестен, недоступен, заинтересован в утаивании интересующей следствие информации и т. д.

Остается один путь — тестирование программного обеспечения. Тестирование обычно заключается в попытке создать или воспроизвести какую-либо задачу.

В этом направлении существует развитая теория, которая используется и разработчиками ПО. Однако это не исключает возможностей ошибок в программах.

10.4. Примеры проявления недокументированных функций программного обеспечения

Приведем некоторые примеры недокументированных возможностей, казалось бы, хорошо известного редактора текстов — программы Microsoft *Word* (в скобках указаны версии редактора). При вводе в данном редакторе некоторых функций с начала строки после нажатия клавиши *Enter* они заменяются на определенный текст.

Функция *rand*()

=rand(x,y)

=rand(x,y) x и y — целые параметры, могут быть опущены. Заменяется на текст образца (2003) или отрывок из текста справки (2007).

Функция *lorem*()

=lorem() Заменяется на отрывок из Lorem ipsum[1] (2007, 2010).

Ошибки в модуле проверки русской орфографии (2003), в настоящее время исправлены.

Набор фразы *Правоспособность — способность иметь права и нести гражданские обязанности* вызывает (иногда после нажатия *Enter*), если включена автоматическая проверка орфографии, незамедлительное закрытие приложения без сохранения изменений. Данную ошибку эксплуатирует троянец «*Trojan.WordCrash*» (по аббревиатуре антивирусной лаборатории *Dr.Web*), который добавляет данную фразу во все документы с расширением **.doc* и **.rtf*.

При наборе в MS Word 97-2010 фразы «Хочу избежать службу в армии» модуль проверки орфографии в качестве одного из вариантов исправлений предлагает текст «Ошибка в управлении. Глагол "избежать" требует дополнения в родительном падеже». Например: «Никому не удалось избежать службы в армии».

---

[1] Классическая панграмма. Условный, подчас бессмысленный текст-запонитель, вставляемый в макет страницы. Является искаженным отрывком из философского трактата Цицерона «О пределах добра и зла».

При проверке орфографии буквы Ё не различаются буквами Е. Поэтому словосочетание «Бёлый Снёг» для *Word* считается верным.

При введении слова «Боль» и нажатии кнопки «Синонимы» предлагается вариант «Наслаждение» и т. д.

В данной лекции мы рассмотрели только основы методологии экспертной оценки программ и данных. Для более детального изучения вопросов лекции следует обратиться к литературе и в сети «Интернет».

Контрольные вопросы:

1. В чем заключается методология компьютерно-технической экспертизы?
2. Типичные правовые ошибки при выполнении компьютерно-технической экспертизы.
3. В чем состоит особенность экспертизы программного обеспечения?
4. Приведите примеры проявления недокументированных функций программного обеспечения.

Заключение

В настоящем курсе лекций изложены основные методы, средства и системы программно-аппаратной защиты информации:

— показаны роль и место ПАЗИ в составе комплексной системы защиты информации;

— проанализированы основные угрозы, каналы утечки и уязвимости объектов ПАЗИ, приведена выборочная статистика нарушений информационной безопасности;

— приведены формализованные требования к компонентам ПАЗИ;

— сформулированы задачи и дана классификация средств и систем ПАЗИ;

— рассмотрены средства защиты информации в компьютерах и в сетях;

— рассмотрены вопросы обеспечения целостности информации, вопросы защиты от вредоносного программного обеспечения;

— рассмотрены некоторые специализированные системы защиты компьютерной информации;

— рассмотрены основы методологии экспертного оценивания программ и данных.

Изучив данный курс лекций, читатель познакомится с базовыми понятиями ПАЗИ, с концепциями и принципами организации современных программно-аппаратных средств и систем защиты информации, с основными подходами к их использованию для решения практических задач информационной безопасности.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Федеральный закон от 26.07.2017 г. № 193-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации "».

4. Федеральный закон от 26.07.2017 г. № 194-ФЗ «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации "».

5. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины ИБ РФ».

6. Указ Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

7. Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании ГосСОПКА».

8. Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации».

9. РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации»: утв. Гостехкомиссией России. — Москва: Изд-во стандартов, 1992.

10. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утв. Гостехкомиссией России. — Москва: Изд-во стандартов, 1992.

11. Серия международных стандартов ISO/IEC 15408 «Общие критерии защищенности информационных технологий».

12. Серия международных стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности».

13. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утв. Гостехкомиссией России. — Москва: Изд-во стандартов, 1992.

Основная литература:

1. Грибунов О. П., Старичков М. В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. — Москва: ДГСК МВД России, 2017. — 160 с.

2. Нестеров С. А. Информационная безопасность: учебник и практикум для академического бакалавриата. — Москва: Юрайт, 2017. — 321 с.

3. Овчинский В. С. Криминология цифрового мира: учебник. — Москва: Инфра-М, 2018. — 352 с.

Дополнительная литература:

1. Аполонский А. В., Примакин А. И. Отчет о НИР «Основы исследования электронных документов». План научной деятельности Санкт-Петербургского университета МВД России. 2010. Поз. 1.69.

2. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации: учебное пособие. — Изд. 4-ое, перераб. и доп. — Москва: URSS, 2015. — 412 с.

3. Варлатая М. В. Программно-аппаратная защита информации: учебное пособие. — Владивосток: Изд-во ДВГТУ, 2007. — 318 с.

4. Голубев В. Некоторые вопросы расследования компьютерных преступлений [Электронный ресурс] // URL: http://www.crime-research.org/library/Atlanta.html.

5. Зайцев А. П., Голубятников И. В., Мещеряков Р. В., Шелупанов А. А. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие. — Изд. 2-ое испр. и доп. — Москва: Машиностроение-1, 2006. — 260 с.

6. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов. — Москва, 2018. Сер.: специалист. — 312 с.

7. Коршунов В. Г. Автоматизированный аудит программного обеспечения // Компьютерно-техническая экспертиза. — 2008. — № 1.

8. Котухов М. М., Калашников А. О., Кубанков А. Н. Информационная безопасность: учебное пособие. — Москва: Издание Академия IBS, 2008. — 148 с.

9. Куватов В. И., Пантиховский О. В., Синещук Ю. И., Обеспечение безопасности информации в АСУ: учебное пособие. — Санкт-Петербург: ВМИРЭ, 2011. — 320 с.

10. Куватов В. И., Синещук Ю. И., Смирнов А. С. Безопасность информационных систем и защита информации в МЧС России: учебное пособие. — Санкт-Петербург: СПбУ ГПС МЧС России, 2010. — 378 с.

11. Платонов В. В. Программно-аппаратные средства защиты информации. — Москва: Академия, 2013. — 331 с.

12. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза // Право и закон. — 2001.

13. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации: учебное пособие. — Екатеринбург: Уральский государственный университет им. М. Горького, 2008. — 237 с.

14. Усов А. И. Концептуальные основы Судебной компьютерно-технической экспертизы: дис. д-ра … юрид. наук. — Москва, 2002.

15. Windows Sysinternals [Электронный ресурс] // URL: http://go.microsoft.com/? linkId=6013253.

16. Документация компании Конфидент по системе Dallas Lock 8.0.

17. Документация по DLP-системе Falcongaze SecureTower 6.0.

18. Материалы конференций по SIEM.

Учебное издание

Куватов Валерий Ильич,
доктор технических наук, профессор,
заслуженный работник высшей школы Российской Федерации;
Чудаков Олег Евгеньевич,
доктор технических наук, профессор,
почётный работник высшего профессионального образования;
Родин Владимир Николаевич,
кандидат технических наук, доцент

ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ

Курс лекций

Редактор *Мамедова А. Х.*
Компьютерная верстка *Душкова А. Ю.*
Дизайн обложки *Савиных А. И.*

ISBN 978-5-91837-307-1

Подписано в печать 16.10.2020. Формат 60×84 $^{1}/_{16}$
Печать цифровая 12,0 п. л. Тираж 50 экз. Заказ № 124/20

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1