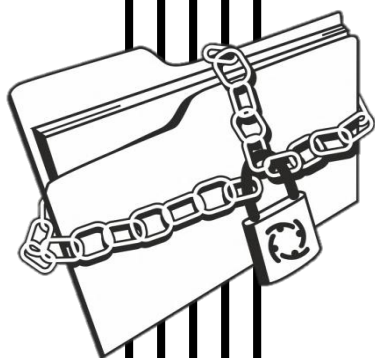


МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «Севастопольский государственный университет»
Институт радиоэлектроники и информационной безопасности



ИНФОРМАЦИОННО- АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Учебное пособие

г. Севастополь
2015

УДК 004.056.52

Информационно-аналитические системы безопасности: учебное пособие / СевГУ; сост. Костюков А. Д., Люльченко А. Н., Ожиганова М. И., Лебеденко А. В., Скороход М. Ю. – Севастополь: Изд-во СевГУ, 2015, – 48 с., ил.

Учебное пособие раскрывает актуальность проблемы защиты информации, показывает историю развития защиты информации в России, характеризует особенности информационной войны и специальных информационных операций. Рассматриваются вопросы сложности проблемы информационной безопасности, сценарии реализации угроз, различные подходы к анализу безопасности информации, как классический – субъективный, так и перспективный – объектно-ориентированный, а так же основные понятия информационной безопасности Российской Федерации. Для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

Утверждено на заседании кафедры Информационной безопасности 02.09.2015, протоколом №2.

Рецензент: кандидат технических наук, профессор Кирияченко В. А.

Ответственный за выпуск: кандидат технических наук, заведующий кафедрой Информационной безопасности Ожиганова М. И.

СОДЕРЖАНИЕ

Раздел 1. Основы информационной безопасности	5
1.1 Понятие информационной безопасности	5
1.2 Основные составляющие информационной безопасности.....	6
1.3 Сложность проблемы информационной безопасности.....	7
1.3.1 Наиболее опасные угрозы информационной безопасности	8
1.3.2 Внутренние угрозы информационной безопасности	10
1.3.3 Средства защиты	15
1.4 Сценарии реализации угроз информационной безопасности	17
1.4.1 Разглашение конфиденциальной информации	17
1.4.2 Обход средств защиты от разглашения конфиденциальной информации.....	17
1.4.3 Кража конфиденциальной информации	18
1.4.4 Нарушение авторских прав на информацию.....	18
1.4.5 Нецелевое использование ресурсов	18
Раздел 2. Безопасность компьютерных систем. Традиционный подход к анализу проблем информационной безопасности	20
2.1 Актуальность задач компьютерной безопасности.....	20
2.2 Основные понятия информационной безопасности автоматизированных систем обработки информации.....	20
2.3 Понятие «угрозы». Основные угрозы безопасности систем обработки информации.....	22
2.4. Понятие несанкционированного доступа	27
Раздел 3. Объектно-ориентированный подход – перспективный принцип анализа вопросов информационной безопасности	30
3.1 Необходимость применения объектно-ориентированного подхода к информационной безопасности	30
3.2 Основные понятия объектно-ориентированного подхода.....	31
3.3 Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.....	35
3.4 Недостатки традиционного подхода к информационной безопасности с объектной точки зрения	39
Раздел 4. Основные определения и критерии классификации угроз.....	42
4.1 Основные понятия об угрозах.....	42

4.2 Наиболее распространенные угрозы доступности	43
4.2.1 Примеры угроз доступности	45
4.2.2 Вредоносное программное обеспечение.....	46
4.3 Основные угрозы целостности.....	49
4.4 Основные угрозы конфиденциальности	50
Список использованных источников	52

РАЗДЕЛ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под информационной безопасностью (ИБ) следует понимать защиту интересов субъектов информационных отношений. Ниже описаны основные ее составляющие – конфиденциальность, целостность, доступность.

Приводится статистика нарушений ИБ, описываются наиболее характерные случаи.

1.1 Понятие информационной безопасности

Под **информационной безопасностью** будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Угрозы информационной безопасности – это обратная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «лучше все сломается, чем враг узнает хоть один секретный бит», во втором – «да нет у нас никаких секретов, лишь бы все работало».

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственной защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Отметим, что термин «**компьютерная безопасность**» (как эквивалент или заменитель понятия «информационная безопасность») представляется слишком узким. Компьютеры – только одна из составляющих информационных систем, и

хотя в первую очередь внимание будет сосредоточено на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на листочке, прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, однако нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

1.2 Основные составляющие информационной безопасности

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя **доступность** остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Целостность можно подразделить на:

- **статическую**, понимаемую как неизменность информационных объектов;
- **динамическую**, относящуюся к корректному выполнению сложных действий. Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций и отдельных пользователей (например, пароли).

1.3 Сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими нижеприведенными примерами [2-4].

– В Доктрине информационной безопасности Российской Федерации (здесь, подчеркнем, термин «информационная безопасность» используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

– По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью информационного оружия. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

– Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

– Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).

– Как сообщил журнал Internet Week от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

– В середине июля 1996 года корпорация General Motors отозвала 292 860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.

– В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

– Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла ИС.

1.3.1 Наиболее опасные угрозы информационной безопасности

Большая часть угроз ИБ с которой пришлось столкнуться Российским организациям – это внутренние угрозы. Анализ исследований [2-4] позволяет обобщить информацию о состоянии вопросов ИБ в российских организациях.

Индекс опасности утечки внутренней информации в российских организациях на 50% опережает аналогичный показатель для любой из внешних

угроз. Государственные структуры и представители частного сектора поставили на первое место утечку информации поскольку большая часть негативных последствий связано с этим инцидентом: прямые финансовые убытки (46%), удар по репутации (42,3%) и потерю клиентов (36,9%). При этом организации начинают присматриваться к своим служащим все более пристально. Свыше 40% респондентов уже зафиксировали за 2006 год более одной утечки, а почти 20% – более пяти утечек.

Доля организаций, внедривших защиту от утечек, возросла за 2007 год на 500%, то есть в пять раз. Однако, пока лишь каждая десятая компания внедрила эффективное решение на основе информационных технологий (ИТ) реализующих элементы ИБ. Только девять из десяти планируют сделать это в ближайшие два-три года. Таким образом, есть все основания полагать, что проникновение систем защиты от утечек на российский рынок продолжится и дальше, причем затронет абсолютно все отрасли экономики.

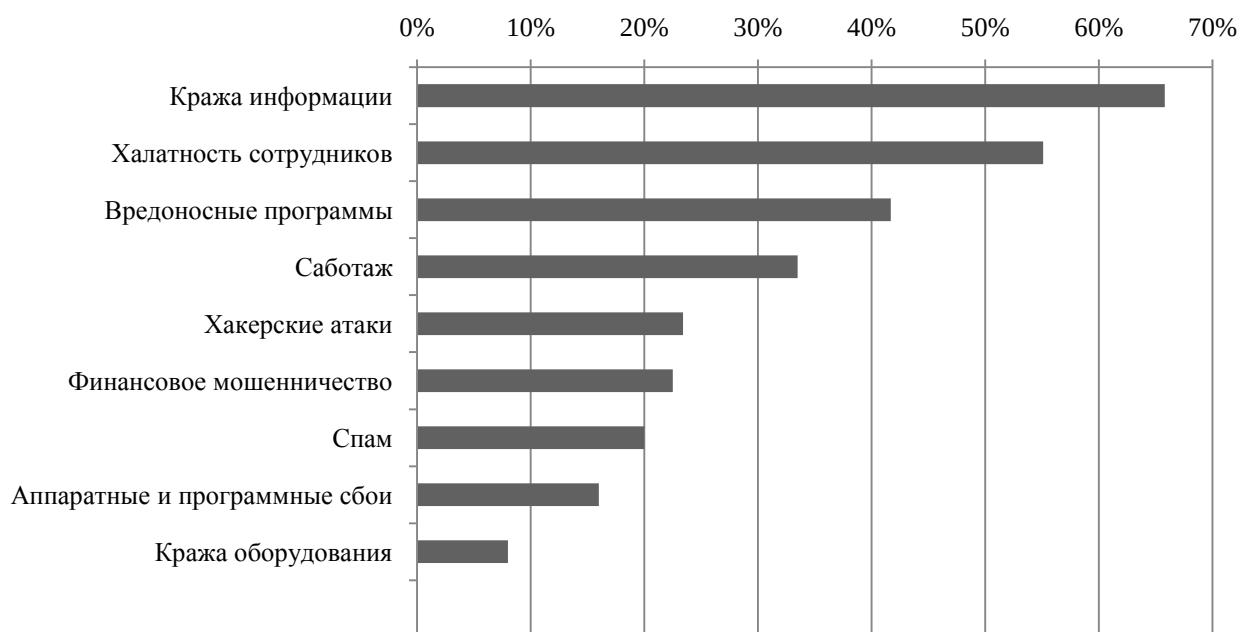


Рис. 1.1 – Угрозы ИБ по оценкам за 2007 год.

Спектр самых опасных угроз ИБ по оценкам за 2007 выглядит следующим образом:

- на первом месте кража информации (65,8%).
- на втором месте оказалась халатность сотрудников (55,1%).
- вирусные атаки заняли третье место, набрав 41,7% голосов респондентов.
- на четвертом месте оказалась угроза саботажа (33,5%). Судя по всему, можно утверждать, что высокий рейтинг опасности саботажа обусловлен тем, что респонденты постепенно теряют чувство страха перед внешними угрозами.
- хакерские атаки занимают пятое место с 23,4% голосов.

Если разделить угрозы на внутренние и внешние, то можно увидеть, что внутренние угрозы преобладают над вирусами, хакерами и спамом. Для построения соответствующей диаграммы (рис. 1.2) в категорию внутренних угроз были отнесены халатность сотрудников, саботаж и финансовое мошенничество, а в категорию внешних угроз – вирусы, хакеры и спам.

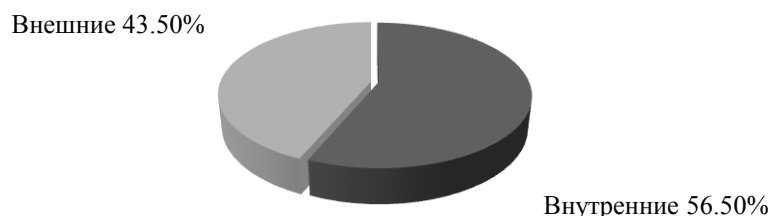


Рис. 1.2 – Соотношение опасности внутренних и внешних угроз ИБ.

Необходимо отметить, что угрозы кражи информации, различных сбоев и кражи оборудования не были отнесены ни к одной из групп. Так как они могут быть реализованы как изнутри, так и снаружи, либо вообще без вмешательства человека (например, аппаратные сбои).

Таким образом, респонденты гораздо больше обеспокоены внутренней ИБ, чем защитой от внешних угроз. Кроме того, следует учитывать, что неклассифицированные риски, например кражу информации или оборудования, чаще всего относят к внутренним угрозам. То есть внешние риски заметно уступают внутренним угрозам.

1.3.2 Внутренние угрозы информационной безопасности

Определив, что самые опасные угрозы ИБ исходят изнутри организации, необходимо изучить структуру внутренних рисков. Как показали результаты исследований [2-4] (респондентов просили оценить, какие угрозы внутренней ИБ являются наиболее опасными для опрашиваемых) – рис. 1.3, в списке самых опасных внутренних угроз с огромным отрывом лидирует:

1. нарушение конфиденциальности информации (70,1%);
2. искажение информации (38,4%) – отстает на целых 31,7%.

Другими словами, риск утечки ценной информации волнует респондентов почти в два раза больше, чем любая другая инсайдерская угроза.

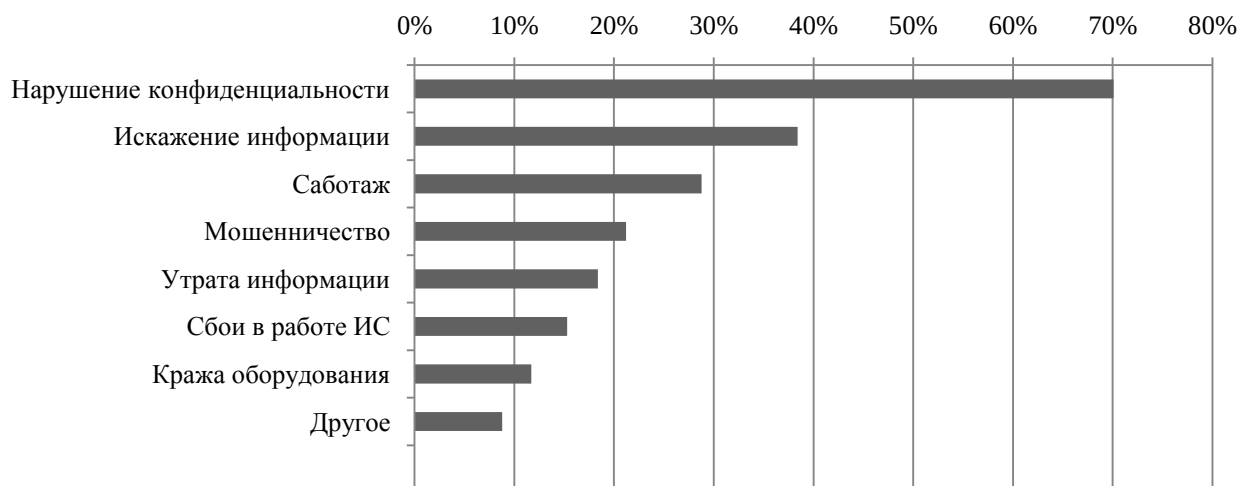


Рис. 1.3 – Наиболее опасные угрозы внутренней ИБ.

В 2006 году были зафиксированы пять крупных утечек, в России и СНГ, а также почти полторы сотни инцидентов внутренней ИБ в других частях света (таблица 1.1).

Таблица 1.1 – Самые крупные утечки 2006 года в России и СНГ

Дата	Организация	Потенциальный ущерб
Август, 2006 год	Российские банки, занимающиеся потребительским кредитованием	Удар по репутации и серьезный подрыв доверия к отечественному финансовому сектору
Август, 2006 год	Банк «Первое ОВК»	Ухудшение имиджа, плохое паблисити, массовый отток клиентов
Сентябрь, 2006 год	МЦС (Мобильная цифровая связь), владелец марки Velcom	Удар по репутации, потеря лояльных клиентов и трудности с привлечением новых
Октябрь, 2006 год	«Вэб Хостинг» (владелец марки Valuehost)	Массовый отток клиентов, юридические издержки, удар по имиджу
Декабрь, 2006 год	«Русский стандарт», ХКФ-банк, Росбанк, Финансбанк, Импэксбанк и др.	Ухудшение репутации всего банковского сектора

Таким образом, с точки зрения респондентов, наиболее опасной угрозой ИБ является утечка конфиденциальной информации, совершаемая инсайдерами. В результате такой утечки, более всего респонденты были озабочены следующими последствиями (рис. 1.4):

1. прямыми финансовыми убытками (46%);
2. ухудшение имиджа и общественного мнения (42,3%);
3. потеря клиентов (36,9%).

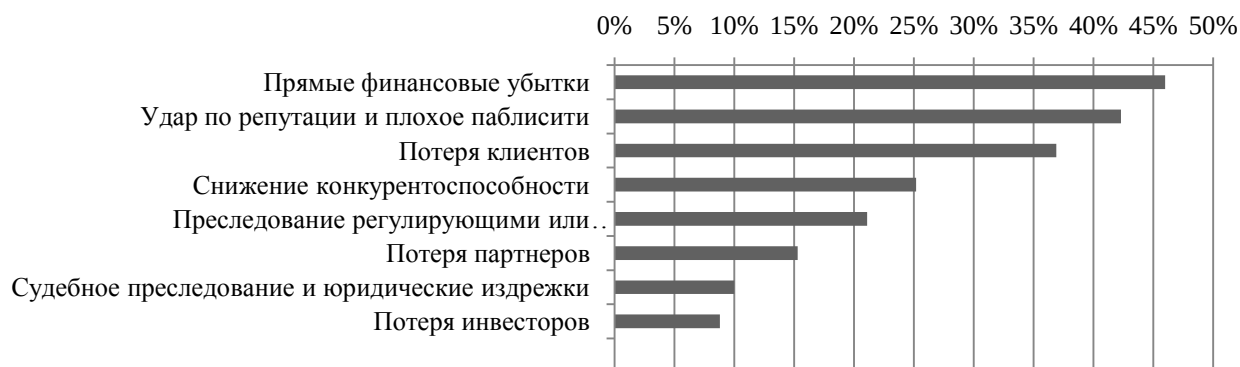


Рис. 1.4 – Наиболее существенные последствия утечки конфиденциальных данных.

Кроме того, респонденты озабочены снижением конкурентоспособности (25,2%) организации, что является скорее следствием целого ряда других негативных последствий утечки. Между тем лишь каждый десятый (10%) упомянул среди наиболее плачевных последствий юридические издержки и судебное преследование, что свидетельствует о неразвитости правоприменительной практики в России.

Результаты анализа [2-4] по выявлению самых распространенных каналов утечки информации представлено на рис. 1.5.

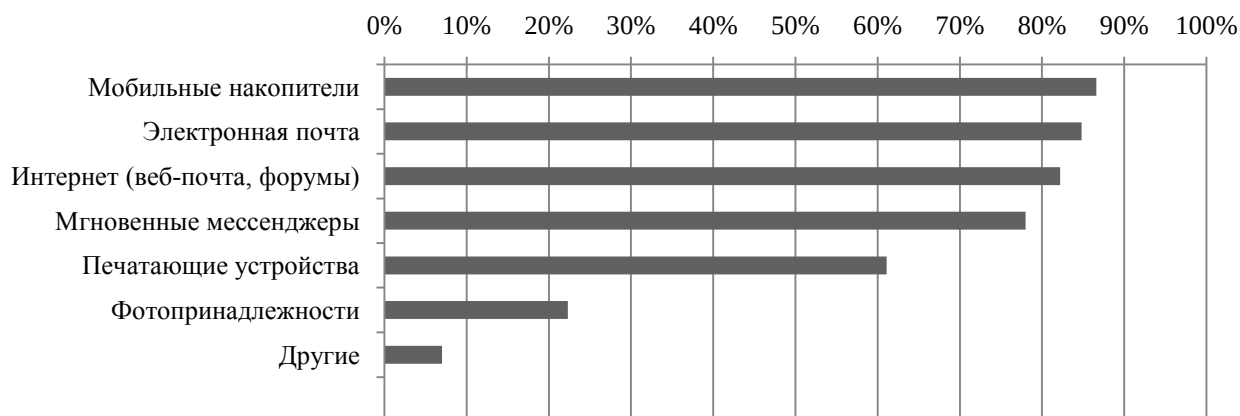


Рис. 1.5 – Каналы утечки конфиденциальных данных.

Заметим, что наибольшей популярностью среди инсайдеров пользуются: мобильные накопители (86,6%), электронная почта (84,8%), web-браузеры (82,2%), Jabber-клиенты (78 %).

Отметим что, крайние три позиции соответствуют использованию Internet приложений, в случае если в организации не используется система контроля доступа и обмена информацией с глобальной сетью Internet.

Исследование [5] позволило сформировать общую статистическую картину типовых уязвимостей при использовании организациями общего подключения к

сети Internet (таблица 1.2). При этом уровень опасности данных угроз различен, а эффективность использования средств защиты от угроз существенно отличается и зачастую низко эффективно (рис. 1.6 а, б).

Таблица 1.2 – Безопасность использования организациями сети Internet

№	Параметр / среднее значение на одного сотрудника за неделю	Все организации	Банки
1	Наличие потенциально опасного контента (активных объектов) в инспектируемом входящем и исходящем Интернет-трафике	1,070	845
2	Посещение пользователями опасных и запрещенных Web-сайтов	639	472
3	Идентифицированные угрозы, инциденты, успешные атаки, действие spyware (шпионов), троянов, эксплойтов	308	127
4	Нецелевое использование Интернет и других ресурсов (Skype, IM, P2P, скачивание музыки и видео, потоковое видео/аудио и др.). Нарушения политик ИБ.	128	21
5	Использование неавторизованных, потенциально опасных приложений	5	1.7
6	Скрытые каналы утечки – неавторизованные и потенциально опасные каналы коммуникаций пользовательских компьютеров с внешними узлами (в т.ч. дистанционное управление компьютерами извне, использование их для массовой рассылки спама и/или распределенных DDoS атак)	3.6	1.8
7	Передача/получение через Интернет опасных, подозрительных и инфицированных файлов	5	0.02



Рис. 1.6 а – Уровень опасности выявленных Интернет-угроз.



Рис. 1.6 б – Эффективность используемых средств защиты и работы служб ИБ.

Таким образом, основной угрозой ИБ, реализация которой приводит к максимальным последствиям является разглашение конфиденциальной информации. Анализ, проведенный выше показывает, что данные, представляющие собой коммерческую тайну, могут покинуть сетевой периметр предприятия несколькими путями: по электронной почте, через чаты, форумы и другие службы Интернета, с помощью средств мгновенного обмена сообщениями, копирования информации на мобильные носители, а также посредством распечатки ее на принтере. Таким образом, для обнаружения факта разглашения конфиденциальной информации необходимо контролировать все пути утечки данных, в частности анализировать исходящий трафик, передаваемый по протоколам SMTP, HTTP, FTP и TCP/IP.

Еще одной серьезной угрозой, требующей анализа входящего/исходящего трафика организации, является **нецелевое использование ресурсов компании**. Сюда входят:

- посещение сайтов общей и развлекательной направленности (не имеющих отношения к исполнению служебных обязанностей) в рабочее время;
- загрузка, хранение и использование мультимедиафайлов и ПО развлекательной направленности в рабочее время;
- использование ресурсов компании для рассылки информации рекламного характера, спама или информации личного характера, включая информацию о сотрудниках, номера кредитных карт и т.д.

Соответственно для борьбы с угрозами подобного типа необходимы технические решения, фильтрующие исходящие веб-запросы и почтовый трафик.

1.3.3 Средства защиты

Для борьбы с разными типами внутренних угроз информационной безопасности используют различные технические средства. Но только комплексное решение поможет действительно решить проблему защиты компьютерной инфраструктуры предприятия.

Анализ [3-5] показывает, что в сфере распространения средств ИБ среди организаций за последний год не произошло сколько-нибудь значительных изменений (рис. 1.7).

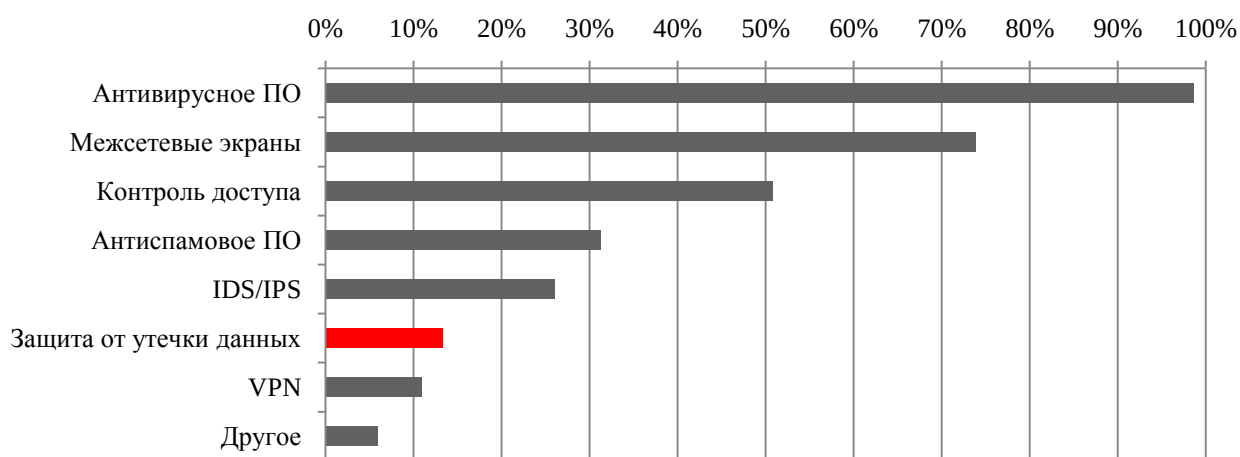


Рис. 1.7 – Средства обеспечения ИБ применяемые организациями.

Основными средствами, которые используют современные компании, для обеспечения ИБ являются: антивирусы (98,6%), межсетевые экраны (73,9%), средства контроля доступа (50,8%).

В качестве наиболее эффективных путей защиты от утечек и решениях, которые представляются организациям наиболее адекватными и приемлемыми для решения проблемы внутренней ИБ, но, по ряду причин, не используемых респондентами на практике. Респонденты назвали ряд мер, популярность которых изображена на рис. 1.8.

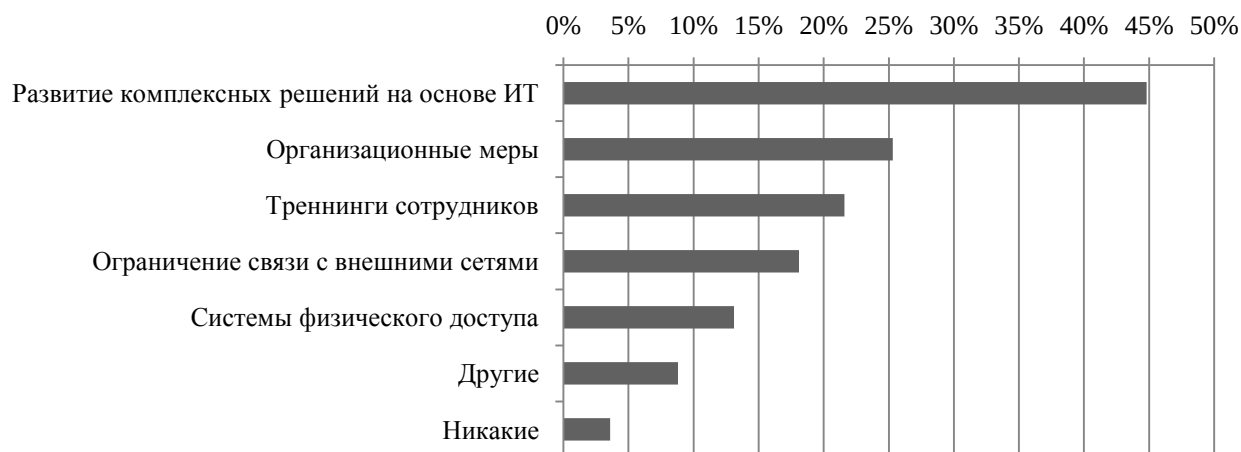


Рис. 1.8 – Наиболее эффективные средства обеспечения ИБ.

Как отмечено в исследованиях [2-5] наиболее эффективным средством защиты от угроз ИБ являются комплексные информационные продукты (44,8%). Далее следуют организационные меры (25,3%), тренинги персонала (21,6%) и ограничение связи с внешними сетями (18,1%). При этом респонденты отметили, что в соответствии с разработанными планами обеспечения ИБ респонденты планируют у себя внедрить ту или иную систему обеспечения ИБ. Согласно распределению ответов (рис. 1.9), девять из десяти (89,9%) организаций планируют внедрить в ближайшие три года ту или иную систему защиты от утечек.



Рис. 1.9 – Планы по внедрению систем защиты ИБ.

Как видно из ответов респондентов комплексные решения ИТ, а именно комплексные системы мониторинга сетевых ресурсов преобладают при выработке решения о выборе средства обеспечения ИБ, при этом они же являются наиболее эффективными средствами обеспечения ИБ (рис. 1.8).

Таким образом, российские компании постепенно в полной мере осознают угрозы и риски от халатного отношения к вопросам информационной

безопасности и начинают проводить активную политику внедрения комплексных средств ИБ с информационные системы сопровождения бизнеса.

1.4 Сценарии реализации угроз информационной безопасности

Существует целый ряд сценариев, согласно которым могут быть реализованы внутренние угрозы. Каждый из этих сценариев учитывает конкретную цель неправомерных действий и технические средства ее достижения.

1.4.1 Разглашение конфиденциальной информации

Данный вид угроз подразумевает разглашение информации, представляющей коммерческую тайну, посредством отсылки ее по электронной почте, через Интернет (чат, форум и т. д.), с помощью средств обмена мгновенными сообщениями, путем копирования информации на переносные носители или распечатки данных. Для обнаружения факта разглашения конфиденциальной информации разные компании предлагают перехват почтового, внутрисетевого (на уровне TCP/IP) и Web-трафика (протоколы HTTP, FTP, IM и т. д.) с последующим анализом различными методами фильтрации, в том числе с помощью анализа контента.

1.4.2 Обход средств защиты от разглашения конфиденциальной информации

Обход средств защиты от разглашения конфиденциальной информации удается добиться при помощи различных преобразований данных, например, шифрования, архивации с большой глубиной вложенности, преобразования в графический формат или редкие текстовые форматы, изменения кодировки, использования неизвестного ПО или общения на иностранном языке, незнакомом большинству сотрудников компании. Системы защиты от утечек конфиденциальных данных борются с такими действиями, поддерживая разнообразные форматы файлов и реагируя на любые подозрительные действия (неизвестный формат файла, шифрование и т. д.).

1.4.3 Кража конфиденциальной информации

Неправомерный доступ к информации возможен при ее передаче через обычное соединение (без шифрования) – путем взлома корпоративной сети; если данные размещены в местах, доступных посторонним людям или сотрудникам, не имеющим соответствующих прав; если посторонний человек имеет возможность читать с экрана монитора; если имеется доступ к напечатанным материалам, переносным носителям или компьютерам.

1.4.4 Нарушение авторских прав на информацию

В рамках угрозы нарушения авторских прав, возможно копирование частей документов одного автора в документы другого автора (а также в почтовые сообщения, Web-формы и т. д.); индивидуальное шифрование документов, при котором компания лишается возможности работать с документом после увольнения или перевода сотрудника или в случае утраты пароля; использование опубликованных в Интернете материалов без обработки в своих документах; использование мультимедиа-файлов (графики, аудио- и видеозаписей), ПО и прочих информационных объектов, защищенных авторским правом; подделка данных адресата или отправителя с целью опорочить его доброе имя или скомпрометировать компанию.

1.4.5 Нецелевое использование ресурсов

Под нецелевым использованием ресурсов подразумеваются посещение сайтов общей и развлекательной направленности (не имеющих отношения к исполнению служебных обязанностей) в рабочее время; загрузка, хранение и использование мультимедиа-файлов и ПО развлекательной направленности в рабочее время; использование ненормативной, грубой, некорректной лексики при ведении деловой переписки; загрузка, просмотр и распространение материалов для взрослых, а также материалов, содержащих нацистскую символику, агитацию или другие противозаконные материалы; использование ресурсов компании для рассылки информации рекламного характера, спама или информации личного характера, в том числе информации о сотрудниках, номерах социального страхования, кредитных карт и т. д.

Следует отметить, что не существует ни одного комплексного решения, которое позволяло бы полностью защитить компанию от воздействия этих и других угроз. Однако многие поставщики предлагают различные варианты решений, позволяющих контролировать и предотвращать реализацию значительной части угроз. Так, продукты компаний ClearSwift (<http://www.clearswift.com>), Cobion (<http://www.cobion.com>) и SurfControl (<http://www.surfcontrol.com>) позволяют исключить нецелевое использование ИТ-ресурсов компании.

Для фильтрации Web-трафика используется база данных URL, хранящая миллионы классифицированных по темам записей. Когда сотрудник компании запрашивает в браузере какую-нибудь страницу, специальный фильтр проверяет записи базы и определяет категорию запрашиваемого ресурса. Список категорий насчитывает несколько десятков, туда входят почтовые, развлекательные, туристические, порнографические и другие группы ресурсов. Если информации о требуемой Web-странице еще нет в базе, то проводится анализ содержимого страницы и определение ее тематики в автоматическом режиме. Такой подход позволяет администратору строить политики на основании групп пользователей и их прав на доступ к страницам соответствующих категорий.

Чтобы исключить нецелевое использование почтовой службы компании, потребуется контентный анализ каждого письма. Современные решения позволяют анализировать не только формальные атрибуты сообщения, но и вложения различных форматов, графическое и текстовое содержимое тела письма, а также все содержащиеся в нем ссылки.

Решения, позволяющие исключить нецелевое использование ИТ-ресурсов компании, часто содержат некоторые возможности предотвращения утечки конфиденциальных данных. Например, продукты Cobion и SurfControl фильтруют исходящий почтовый трафик еще и на предмет содержания в нем конфиденциальной информации. Чтобы настроить такой анализ, администратору необходимо вручную указать в консоли управления те документы, утечку которых необходимо предотвратить.

Важно отметить, что задача предотвращения утечки конфиденциальных данных не решена в этих продуктах полностью. Так, без всякого присмотра остается рабочая станция сотрудника, с которой он может переписать файл на мобильный носитель или просто его распечатать. Особый контроль требуется и для Web-трафика. В Интернете есть множество чатов, форумов, открытых почтовых сервисов и т. д. Все эти ресурсы могут быть использованы для разглашения конфиденциальной информации.

Рынок систем, специализирующихся только на защите от утечек конфиденциальных данных (Anti-Leakage Software), только начинает формироваться. Среди существующих решений пока лишь InfoWatch Enterprise Solution компании InfoWatch (<http://www.infowatch.ru>) обеспечивает контроль над всеми видами коммуникаций в ИТ-инфраструктуре компании. Данное решение предусматривает средства анализа почтового и Web-трафика, а также механизмы контроля за рабочими станциями служащих.

РАЗДЕЛ 2. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Актуальность задач компьютерной безопасности

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых порой зависит благополучие, а иногда и жизнь многих людей.

Актуальность и важность проблемы обеспечения безопасности информационных технологий обусловлены следующими причинами:

- резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации;
- резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- высокие темпы роста парка персональных компьютеров, находящихся в эксплуатации в самых разных сферах деятельности;
- резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
- бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
- повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;
- развитие глобальной сети Internet, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

2.2 Основные понятия информационной безопасности автоматизированных систем обработки информации

Безопасность автоматизированной системы обработки информации (АСОИ) – свойство защищенности системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.

Природа воздействий на АСОИ может быть самой разнообразной. Это и стихийные бедствия (землетрясение, ураган, пожар), и выход из строя составных элементов АСОИ, и ошибки персонала, и попытка проникновения злоумышленника.

Безопасность АСОИ достигается принятием мер по обеспечению конфиденциальности и целостности обрабатываемой ею информации, а также доступности и целостности компонентов и ресурсов системы.

Под доступом к информации понимается ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Различают следующие виды доступа к информации:

– **санкционированный доступ** – доступ к информации, не нарушающий установленные правила разграничения доступа;

– **несанкционированный доступ (НСД)** – характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа.

Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Правила разграничения доступа служат для регламентации права доступа субъектов доступа к объектам доступа.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. По существу – это свойство информации быть известной только допущенным и прошедшим проверку (авторизированным) субъектам системы (пользователям, процессам, программам).

Для остальных субъектов системы эта информация должна быть неизвестной.

Субъект – это активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.

Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

Целостность информации обеспечивается в том случае, если данные в системе не отличаются семантическим отношением от данных в исходных документах, т.е. если не произошло их случайного или преднамеренного искажения или разрушения.

Целостность компонента или ресурса системы – это свойство компонента или ресурса быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

Доступность компонента или ресурса системы – это свойство компонента или ресурса быть доступным для авторизованных законных субъектов системы.

Под угрозой безопасности АСОИ понимаются возможные воздействия на АСОИ, которые прямо или косвенно могут нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в АСОИ.

С понятием угрозы безопасности тесно связано понятие уязвимости АСОИ.

Уязвимость АСОИ – это некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака – это одна из реализаций угрозы безопасности.

Противодействие угрозам безопасности является целью защиты систем обработки информации.

Безопасная или защищенная система – это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплекс средств защиты – программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности АСОИ. Комплекс создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

2.3 Понятие «угрозы». Основные угрозы безопасности систем обработки информации

По цели воздействия различают три основных типа угроз безопасности АСОИ:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз,

когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

Целостность информации может быть нарушена умышленно злоумышленником, атак же в результате объективных воздействий со стороны среды, окружающей систему.

Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций.

Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением,

которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных).

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании.

Блокирование доступа к ресурсу может быть постоянным или временным.

Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

АСОИ состоит из следующих компонент:

- аппаратные средства – ЭВМ и их составные части (процессоры, мониторы, терминалы, периферийные устройства-дисководы, принтеры, контроллеры, кабели, линии связи) и т.д.;

- программное обеспечение – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

- данные – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;

- персонал – обслуживающий персонал и пользователи.

Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Опасные воздействия на АСОИ можно подразделить на: случайные и преднамеренные.

Случайные воздействия. Анализ опыта проектирований, изготовления и эксплуатации АСОИ показывает, что информация подвергается различным

случайным воздействиям на всех этапах цикла жизни и функционирования АСОИ.

Причинами случайных воздействий при эксплуатации АСОИ могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т.д.

Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить **гипотетическую модель потенциального нарушителя:**

1. квалификация нарушителя может быть на уровне разработчика данной системы;
2. нарушителем может быть как постороннее лицо, так и законный пользователь системы;
3. нарушителю известна информация о принципах работы системы;
4. нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие **преднамеренные угрозы:**

1. несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
2. ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
3. несанкционированное копирование программ и данных;
4. кража магнитных носителей, содержащих конфиденциальную информацию;
5. кража распечатанных банковских документов;
6. умышленное уничтожение информации;
7. несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
8. фальсификация сообщений, передаваемых по каналам связи;

9. отказ от авторства сообщения, переданного по каналам связи;
10. отказ от факта получения информации;
11. навязывание ранее переданного сообщения;
12. разрушение информации, вызванное вирусными воздействиями;
13. разрушение архивной банковской информации, хранящейся на магнитных носителях;
14. кража оборудования.

В таблице 2.1 показаны основные пути реализации угроз безопасности АСОИ при воздействии на ее компоненты. Конечно, таблица 2.1 дает самую общую картину того, что может произойти с системой. Конкретные обстоятельства и особенности должны рассматриваться отдельно.

Таблица 2.1 – Основные пути реализации угроз безопасности АСОИ при воздействии на ее компоненты

Объекты воздействия	Нарушение конфиденциальности информации	Нерушение целостности информации	Нарушение работоспособности системы
Аппаратные средства	НСД-подключение; использование ресурсов; хищение носителей.	НСД-подключение; использование ресурсов; модификация, изменение режимов.	НСД-изменение режимов; вывод из строя; разрушение.
Программное обеспечение	НСД-копирование; хищение; перехват.	НСД, внедрение «троянского коня», «вирусов». «червей».	НСД-искажение; удаление; подмена.
Данные	НСД-копирование; хищение; перехват.	НСД-искажение; модификация.	НСД-искажение; удаление; подмена.
Персонал	Разглашение: передача сведений о защите; халатность.	«Маскарад»; вербовка; подкуп персонала.	Уход с рабочего места; физическое устранение.

Термин «вирус» в применении к компьютерам был предложен Фредом Коэном из Университета Южной Калифорнии. Исторически первое определение, которое дал Ф. Коэн: **«Компьютерный вирус»** – это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению».

Ключевыми понятиями в определении компьютерного вируса являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны паразитированию в живой природе биологического вируса.

Компьютерный вирус пытается тайно записать себя на компьютерные диски. Способ функционирования большинства вирусов заключается в таком изменении системных файлов компьютера, чтобы вирус начинал свою деятельность при каждой загрузке. Например, вирусы, поражающие загрузочный сектор, пытаются инфицировать часть дискеты или жесткого диска, зарезервированную только для операционной системы хранения файлов запуска. Эти вирусы особенно коварны, так как они загружаются в память при каждом включении компьютера. Такие вирусы обладают наибольшей способностью к размножению и могут постоянно распространяться на новые диски.

Сетевой «червь» представляет собой разновидность программы-вируса, которая распространяется по глобальной сети и не оставляет своей копии на магнитном носителе. Термин «червь» пришел из научно-фантастического романа Джона Бруннера «Побурным волнам».

Этот термин используется для именования программ, которые подобно ленточным червям перемещаются по компьютерной сети от одной системы к другой.

Первоначально «черви» были разработаны для поиска в сети других компьютеров с свободными ресурсами, чтобы получить возможность выполнить распределенные вычисления. При правильном использовании технология «червей» может быть весьма полезной. Например, «червь» WorldWide Web Worm формирует индекс поиска участков Web. Однако «червь» легко превращается в вредоносную программу. «Червь» использует механизмы поддержки сети для определения узла, который может быть поражен. Затем с помощью этих же механизмов передает свое тело в тот узел или активируется, либо ждет подходящих условий для активизации.

2.4. Понятие несанкционированного доступа

Несанкционированный доступ (НСД) состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД является наиболее распространенным многообразным видом компьютерных нарушений.

НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

- все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами АСОИ;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов приёма несанкционированного доступа **наиболее распространенными нарушениями являются:**

- перехват паролей;
- «маскарад»;
- незаконное использование привилегий.

Перехват

паролей

осуществляется специально разработанными программами.

При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля.

Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях.

Существуют и другие способы перехвата паролей.

«Маскарад» – это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий или привилегий другого пользователя.

Примерами реализации «маскарада» являются:

- вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

Незаконное

использование

привилегий.

Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций.

Каждый пользователь получает свой набор привилегий: обычный пользователь – минимальный, администраторы – максимальный.

Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в системе защиты.

Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Угрозы, компьютерных сетей.

Особое следует остановиться на угрозах, которыми могут подвергаться компьютерные сети.

Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами (объектами) сети осуществляется физически с помощью сетевых линий связи и программно с помощью механизмов сообщений. При этом управляющие сообщения и данные, пересылаемые между объектами сети, передаются в виде пакетов обмена.

При вторжении в компьютерную сеть злоумышленник может использовать как пассивные, так и активные методы вторжения.

Пассивное вторжение (перехват информации) – нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации. Как правило, злоумышленник может определить пункты назначения и идентификаторы либо только факт прохождения сообщения, его длину и частоту обмена, если содержимое сообщения нераспознаваемо, т.е. выполнить анализ трафика (потока сообщений) в данном канале.

Активное вторжение – нарушитель стремится подменить информацию, передаваемую в сообщении. Он может выборочно модифицировать, изменить или добавить правильное или ложное сообщение, удалить, задержать или изменить порядок следования сообщений. Злоумышленник может также аннулировать и задержать все сообщения, передаваемые по каналу. Подобные действия можно квалифицировать как отказ в передаче сообщений.

РАЗДЕЛ 3. ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Необходимость применения объектно-ориентированного подхода к информационной безопасности

В настоящее время информационная безопасность является относительно замкнутой дисциплиной, развитие которой не всегда синхронизировано с изменениями в других областях информационных технологий. В частности, в ИБ пока не нашло отражения основные положения *объектно-ориентированного подхода*, ставшего основой при построении современных информационных систем. Не учитываются в ИБ достижения в технологии программирования, основанные на накоплении многократного использования программистских знаний. Это очень серьезная проблема, затрудняющая прогресс в области ИБ.

Попытки создания больших систем за последние 60-х годов вскрыли много численные проблемы программирования, главной из которых является сложность создаваемых и сопровождаемых систем. Результатами исследований в области технологии программирования стали сначала структурированное программирование, затем *объектно-ориентированный подход*.

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем. Представляется естественными, более того, необходимым, стремление распространить этот подход на системы информационно-безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Любой разумный метод борьбы со сложностью опирается на принцип «divide et impera» – «разделяй и властвуй». Этот **принцип** означает, что сложная система (информационной безопасности) на верхнем уровне должна состоять из небольшого числа относительно независимых **компонентов**. Относительная независимость здесь и далее понимается как минимизация числа связей между компонентами. Затем **декомпозиции** подвергаются выделенные на первом этапе **компоненты**, и так далее до заданного **уровня детализации**. В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции. **Структурный подход** опирается на **алгоритмическую декомпозицию**, когда выделяются **функциональные элементы** системы.

Основная проблема *структурного подхода* состоит в том, что он неприменим на ранних этапах анализа и моделирования предметной области, когда алгоритмы функций деловещено дошло. Нужен подход «широкого спектра», не имеющий такого концептуального разрыва анализируемыми системами и примен

имый на всех этапах разработки и реализации сложных систем.
Мы стараемся показать, что объектно-ориентированный подход удовлетворяет таким требованиям.

3.2 Основные понятия объектно-ориентированного подхода

Объектно-ориентированный подход использует объектную декомпозицию, то есть поведение системы описывается в терминах взаимодействия объектов.

Необходимо ввести понятие *класса*.

Класс – это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Объект – это элемент класса, то есть абстракция определенной сущности.

Подчеркнем, что **объекты** активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми **методами объекта**. Например, может быть определен класс «пользователь», характеризующий «пользователя вообще», то есть ассоциированные с пользователем данные и их поведение (методы). После этого может быть создан объект «пользователь Иванов» соответствующей конкретизацией данных и, возможно, методов.

Следующую группу важнейших понятий объектного подхода составляют: *инкапсуляция, наследование, полиморфизм*.

Основным инструментом борьбы со сложностью в объектно-ориентированном подходе является **инкапсуляция** – сокрытие реализации объектов (их внутренней структуры и деталей реализации методов) с предоставлением во вне только строго определенных интерфейсов.

Понятие «**полиморфизм**» может трактоваться как способность объекта принадлежать более чем одному классу. Введение этого понятия отражает необходимость смотреть на объекты под разными углами зрения, выделять при построении абстракций разные аспекты сущностей моделируемой предметной области, не нарушая при этом целостности объекта. (Строго говоря, существуют и другие виды полиморфизма, такие как перегрузка и параметрический полиморфизм, но на них сейчас не интересно.)

Наследование означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов.

Наследование является важным инструментом борьбы с размножением сущностей без необходимости. Общая информация не дублируется, указывается только то, что меняется. При этом класс-потомок помнит своих «предков».

Очень важно и то, что наследование и полиморфизм в совокупности наделяют объектно-

ориентированную систему способностью относительно безболезненной эволюции. Средства информационной безопасности приходится постоянно модифицировать и обновлять, и если нельзя сделать так, чтобы это было экономически выгодно, ИБ-инструмент защиты превращается в обузу.

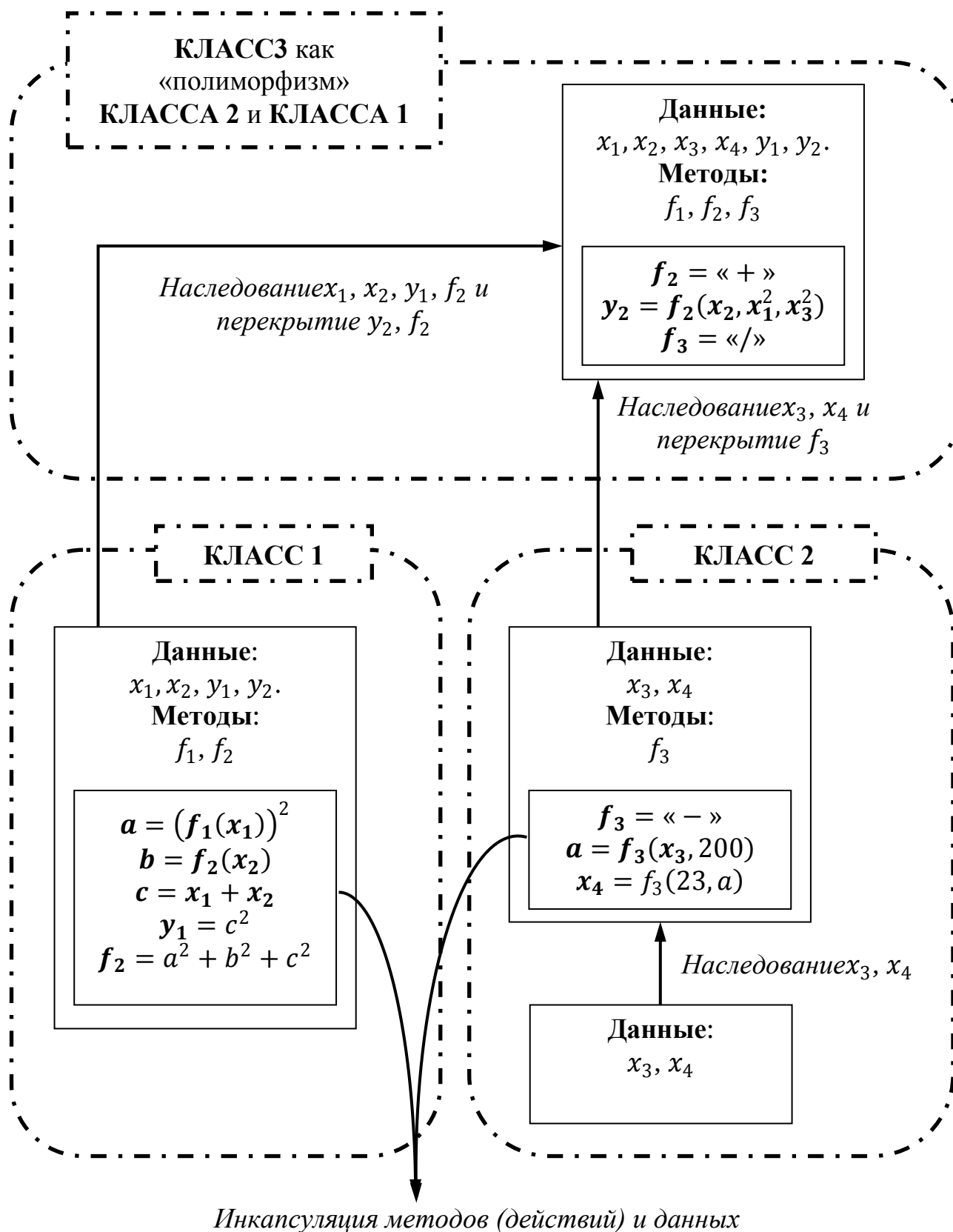


Рис. 3.1 – Объектно-ориентированный подход к вопросам ИБ.

Объекты реального мира обладают, как правило, несколькими относительно независимыми характеристиками. Применительно к объектной модели будем называть такие характеристики **гранями**.

Основными **гранями** ИБ является:

- доступностью,
- целостностью,
- конфиденциальностью.

Понятие *границы* позволяет более естественно, чем полиморфизм, смотреть на объекты с разных точек зрения и строить разноплановые абстракции.

Понятие **уровня детализации** важно не только для визуализации объектов, но и для систематического рассмотрения сложных систем, представленных в иерархическом виде. Само по себе оно очень простое: если очередной уровень иерархии рассматривается с уровнем детализации $n > 0$, то следующий – с уровнем $(n - 1)$. Объект с уровнем детализации 0 считается атомарным.

Понятие *уровня детализации* позволяет рассматривать иерархии с потенциально бесконечной высотой, варьировать детализацию как объектов в целом, так и их *граней*.

Весьма распространенной конкретизацией *объектно-ориентированного подхода* являются **компонентные объектные среды**, к числу которых принадлежит, например, JavaBeans. Здесь появляется два новых важных понятия: *компонент* и *контейнер*.

Компонент можно определить как многократно используемый **объект**, допускающий обработку в графическом инструментальном окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество **компонентов**, образуя общий контекст взаимодействия с другими компонентами и сокращением. Контейнеры могут выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими **объектно-ориентированному подходу**:

- инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый во вне интерфейс;
- наследование позволяет развивать созданные ранее компоненты, не нарушая целостности объектной оболочки;
- полиморфизм по сути дает возможность группировать объекты, характеристики которых с некоторой точкой зрения можно считать сходными.

Понятия же *компонента* и *контейнера* необходимы нам потому, что с их помощью можно естественным образом представить защищаемую ИС и сами защитные средства. В частности, *контейнер* может определять границы контролируемой зоны (задавать так называемый «периметр безопасности»).

3.3 Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Применим *объектно-ориентированный* *подход* к вопросу информационной безопасности.

Проблема обеспечения информационной безопасности – комплексная, защищать приходится *сложные системы*, и сами защитные средства тоже сложны, поэтому нам понадобятся все введенные понятия. Начнем с понятия *грани*.

Фактически *три грани* уже были введены: это доступность, целостность и конфиденциальность.

Их можно рассматривать относительно независимо, *исчисляется*, что если все они обеспечены, то обеспечена и ИБ в целом (то есть субъектами информационных отношений не будет нанесен неприемлемый ущерб).

Таким образом, мы структурировали нашу цель. Теперь нужно структурировать средства ее достижения. Введем следующие *грани*:

- законодательные меры обеспечения информационной безопасности;
- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

Отметим, что, *в принципе*, их можно рассматривать как результат варьирования *уровня детализации* (по этой причине мы будем употреблять словосочетания «законодательный уровень», «процедурный уровень» и т.п.).

Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия), административные меры – на всех субъектов в пределах организации, процедурные – на отдельных людей (или небольшие категории субъектов), программно-технические – на оборудование и программное обеспечение.

При такой трактовке переход с уровня на уровень можно рассмотреть применительно к *наследования* (каждый следующий уровень не отменяет, а дополняет предыдущий), а также *полиморфизма* (субъекты выступают сразу в нескольких ипостасях – например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться).

Очевидно, для всех выделенных, относительно независимых *граней* действует принцип *инкапсуляции* (это означает, что *грани* «относительно независимы»). Более того, эти две совокупности *граней*

можно назвать *ортгональными*, поскольку для фиксированной *границы* водной совокупности (например, доступности) *границы* в другой совокупности должны пробежать все множество возможных значений (нужно рассмотреть законодательные, административные, процедурные и программно-технические меры). *Ортгональных совокупностей* не должно быть много; думается, двух совокупностей с числом элементов, соответственно, 3 и 4 уже достаточно, так как они дают 12 комбинаций.

Продemonстрируем теперь, как можно рассматривать защищаемую ИС, варьируя *уровень детализации*.

Пусть интересы субъектов информационных отношений концентрируются вокруг ИС некой организации, располагающей двумя территориально разнесенными производственными площадками, на каждой из которых есть серверы, обслуживающие своих внешних пользователей, а также пользователи, нуждающиеся в внутренних и внешних сервисах. Одна из площадок оборудована внешним подключением (то есть имеет выход в Internet).

Привзгляд с нулевым *уровнем детализации* мы увидим лишь то, что у организации есть информационная система (см. рис. 3.2).

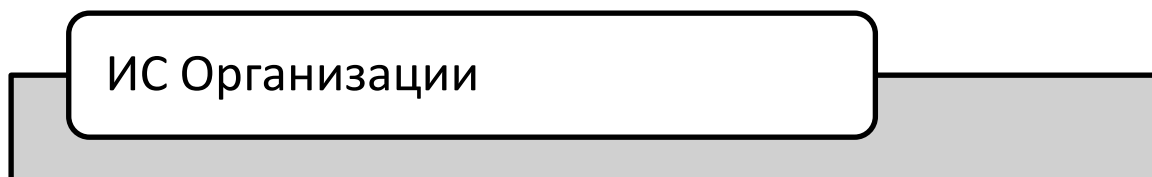


Рис. 3.2 – ИС при рассмотрении с уровнем детализации 0.

Уже здесь необходимо учесть законы, применимые к организациям, располагающим информационными системами. Возможно, какую-либо информацию нельзя хранить и обрабатывать на компьютерах, если ИС не была аттестована на соответствие определенным требованиям. На административном уровне могут быть декларированы цели, ради которых создавалась ИС, общие правила закупок, внедрения новых *компонентов*, эксплуатации и т.п. На процедурном уровне нужно определить требования к физической безопасности ИС и пути их выполнения, правила противопожарной безопасности и т.п. На программно-техническом уровне могут быть определены предпочтительные аппаратно-программные платформы и т.п.

Пока мы критериям проводить *декомпозицию* ИС – в значительной степени идеалов. Будем считать, что на первом *уровне*

детализации делаются видимыми сервисы и пользователи, разделены на клиентскую и серверную часть (рис. 3.3).

точнее,

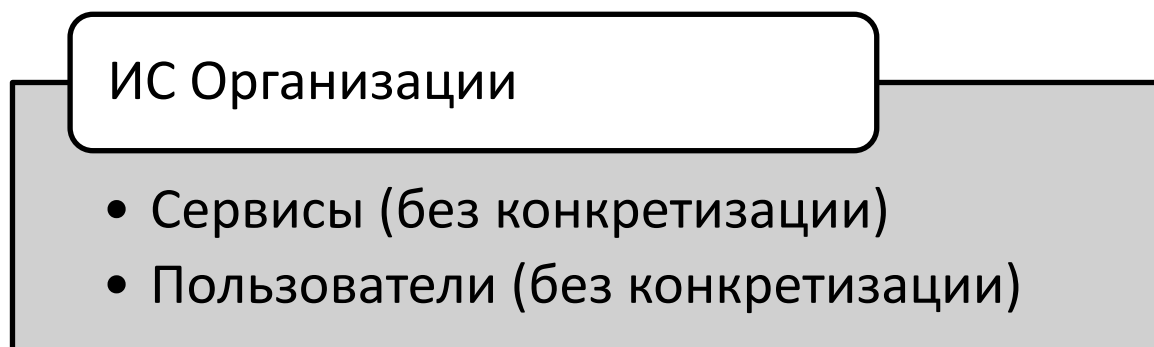


Рис. 3.3 – ИС при рассмотрении с уровнем детализации 1.

На этом уровне следует сформулировать требования к сервисам (к самому их наличию, к доступности, целостности и конфиденциальности предоставляемых информационных услуг), изложить способы выполнения этих требований, определить общие правила поведения пользователей, необходимый уровень их предварительной подготовки, методы контроля их поведения, порядок поощрения и наказания и т.п. Могут быть сформулированы требования и предпочтения по отношению к серверным и клиентским платформам.

На втором уровне *детализации* мы увидим следующее (см. рис. 3.4).

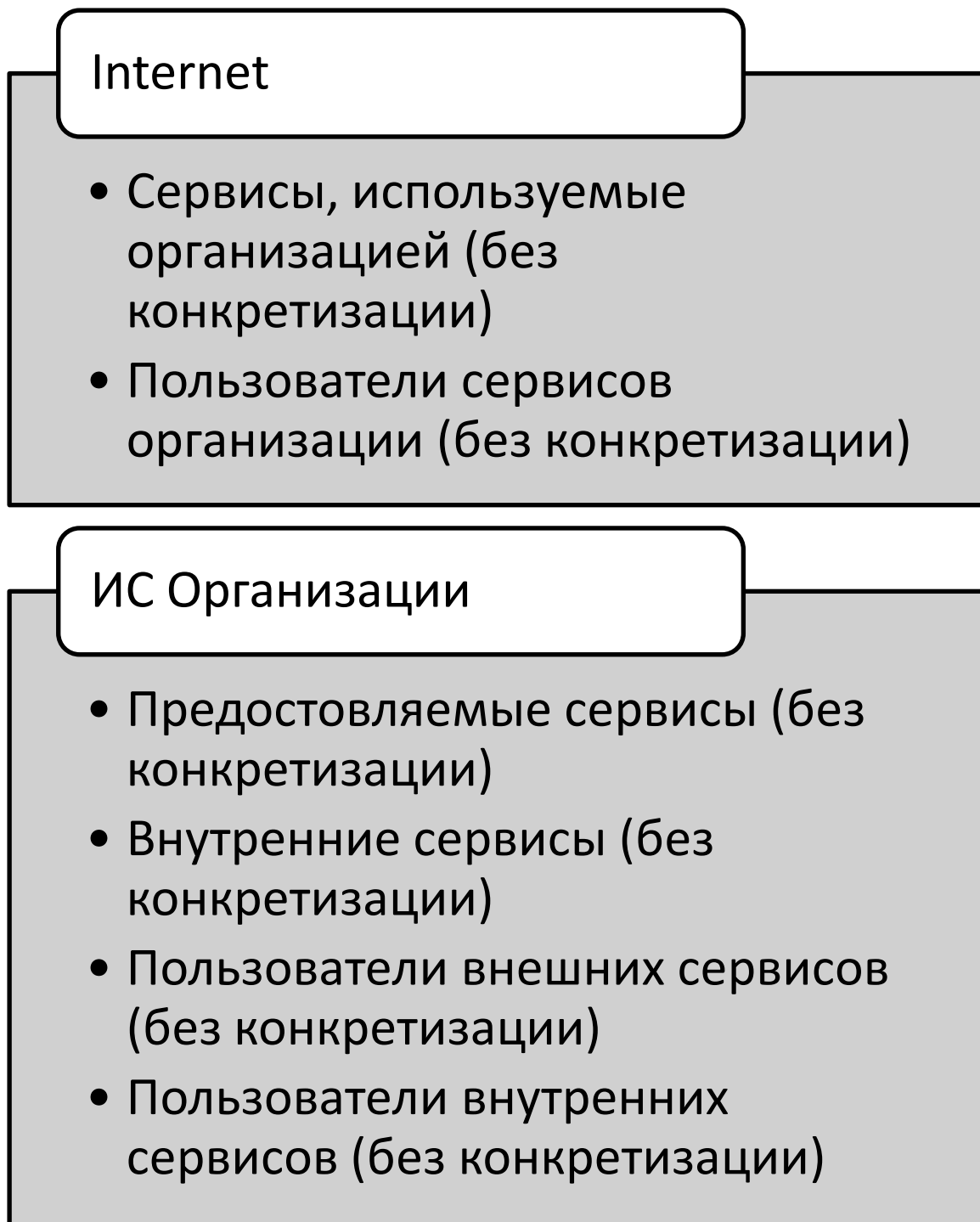


Рис. 3.4 – ИС при рассмотрении с уровнем детализации 2.

На этом уровне нас все еще не интересует внутренняя структура ИС организации, равно как и детали Internet. Констатируется только существование связи между этими сетями, наличие внешних пользователей, а также предоставляемых и внутренних сервисов. Что это за сервисы, пока неважно.

Находясь на уровне детализации 2, мы должны учитывать законы, применимые к организациям, ИС которых снабжены внешними подключениями. Речь идет о допустимости такого подключения, о его защите, об ответственности пользователей, обращающихся к внешним сервисам, и об ответственности организаций, открывающих свои сервисы для внешнего доступа. Конкретизация аналогичной направленности, с учетом наличия внешнего подключения, должна быть выполнена на административном, процедурном и программно-техническом уровнях.

Обратим внимание на то, что контейнер (в смысле компонентной объектной среды) «ИС организации» задает границы контролируемой зоны, в пределах которой организация проводит определенную политику. Internet живет по другим правилам, которые организация должна принимать, как данность.

Увеличивая уровень детализации, можно разглядеть два разнесенных производственных площадки и каналы связи между ними, распределение сервисов и пользователей по этим площадкам и средства обеспечения безопасности внутренних коммуникаций, специфика отдельных сервисов, разные категории пользователей и т.п. Мы, однако, на этом остановимся.

3.4 Недостатки традиционного подхода к информационной безопасности с объектной точки зрения

Исходя из основных положений объектно-ориентированного подхода, следует в первую очередь признать устаревшим традиционное деление на активные и пассивные сущности (субъекты и объекты в привычной для дообъектной ИБ терминологии).

Подобное деление устарело, по крайней мере, по двум причинам.

Во-первых, в объектном подходе пассивных объектов нет. Можно считать, что все объекты активны одновременно и при необходимости вызывают методы друг друга. Как реализованы эти методы (и, в частности, как организовано доступ к переменным их значениям) – внутреннее дело вызываемого объекта; детали реализации скрыты, инкапсулированы.

Вызывающему объекту доступен только предоставляемый интерфейс.

Во-вторых, нельзя сказать, что какие-то программы (методы) выполняются от имени пользователя. Реализации объектов сложны, так что последние нельзя рассматривать всего лишь как инструменты выполнения воли

пользователей. Скорее можно считать, что пользователь прямо или (как правило) косвенно, на свой страх и риск, «просит» некоторый объект об определенной информационной услуге.

Когда активизируется вызываемый метод, объект действует скорее от имени (в всяком случае, по воле) своего создателя, чем от имени вызвавшего его пользователя. Можно считать, что объекты обладают достаточной «свободой воли», чтобы выполнять действия, о которых пользователь не только не просил, но даже не догадывается об их возможности. Особенно это справедливо в сетевой среде и для программного Обеспечения (ПО), полученного через Internet, но может оказаться верным и для коммерческого ПО, закупленного по всем правилам солидной фирмы.

Для иллюстрации приведем следующий гипотетический пример.

Банк, ИС которого имеет соединение с Internet, приобрел зарубежную автоматизированную банковскую систему (АБС). Только спустя некоторое время в банке решили, что внешнее соединение не нуждается в защите, и установили межсетевой экран. Изучение регистрационной информации экрана показало, что время от времени из зарубежа отправляются IP-пакеты, содержащие какие-то непонятные данные (наверное, зашифрованные, решили в банке). Стали разбираться, куда же пакеты направляются, и оказалось, что идут они в фирму, разработавшую АБС. Возникло подозрение, что в АБС встроена закладка, чтобы получать информацию о деятельности банка. Связались с фирмой; там очень удивились, поначалу все отрицали, но в конце концов выяснили, что один из программистов не убрал из поставленного в банк варианта отладочную выдачу, которая была организована через сеть (как передача IP-пакетов специфического вида, с вносом заданных IP-адресов рабочего места этого программиста). Таким образом, никакого злого умысла не было, однако некоторое время информация о платежах свободно гуляла по сетям.

Отметим, что при определении допустимости доступа важно не только (и не столько), кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя определить так называемые «тройные программы», выполняющие, помимо декларированных, некоторые скрытые (обычно негативные) действия.

Следует также признать устаревшим и положение о том, что разграничение доступа направлено на защиту от злоумышленников. Приведенный выше пример показывает, что внутренние ошибки распределенных ИС представляют не меньшую опасность, а гарантировать их отсутствие в сложных системах современная технология программирования не позволяет.

ВдообъектнойИБоднимизважнейшихтребованийявляется**безопасностьповторногоиспользования**пассивныхсущностей (таких,например, какдинамическивыделяемыеобластипамяти).

Очевидно,подобноетребованиевступаетвконфликтсакимфундаментальнымпринципом, *какинкапсуляция.* *Объект* нельзяочиститьвнешнимобразом(заполнитьнулямиилислучайнойпоследовательностьюбит), *если* толькоонсамнепредоставляетсоответствующий*метод*. Приналичии таког*ометода*надежностьочисткизависитоткорректностиегореализацииивызова.

ОднимизсамыхпрочныхстереотиповсредиспециалистовпоИБявляетсятрактовка**операционнойсистемы**какдоминирующег*осредствабезопасности*. НаразработкузащищенныхОСвыделяютсязначительныесредства, зачастуюущербостальнымнаправлениямзащитыи,следовательно, вущербреальнойбезопасности. ВсовременныхИС,выстроенныхвмногоуровневойархитектуре клиент/сервер, ОСнеконтролирует*объекты*, *скоторыми* работаютпользователи, равнокакидействиясамихпользователей, которыерегистрируютсяиучитываютсяприкладнымисредствами. ОсновнойфункциейбезопасностиОСстановитсязащитавозможностей, предоставляемыхпривилегированнымпользователям,отатакобычныхпользователей.

РАЗДЕЛ 4. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ

4.1 Основные понятия об угрозах

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку – **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или к ошибке в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибке в программном обеспечении, то окно опасности «открывается» с появлением средств использования ошибки или ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест время существования окна опасности определяются следующими событиями:

1. должно стать известно о средствах использования пробела в защите;
2. должны быть выпущены соответствующие заплаты;
3. заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск наложение заплат – как можно более оперативно.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнута открытой организации угроза конфиденциальности может просто не существовать – вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью.

тью. Иными словами, угрозы, как и все ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

4.2 Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки являются собственными угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

– нежелание работать с информационной системой (чаще всего проявляется при необходимости освоения новых возможностей и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;

- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

- разрушение или повреждение помещений;

- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые «обиженные» сотрудники – нынешние и бывшие. Как правило, они стремятся нанести вред организации – «обидчику», например:

- испортить оборудование;
- встроить логическую бомбу,

которая со временем разрушит программы и/или данные;

- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы по порядкам в организации и способны нанести немалый ущерб.

Необходимо следить за тем, чтобы при увольнении сотрудник его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия: пожары, наводнения, землетрясения,

ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

4.2.1 Примеры угроз доступности

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение **оборудования** (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего – грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования – нередкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно генерировать искусственным образом – с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы.

Летом, в сильную жару, могут сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится репутации, и финансовому положению организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранятся небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды.

Иногда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем к другим угрозам доступности – программным атакам на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно – полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое **потребление** подразделяется на локальное и удаленное.

При просчетах в конфигурации системы локальная программа способна практически

монополизировать процессоры и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование «DoS – атака». Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер множества различных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Временем начала «моды» на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее – владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения системы из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, программа «Teardrop» удаленно «подвешивает» компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

4.2.2 Вредоносное программное обеспечение

Одним из опаснейших способов проведения атаки является внедрение в атакуемую систему вредоносного программного обеспечения.

Выделяют следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть «бомбой». Вообще говоря, спектр вредоносных функций неограничен, поскольку «бомба», как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно «бомбы» предназначены для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

«**черви**» – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на распространение по сети.

Иногда самораспространение вредоносного ПО вызывает агрессивное потребление ресурсов, следовательно, является вредоносной функцией. Например, «черви» «съедают» полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются в встраивании специальных «бомб».

Вредоносный код, который выглядит как функционально полезная программа, называется **троянским вирусом**. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изгибают в ручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» содержится следующее определение:

«**Программный вирус** – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

Наш взгляд, подобное определение не совсем удачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности «бомб», вирусов и/или «червей» и перестает существовать с обновлением баз данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года полным правом можно было утверждать, что «несмотря на экспоненциальный рост числа известных вирусов, аналогично росту количества инцидентов, вызванных ими, незарегистрировано. Соблюдение несложных правил «компьютерной гигиены» практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента».

В марте 1999 года, с появлением вируса «Melissa», ситуация кардинальным образом изменилась. «Melissa» – это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда какой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

Вслед за «Melissa» появилась целая серия вирусов, «червей» и их комбинаций: «Explorer.zip» (июнь 1999), «BubbleBoy» (ноябрь 1999),

«ILOVEYOU» (май 2000) и т.д. Нет чтобы от них было особенно большой ущерб, но общественный резонанс они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье – так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов – Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель безошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения «бомб» часто используются ошибки типа «переполнение буфера», когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый «червь Морриса»; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности схватилось сразу около полтора миллиона серверных систем...

Не забыты современные злоумышленники и испытанные троянские программы. Например, «троянцы» Back Orifice и Netbus позволяют получить контроль над пользовательскими системами различными вариантами MS-Windows.

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

4.3 Основные угрозы целостности

На втором месте по размеру ущерба (после не преднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американскими организациями был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Целостность подразделяется на: статическую и динамическую.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) **может:** ввести неверные данные или изменить данные. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении и после того, как она отвергла его ухаживания.

В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту.

Содержание письма для нас сейчас неважно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл регистрации информации компании сотовой связи, из которого явствовало,

что указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места.

Таким образом,

в суде состоялось противостояние «файл против файла».

Очевидно,

один из них был фальсифицирован или изменен,

то есть была нарушена его целостность.

Суд решил,

что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными источниками целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странно для вице-президента действие.)

Еще один урок: **угрозой целостности** является не только фальсификация или изменение данных, но и отказ от совершенных действий.

Если интернет-средство обеспечить «неотказуемость», компьютерные данные не могут рассматриваться как свидетельство.

Потенциально уязвимы с точки зрения нарушения **целостности** не только **данные**, но и **программы**. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения.

Угрозами динамической целостности являются

- нарушение атомарности транзакций;
- переупорядочение, кража, дублирование данных;
- внесение дополнительных сообщений (сетевых пакетов и т.п.).

Соответствующие действия в сетевой среде называются активным прослушиванием.

4.4 Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на:

- предметную;
- служебную.

Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить не компьютерный и вообще технический характер.

Если для доступа к различным системам используются много разовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке, которые пользователь часто оставляет на рабочем столе, а то и просто теряет. Невозможно помнить много разных паролей как результат применения несложных схем чередования или использования двух-трех легко запоминающихся (иногда легко угадываемых) паролей. Описанный класс уязвимых мест можно назвать **размещением конфиденциальных данных в среде, где им не обеспечена (зачастую – и не может быть обеспечена) необходимая защита**. Угроза состоит в том, что кто-то откажется узнать секреты, которые сами просятся в руки.

Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает **передача конфиденциальных данных в открытом виде** (в разговоре, в письме, в посещении), которая делает возможным перехват данных. Для этого могут использоваться разные технические средства (подслушивание или прослушивание разговоров,

пассивное прослушивание сети и т. п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Весьма опасной угрозой являются... **выставки,**
на которые многие организации, **недолго думая,**
отправляют оборудование из производственной сети,
совсем хранящимися на них данными. Остаются прежними пароли,
при удаленном доступе они продолжают передаваться в открытом виде.
Это плохо даже в пределах защищенной сети организации;
во объединенной сети выставки –
это слишком суровое испытание честности всех участников.

Еще один пример измещения, **о котором часто забывают, –**
хранение данных на резервных носителях.

Для защиты данных на основных носителях применяются развитые системы управления доступом;

копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза,
и если конфиденциальность действительно является критичной,
а данные передаются по многим каналам,
их защита может оказаться весьма сложной и дорогостоящей.
Технические средства перехвата хорошо проработаны, доступны,
просты в эксплуатации, **а у установивших, например на кабельную сеть,**
может кто угодно,
так что эту угрозу нужно принимать во внимание по отношению не только к внешним,
но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей,
но и для компьютеров, **особенно портативных.**
Часто ноутбук оставляют без присмотра на работе или в автомобиле,
иногда просто теряют.

Опасной не технической угрозой конфиденциальности являются **методы морально-психологического воздействия, такие как маскард –**
выполнение действий под видом лица,
обладающего полномочиями для доступа к данным.

К неприятным угрозам, **от которых трудно защищаться,**
можно отнести **злоупотребление полномочиями.**

На многих типах систем привилегированный пользователь
(например системный администратор) способен прочесть любой
(незашифрованный) файл, получить доступ к почте любого пользователя и т. д.
Другой пример – **нанесение ущерба при сервисном обслуживании.**
Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет
возможность действовать в обход программных защитных механизмов. Таковы основные угрозы,
которые наносят наибольший ущерб субъектам информационных отношений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Галатенко В. А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2008. – 208 с.
2. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФМГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
3. Астахова А.
Анализ защищенности корпоративных автоматизированных систем // Jet Info [Эл. ресурс] – URL: www.jetinfo.ru/2002/7/1/article1.7.2002.html
4. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Эл. ресурс] – N 12, 2004. – URL: www.bytemag.ru/?ID=603365
5. Доля А. Внутренние ИТ-угрозы в России 2006 // Компьютер Пресс N 5, 2007.
6. Грудзаев С. Полезные мелочи – Aladdin Security Solution // LAN [Эл. ресурс] – URL: <http://www.osp.ru/lan/2008/05/5068377/>
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.
Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
8. Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2005. – 264 с.
9. Lonely R. Алгоритм шифрования данных с открытым ключом RSA. [Эл. ресурс] – URL: www.rusdoc.ru/material/raznoe/rsa.shtml
10. Лапонина О. Р. Криптографические основы безопасности: курс лекций для Интернет-университета информационных технологий.
11. Антивирусная защита компьютерных систем: курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/security/antiviruskasp/
12. Вирусы и средства борьбы с ними: курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/security/viruskasper/
13. Атака через Интернет / Медведевский И. Д., Семьянов П. В., Платонов В. В.; под ред. П. Д. Зегжды. – СПб.: изд. НПО «Мир семьи-95», 1997.
14. Мэйволд Э. Безопасность сетей: курс лекций для Интернет-университета информационных технологий – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/security/netsec/
15. Кобб М. Джост М. Безопасность ИС: курс лекций для Интернет-университета информационных технологий – М.: Интернет-

- университет информационных технологий – www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/internet/iisecurity/
16. БейсР. Введение в обнаружение атак и анализ защищенности // НИП «Информзащита» [Эл. ресурс] – URL: <http://bugtraq.ru/library/books/icsa/>
17. Семенов Ю. А. Процедуры, диагностики и безопасность в Интернет: курс лекций для Интернет-университета информационных технологий – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/network/pdsi/
18. Пировских А. Взлом WPA // TNG.ru [Эл. ресурс] – URL: www.thg.ru/network/20050806/print.html
19. Таранов А., Слепов О. Безопасность систем электронной почты // Jet Info [Эл. ресурс] – № 6, 2003. – URL: www.citforum.ru/security/internet/email/article1.6.2003.html#AEN11
20. Иржавский А. Безопасность электронной почты // СЮ – № 8, 2003. – URL: offline.cio-world.ru/2003/18/29383/index.html
21. Карпов В. Е., Коньков К. А. Основы операционных систем. – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2005. – 536 с.
22. Коньков К. А. Устройство и функционирование ОС Windows. – М.: Интернет-университет информационных технологий – ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2008. – 208 с.
23. Коньков К. А. Основы организации операционных систем Microsoft Windows: курс лекций для Интернет-университета информационных технологий – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/os/osmswin/
24. Казарин О. В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003. – 212 с. – URL: www.citforum.ru/security/articles/kazarin/#1-5
25. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Уч. пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.
26. Основы информационной безопасности. Учебное пособие для вузов/ Е. Б. Белов, В. П. Лось, Р. В. Мещериков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
27. Грушо А. А. Тимонина Е. Е. Теоретические основы защиты информации. – М.: Изд. агентства «Яхтсмен», 1996. – 72 с.