ЧАСТЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 оборотная 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 «пусть 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) собственно 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 безопастность») 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 (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о личных данных сотрудников) и отдельных пользователей (например, пароли).

1.3 Важность и 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 292860 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 связанно 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.

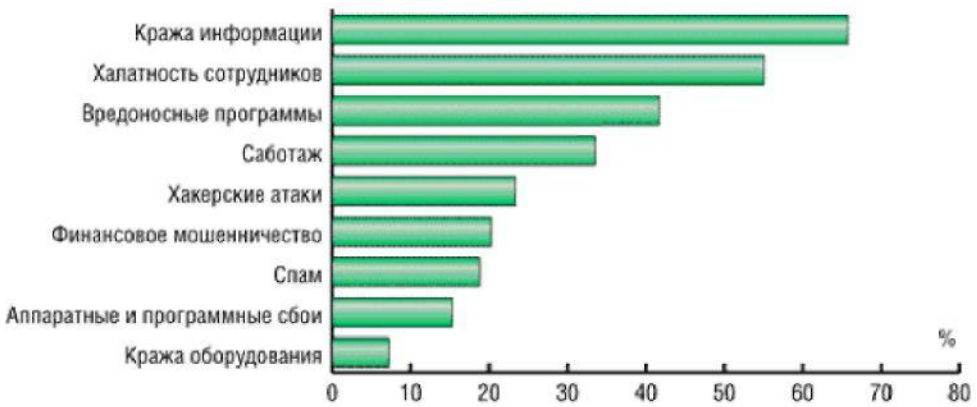


Рис. 1.1 - Угрозы ИБ по оценкам за 2007 год

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 превалируют 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.

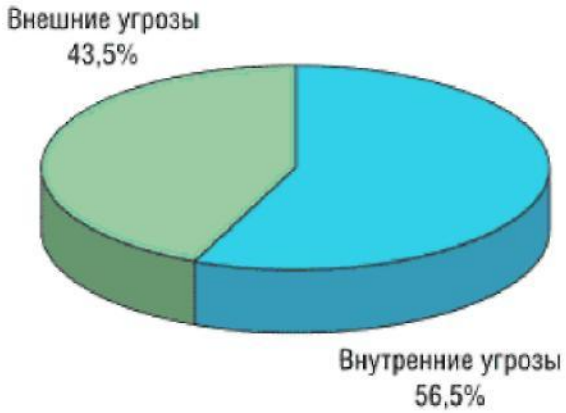


Рис. 1.2 - Соотношение опасности внутренних и внешних угроз ИБ

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 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» (поглощен Росбанком в 2005 году)	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%).

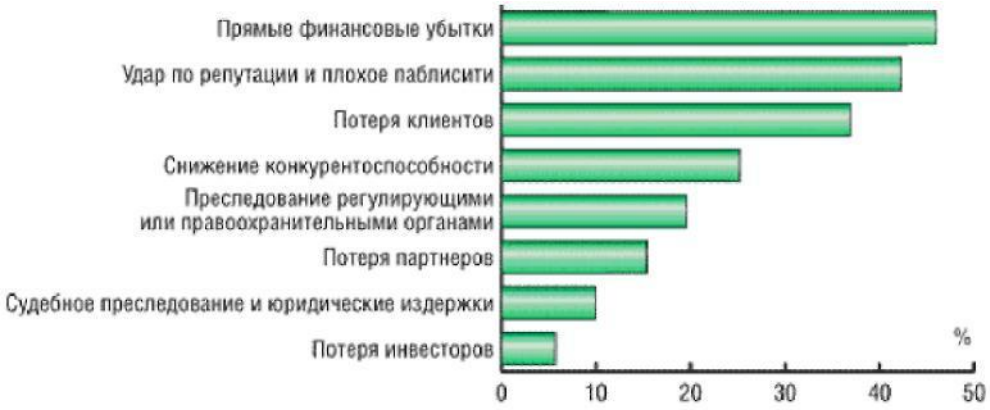


Рис. 1.4 - Наиболее существенные последствия утечки конфиденциальных данных

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.

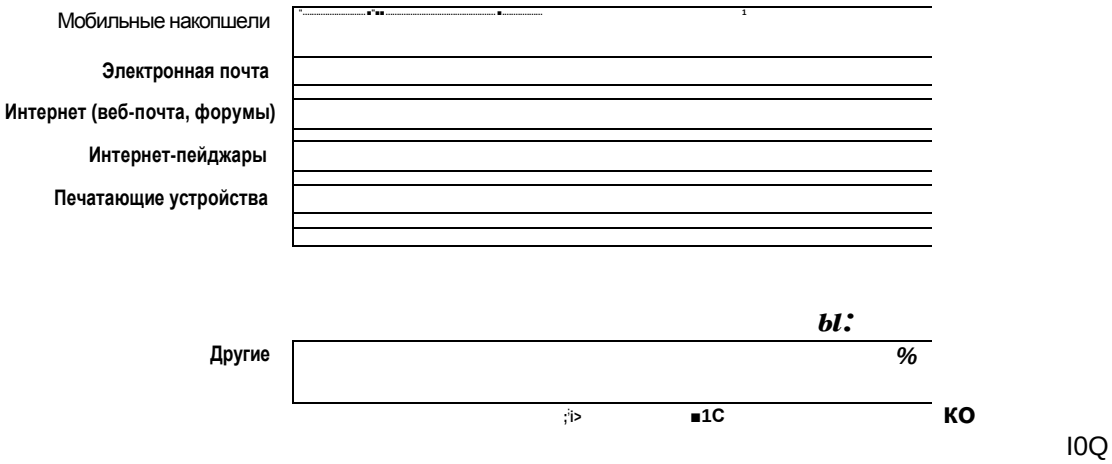


Рис. 1.5 - Каналы утечки конфиденциальных данных

Заметим, что наибольшей популярностью среди инсайдеров пользуются:

1. мобильные накопители (86,6%),
2. электронная почта (84,8%),
3. web-браузеры (82,2%),
4. ICQ клиенты (78 %).

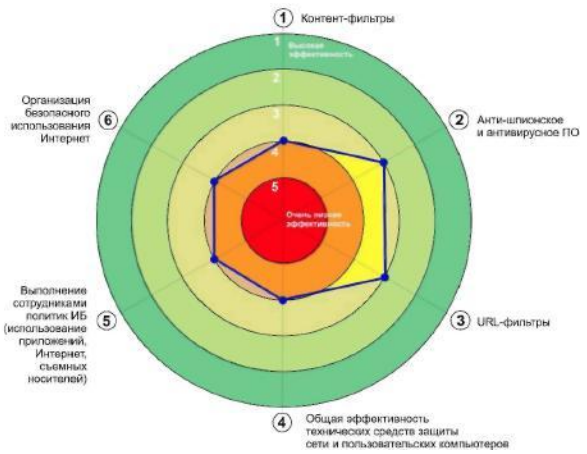
Отметим что, крайние три позиции соответствуют использованию Internet приложений, в случае если в организации не используется система контроля доступа и обмена информацией с глобальной сетью Internet.

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).

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

Уровень опасности выявленных Интернет-угроз



Эффективность используемых средств защиты и работы служб ИБ

Рис. 1.6

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).

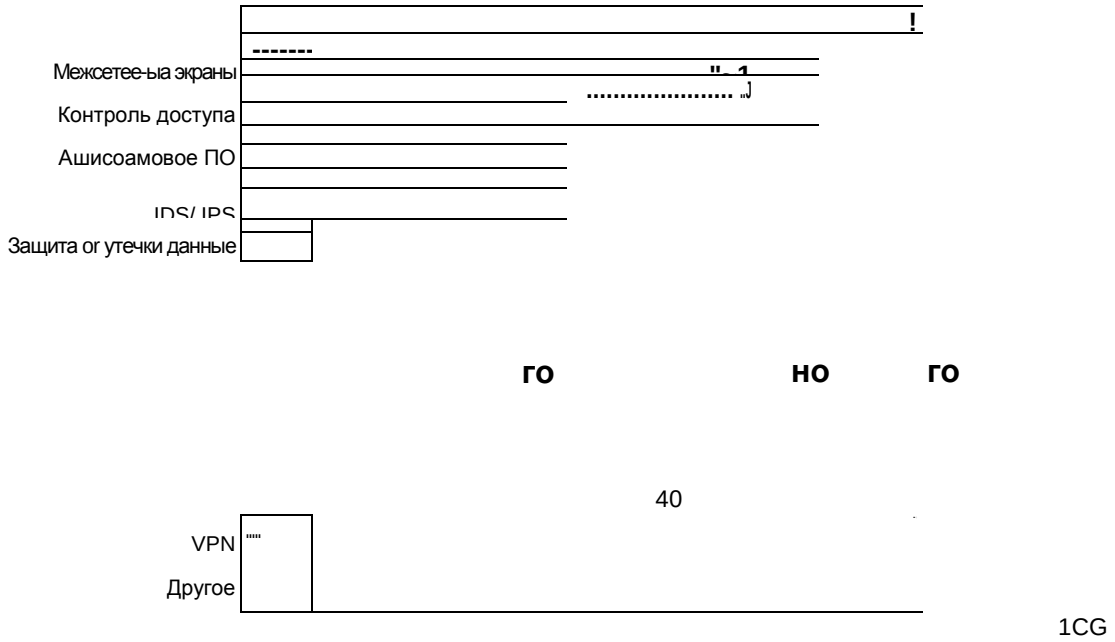


Рис. 1.7 - Средства обеспечения ИБ применяемые организациями

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.

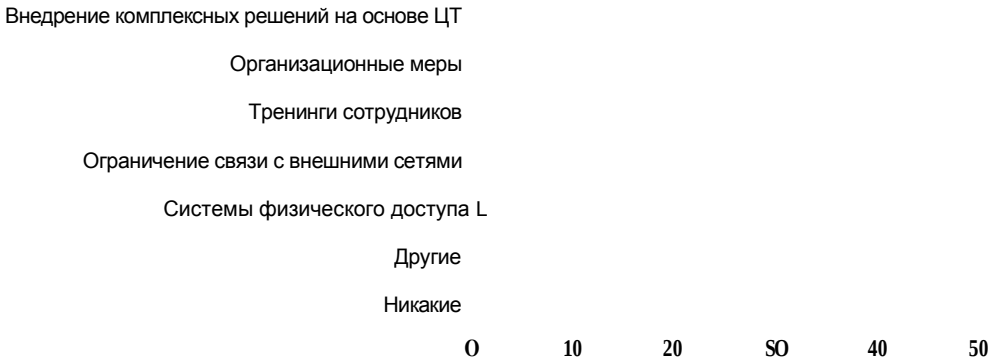


Рис. 1.8 - Наиболее эффективные средства обеспечения ИБ

Как отмечено в исследованиях [2-5] наиболее эффективным средством зашиты 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 планирую 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 защиту от утечек.

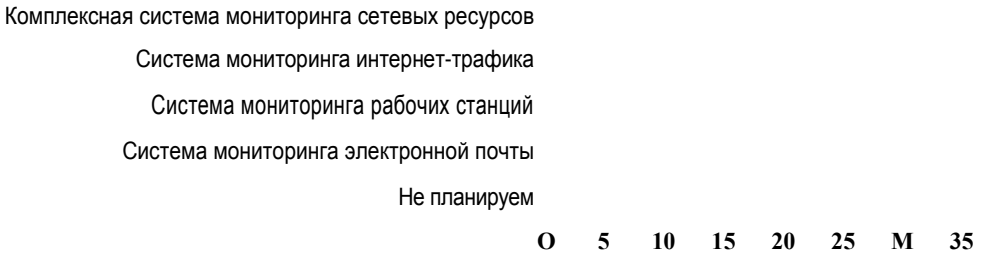


Рис. 1.9 - Планы по внедрению систем защиты ИБ

Как видно из ответов респондентов комплексные решения ИТ, а именно комплексные системы мониторинга сетевых ресурсов превалируют 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.