Содержание

Глава 2

Практика аудита безопасности корпоративных систем Internet/Intranet ... 73

Предисловие

Понятие *аудит информационной безопасности компании* появилось сравнительно недавно и сегодня вызывает постоянный интерес специалистов в области менеджмента и безопасности корпоративных систем Internet/Intranet. Примерно с 1995 года в ряде высокотехнологичных стран мира, главным образом в США, Великобритании, Германии и Канаде, проводятся ежегодные слушания и совещания специально созданных комитетов и комиссий по вопросам аудита информационной безопасности корпоративных систем. Подготовлено более десятка различных стандартов и спецификаций, посвященных аудиту информационной безопасности, среди которых наибольшую известность приобрели международные стандарты ISO 17799 (BS 7799), BSI и COBIT.

В настоящее время аудит информационной безопасности корпоративных систем Internet/Intranet представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области безопасности корпоративных систем Internet/Intranet. Его основная задача – объективно оценить текущее состояние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином *аудит информационной безопасности корпоративной системы Internet/Intranet* обычно понимается системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности. Считается, что результаты качественно выполненного аудита информационной безопасности компании позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Насколько аудит безопасности может быть полезен для вашей компании? Давайте посмотрим вместе. Не секрет, что сегодня наблюдается повсеместное усиление зависимости успешной бизнес-деятельности компании от корпоративной системы защиты информации. Объясняется это увеличением объема жизненно важных для компании конфиденциальных данных, обрабатываемых в корпоративной информационной системе Internet/Intranet. Этим же объясняются и дополнительные капиталовложения в информационные системы компании. В связи с этим актуальность аудита информационной безопасности резко возрастает. Более того, практика внедрения новых корпоративных информационных систем свидетельствует о том, что компании не всегда получают полную отдачу капиталовложений. Прежде всего, из-за усложнения современных корпоративных систем Internet/Intranet и роста их уязвимости. Можно выделить две основные причины роста уязвимости корпоративных систем Internet/Intranet. Во-первых, повысилась уязвимость собственно корпоративных информационных систем за счет обоснованного усложнения аппаратно-программных элементов этих систем, увеличения структурной

и функциональной сложности системного и прикладного программного обеспечения, применения новых технологий обработки, передачи и хранения данных. А во-вторых, расширился спектр угроз корпоративным информационным системам из-за передачи информации по открытым каналам сетей общего назначения, «информационных войн и электронных диверсий» конкурирующих организаций, активного промышленного шпионажа с привлечением профессионалов в области IT-security и пр.

Сегодня современный рынок безопасности насыщен средствами обеспечения информационной безопасности. Постоянно изучая существующие предложения рынка безопасности, многие компании видят неадекватность ранее вложенных средств в системы информационной безопасности, например, по причине морального старения оборудования и программного обеспечения. Поэтому они ищут варианты решения этой проблемы. Таких вариантов может быть два: с одной стороны — это полная замена системы корпоративной защиты информации, что потребует больших капиталовложений, а с другой — модернизация существующих систем безопасности. Последний вариант решения этой проблемы является наименее затратным, но несет новые проблемы, например, требует ответа на следующие вопросы: как обеспечить совместимость старых, оставляемых из имеющихся аппаратно-программных средств безопасности, и новых элементов системы защиты информации; как обеспечить централизованное управление разнородными средствами обеспечения безопасности; как оценить, а при необходимости и переоценить информационные риски компании. Более существенная причина необходимости проведения аудита безопасности состоит в том, что при модернизации и внедрении новых технологий защиты информации их потенциал полностью не реализуется. Здесь аудит позволяет оценить текущую безопасность функционирования корпоративной информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы компании, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов: стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных. В конечном счете грамотно проведенный аудит безопасности корпоративной информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание систем безопасности.

А для практики исключительно важным является то, что аудит информационной безопасности ориентирован как на специалистов в области безопасности корпоративных систем Internet/Intranet, так и на специалистов в области менеджмента. Такой подход устраняет существующее недопонимание специалистов в области информационной безопасности TOP-менеджерами компании. В данном случае они объединяются в единую команду, ориентированную на повышение экономической эффективности и рентабельности бизнес-деятельности компании. Еще один существенный плюс подобного подхода – поддержка полного жизненного цикла корпоративной системы защиты информации, начиная с анализа требований и заканчивая этапами эксплуатации и сопровождения системы. Примечательно,

что использование структурных и объектно-ориентированных CASE-средств анализа и управления рисками позволяет наглядно и эффективно представлять компоненты информационной инфраструктуры компании, выделять наиболее критичные из них, а также оценивать информационные риски компании. Компоненты представляются в удобной графической форме, с выделением существенных с точки зрения управления компанией компонентов ее информационной инфраструктуры и связей по управлению и данными между ними. Такая общая визуализация бизнес-процессов и информационной безопасности компании позволяет оперативно генерировать различные варианты защиты, сравнивать их между собой с точки зрения экономической эффективности и в результате выбирать оптимальный вариант построения или модификации защиты корпоративной системы Internet/Intranet.

В настоящее время многие поставщики средств защиты информации декларируют поставку полного, законченного решения в области безопасности корпоративных систем Internet/Intranet. К сожалению, в лучшем случае все сводится к проектированию и поставке соответствующего оборудования и программного обеспечения. Построение корпоративной системы безопасности «остается в тени» и к решению не прилагается. Поэтому у корпоративных заказчиков все чаще и чаще к поставщикам соответствующих решений возникают следующие вопросы:

- соответствует ли наша корпоративная система информационной безопасности целям и задачам бизнеса компании;
- насколько адекватна принятая в компании политика безопасности ее задачам и целям бизнеса;
- как корректно контролировать реализацию и выполнение политики безопасности в компании;
- когда необходимо провести модернизацию системы безопасности; как обосновать необходимость модернизации и затрат;
- как быстро окупятся инвестиции в корпоративную систему безопасности; где здесь точка безубыточности;
- насколько правильно и корректно сконфигурированы и настроены штатные средства обеспечения информационной безопасности компании;
- как убедиться в том, что существующие в компании средства защиты – межсетевые экраны (firewalls), системы обнаружения вторжений (IDS), антивирусные шлюзы, VPN-шлюзы – эффективно справляются со своими задачами;
- как решаются вопросы обеспечения конфиденциальности, доступности и целостности;
- подрядные организации и компании провели проектирование, поставку, монтаж, пуско-наладку средств безопасности. Как оценить их работу? Есть ли недостатки и, если есть, то какие;
- как обеспечить такую необходимую для практики «вертикаль власти» для централизованного управления безопасностью компании;
- как контролировать состояние информационной безопасности компании; какие методы и средства здесь необходимо использовать;

- корпоративная система обеспечения безопасности построена, что делать дальше? (Наличие стратегического и тактических Планов защиты компании, Планов работы при возникновении чрезвычайных ситуаций);
- есть ли необходимость постоянно обучать сотрудников службы информационной безопасности компании и какие бюджетные средства для этого нужны;
- как управлять информационными рисками компании; какие инструментальные средства для этого необходимо задействовать;
- удовлетворяет ли организация информационной безопасности компании требованиям международных стандартов оценки и управления безопасностью, например ISO 15408, ISO 17799 (BS 7799), BSI.

Очевидно, что на перечисленные вопросы *нельзя* мгновенно дать однозначный ответ. Только объективный и независимый аудит безопасности корпоративной системы Internet/Intranet позволит вам получить достоверную и обоснованную информацию. Такой аудит, который позволит комплексно проверить все основные уровни обеспечения информационной безопасности компании: *нормативно-правовой, организационный, технологический и аппаратно-программный*. А для того, чтобы вы были готовы к проведению аудита и смогли грамотно воспользоваться его результатами, и была задумана данная книга.

По мнению авторов, книга является первым полным русскоязычным практическим руководством по вопросам аудита информационной безопасности компаний и отличается от других источников, преимущественно изданных за рубежом, тем, что в ней последовательно изложены все основные вопросы аудита информационной безопасности: идеи, принципы, методология, формальные модели и методы, анализ выполнения конкретных аудиторских проверок информационной безопасности различных государственных и коммерческих организаций и структур.

Книга ориентирована на следующие основные группы читателей:

- *менеджеров высшего эшелона управления компанией (TOP-менеджеров)*, которые хотят получить ответы на следующие вопросы: что такое аудит информационной безопасности; в чем его суть; зачем и кому он нужен; насколько он актуален для компании и ее бизнес-деятельности; какова его стоимость и последующие затраты; каковы последствия для компании; какую роль играют инструментальные CASE-средства анализа и управления рисками; кто и как его осуществляет; какие существуют ограничения законодательного характера; какие отечественные и западные методики и технологии аудита предпочтительно использовать; как эффективно управлять информационной безопасностью компании в интересах бизнеса; как подготовить свою компанию к аудиту и аккредитации в соответствии с требованиями международных стандартов ISO 17799 (BS 7799), BSI и COBIT.
  Ответы на эти вопросы даются в главах 1–4;

- *руководителей служб автоматизации (CIO) и служб информационной безопасности (CISO),* которые желают получить объективную и независимую оценку текущего состояния информационной безопасности компании, оценить потенциальный экономический ущерб от возможных посягательств разного рода злоумышленников, выработать требования к корпоративной системе защиты информации, проверить адекватность и эффективность политики безопасности компании, рассчитать необходимые затраты на совершенствование корпоративной системы защиты информации и предпринять все необходимые меры организационно-управленческого и технического характера для повышения (адекватного обеспечения) уровня информационной безопасности компании. Ответы на эти вопросы даются в главах 2-4;
- *специалистов в области безопасности компьютерных систем, IT-менеджеров,* которые желают получить детальное представление об аудите информационной безопасности, достаточное для того, чтобы грамотно разбираться в этих вопросах, а возможно, и руководить работами, связанными с аудитом информационной безопасности своей компании.
  Этой категории читателей адресованы главы 1-4;
- *разработчиков систем защиты корпоративных систем Internet/Intranet и начинающих аудиторов.*
  Данная категория читателей сможет получить ответы на интересующие их вопросы в главах 1,2,4.

Книга также может использоваться в качестве учебного пособия студентами и аспирантами соответствующих технических специальностей, тем более что материалы многих глав основаны в том числе и на опыте преподавания авторов в Научно-информационном центре проблем безопасности компании Конфидент (www.confident.ru), а также в Санкт-Петербургском госуниверситете.

Книга написана кандидатом технических наук С. А. Петренко и кандидатом технических наук старшим научным сотрудником А. А. Петренко, за исключением следующих ее частей:

- главы 1 – написанной совместно с Мамаевым М. А. (Ланит);
- раздела 2.5.4 – написанного совместно с Панасенко С. П., Абрамовым А. В. (Анкад);
- разделов 4.1.1 и 4.1.3 – совместно со Шпак В. Ф. (СЗО РАН);
- приложения 1 – авторы Трубачев А. П., Егоркин И. В., Кобзарь М. Т., Сидак А. А. (Центр безопасности информации);
- приложения 2 – написанного совместно с Плескач Е. В. (Symantec);
- приложения 3 – авторы Кононов А. А., Бурдин О. А. (Лаборатория системного анализа процессов информатизации Института системного анализа РАН);
- приложения 4 – автор Вихорев С. В. (Элвис+).

Авторы выражают глубокую благодарность докторам технических наук профессорам Хомоненко А. Д., Рыжикову Ю. И., Кустову В. Н., Соколову Б. В., Ломако А. Г., кандидату технических наук профессору Ковалеву В. В., кандидату

технических наук Березину А. С., CISSR Шепелявому Д. А. за ценные советы и сделанные ими замечания по рукописи, устранение которых способствовало улучшению ее качества.

Авторы заранее выражают признательность всем читателям, которые готовы сообщить свое мнение о данной книге. Вы можете отправлять свои письма в издательство «ДМК Пресс» (editor-in-chief@dmkpress.ru) или в Управление по издательской деятельности «АйТи Пресс» компании «АйТи» (info@it.ru).

С уважением,
Сергей и Александр Петренко

Соглашения

Для упрощения зрительного восприятия материала в книге принят ряд соглашений.

Курсивом выделяются впервые встречающиеся в тексте термины, а также фрагменты текста, на которые следует обратить особое внимание.

`Моноширинным` шрифтом в книге помечены листинги – фрагменты программного кода (причем команды, даваемые клиентом, выделены **`полужирным`** шрифтом), названия и расширения файлов, а также информационные компоненты.

Полужирным шрифтом отмечены элементы интерфейса рассматриваемых программ (пункты меню, заголовки диалоговых окон, кнопок и др.)

Кроме того, в тексте принят ряд сокращений.

Перечень сокращений

АИС	Автоматизированная информационная система
БД	База данных
ЗБ	Задание по безопасности
ЗИ	Защита информации
ИБ	Информационная безопасность
ИР	Информационные ресурсы
ИТ	Информационные технологии
КИС	Корпоративная информационная система
КМ	Криптографический маршрутизатор
КЭС	Комплексная экспертная система
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОК	«Общие критерии» (международный стандарт ИСО/МЭК15408-99)
ОО	Объект оценки
ОС	Операционная среда
ОУД	Оценочный уровень доверия к безопасности
ПБО	Политика безопасности объекта оценки
ПЗ	Профиль защиты
ПИБ	Подсистема информационной безопасности
ПО	Программное обеспечение
СБД	Справочные базы данных
СЗИ	Система защиты информации
СИБ	Система информационной безопасности
СКЗИ	Система криптографической защиты информации
СУБД	Система управления базами данных
ТЗ	Техническое задание
УК	Управление конфигурацией

Введение

Статистика компьютерных преступлений, совершенных в России в последнее время, достаточно впечатляюща и наглядна, и речь идет о далеко не всех официально зафиксированных случаях. Так, например, в 1997–98 годах только в кредитно-финансовой сфере выявлено более 29,2 тыс. преступлений [49], большинство из которых совершено с использованием компьютерной техники. И если (по данным Главного информационного центра МВД РФ) еще несколько лет тому назад доля *явных* компьютерных преступлений от общего в кредитно-финансовой сфере числа составляла не более 2%, что в абсолютных цифрах насчитывало около сотни [55], то, например, в 2000 году по данным Управления «Р» зафиксировано 1375 компьютерных преступлений. При этом состав совершенных компьютерных преступлений определился следующим образом:

- 584 – неправомерный доступ к компьютерной информации;
- 258 – причинение имущественного ущерба путем обмана или злоупотребления доверием с применением компьютерной техники;
- 210 – мошенничество с применением компьютерной техники и телекоммуникационных сетей;
- 172 – создание, использование и распространение вредоносных программ для ЭВМ;
- 101 – незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации;
- 44 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

А «цена» одного компьютерного преступления составила в среднем 300–500 тысяч рублей, а в отдельных случаях и значительно больше.

Это далеко не все официально зарегистрированные случаи. По мнению юристов, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков более сложную, чем задачи, сопряженные с их предупреждением. Поэтому уровень латентности (скрытности) компьютерных преступлений определяется в настоящее время в 90%, а из оставшихся 10% выявленных компьютерных преступлений раскрывается только 1%.

Позволим себе процитировать некоторые «примеры из жизни», приведенные в книге Лукацкого А. В. [17], которые относятся к последнему временно^ му периоду.

Атака на Центр управления полетами: «...10 февраля 2000 года неизвестные хакеры взломали официальный сайт российского Центра управления полетами. По сообщению «Известий», в субботу 10 февраля на главной странице появилась надпись «Windows Rulezzzz». Взломщики воспользовались временным административным паролем. ...Никакие сведения похищены не были, а базы данных, содержащиеся на сервере, не пострадали».

Атака на Газпром: «В ноябре 2000 года ... злоумышленники осуществили несанкционированный доступ к компьютерной сети «Газпрома» и временно получили полный контроль над газовыми потоками. Об этом журналистов оповестил на брифинге в МВД РФ исполняющий обязанности начальника управления «Р» МВД полковник Константин Мачабели. ...В компьютерные сети «Газпрома» были внедрены 24 программы, называемые «троянскими конями», посредством которых и были получены соответствующие данные для успешной хакерской атаки. «В итоге Центральный пункт управления газовыми потоками стал временно подконтролен внешним пользователям», — подчеркнул представитель МВД».

Атака на базу данных компании Western Union: «Как сообщило агентство «Росбизнесконсалтинг», 8 сентября 2000 года компания Western Union, специализирующаяся на денежных переводах, объявила о том, что из-за «человеческого фактора» неизвестному злоумышленнику удалось скопировать информацию о кредитных карточках около 15,7 тыс. клиентов ее Web-сайта. Представитель Western Union сообщил, что взлом произошел, когда во время проведения регламентных работ были открыты системные файлы, доступ к которым во время штатной работы сайта имеют только администраторы».

Атака на Тульский оружейный завод: «Как сообщила газета «Новые Известия» (29 мая 2000 года), 17-летний студент Тульского университета с помощью примитивной программки, рассылаемой по электронной почте пользователям Internet, получил логин /пароль и украл около 70 часов онлайнового времени у Тульского оружейного завода. Сотрудники завода «засекли» его случайно: попытавшись войти в Internet, они обнаружили, что доступ заблокирован, хотя в Сети в это время никто из них не работал. В результате судебного разбирательства «хакеру» дали полтора года условно и конфисковали компьютер».

Атака на сайт спикера Госдумы: «По данным агентства «Инфоарт» 24 октября 2000 года состоялось официальное открытие сайта председателя Государственной Думы Геннадия Селезнева. Во время презентации выяснилось, что сайт уже успели взломать. В момент ознакомления непосредственно с сайтом по адресу www.seleznev.ru оказалось, что там совершенно не то, о чем было рассказано. Содержимое сайта было подменено».

Международный опыт уголовно-правовой классификации компьютерных преступлений, накопленный в ряде ведущих высокотехнологичных стран мира, позволил сформировать так называемые «Минимальный список нарушений» и «Необязательный список нарушений». Данные списки были разработаны государствами – участниками Европейского сообщества и официально оформлены как «Руководство Интерпола по компьютерной преступности» [15].

Так, например, «Минимальный список нарушений» содержит восемь основных видов компьютерных преступлений:

- компьютерное мошенничество;
- подделка компьютерной информации;
- повреждение данных ЭВМ или программ ЭВМ;
- компьютерный саботаж;

- несанкционированный доступ;
- несанкционированный перехват данных;
- несанкционированное использование защищенных компьютерных программ;
- несанкционированное воспроизведение схем.

А «Необязательный список» состоит из следующего перечня компьютерных преступлений:

- изменение данных ЭВМ или программ ЭВМ;
- компьютерный шпионаж;
- неразрешенное использование ЭВМ;
- неразрешенное использование защищенной программы ЭВМ.

Также существует ряд других классификаций компьютерных технологий, например *кодификатор рабочей группы Интерпола,* который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов [22]. В соответствии с данным кодификатором Интерпола все компьютерные преступления подразделяются на следующие основные группы.

Несанкционированный доступ и перехват:

- компьютерный абордаж;
- перехват;
- кража времени;
- прочие виды несанкционированного доступа и перехвата.

Изменение компьютерных данных:

- «логическая бомба»;
- «троянский конь»;
- компьютерный вирус;
- компьютерный «червь»;
- прочие виды изменения данных.

Компьютерное мошенничество:

- мошенничество с банкоматами;
- компьютерная подделка;
- мошенничество с игровыми автоматами;
- манипуляции с программами ввода/вывода;
- мошенничество с платежными средствами;
- телефонное мошенничество;
- прочие компьютерные мошенничества.

Незаконное копирование:

- компьютерные игры;
- прочее программное обеспечение;
- топология полупроводниковых устройств;
- прочее незаконное копирование.

Компьютерный саботаж:

- с аппаратным обеспечением;
- с программным обеспечением;
- прочие виды саботажа.

Прочие компьютерные преступления:

- с использованием компьютерных досок объявлений;
- хищение информации, составляющей коммерческую тайну;
- передача информации, подлежащая судебному рассмотрению;
- прочие компьютерные преступления.

До недавнего времени, а именно до 1 января 1997 года – даты вступления в действие нового Уголовного Кодекса Российской Федерации (УК РФ), в России отсутствовала возможность эффективно бороться с компьютерными преступлениями и нарушениями. Несмотря на явную опасность для отечественного бизнеса, данные посягательства не были противозаконными, то есть они не упоминались российским уголовным законодательством. Хотя еще до принятия нового УК в России была осознана необходимость правовой борьбы с компьютерными преступлениями.

Сегодня составы компьютерных преступлений (то есть перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в главе 28 УК РФ, которая называется «Преступления в сфере компьютерной информации» (приложение 2) и содержит три статьи: «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

В большинстве стран соответствующие нормы сильно рассредоточены по соответствующим УК либо даже по разным законам, так что *помещение их в одну главу* было несомненным успехом российских законодателей. В то же время следует заметить, что, например, американское законодательство более конкретно [21]. Действительно, в отличие от российских специалистов, агенты ФБР имеют четкое руководство к действию в виде части 18 Свода законов. Здесь содержится множество статей, параграфов и пунктов, однозначно классифицирующих, например, ответственность за *торговлю компьютерными паролями; за причинение ущерба передаче данных, повлекших за собой повреждение компьютера и информации; незаконный доступ к компьютеру, используемому правительством*, и т.д. К тому же ответственность за разного рода компьютерные преступления может составлять *до 30 лет тюрьмы или до 1 млн. долларов штрафа*. В ФБР введена стройная классификация с упоминанием и разбором типичных примеров: «Пирамида», «Операции с предварительно уплаченным взносом», «Спланированное банкротство» или «Мошеннические операции в телемаркетинге».

Характеризуя в целом текущее состояние отечественного нормативно-правового обеспечения информационной безопасности, специалисты отмечают, что сложность компьютерной техники, неоднозначность квалификации, а также трудность

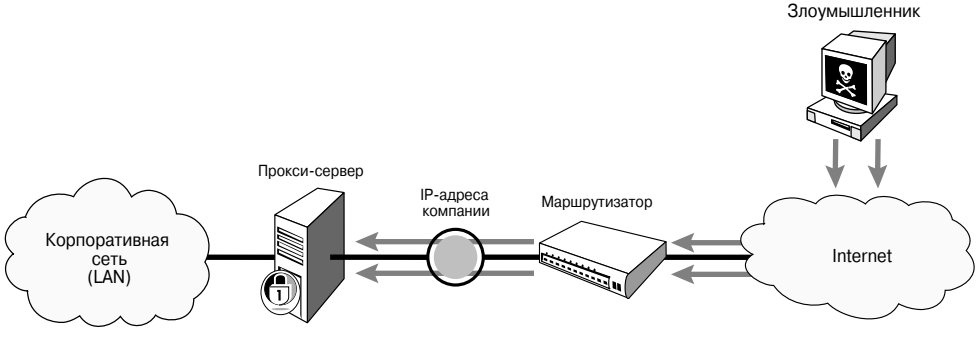
сбора доказательственной информации, по-видимому, не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272–274 УК РФ. Кроме того, предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения компьютерных преступлений и нарушений. Хотя, возможно, в этом случае придут на «помощь» статьи 146 УК РФ (нарушение авторских и смежных прав) и 147 УК РФ (нарушение изобретательских и патентных прав), дающие возможность уголовного преследования за незаконное использование программного обеспечения. Также эксперты отмечают неудачность формулировок статей главы 28 УК РФ. Поэтому, учитывая повсеместное подключение отечественных компаний к Internet, требуется, по-видимому, принять упреждающие меры уголовно-правового характера, заключающиеся в издании норм, пресекающих и предупреждающих различные компьютерные преступления и нарушения с учетом ее специфики. Тем не менее, позитивность произошедших перемен в российском правовом поле очевидна, и это внушает определенный оптимизм и надежду в эффективное обеспечение информационной безопасности российских компаний.

Внедрение и развитие технологий Internet/Intranet в отечественных компаниях и организациях стремительно продолжается и сегодня уже затрагивает все основные сферы отечественного бизнеса. Однако надо помнить, что такое развитие несет не только благо. Здесь, очевидно, стоит прислушаться к советам опытных в этих делах людей. Например, бывший директор ЦРУ Джон Дейч поставил электронную угрозу, ввиду ее значимости, в один ряд с такими страшными угрозами, как ядерная, химическая и бактериологическая. Сегодня корпоративные системы Internet/Intranet, соединенные с помощью открытых каналов связи в единую глобальную сеть, становятся прекрасными мишенями для проведения различных атак и являются уязвимыми для разного рода злоумышленников и в целом предоставляют возможность проведения самых настоящих электронных диверсий и информационных войн.

Отметим, что для современного общественного мнения характерен так называемый «синдром Робина Гуда» [55] – компьютерные злоумышленники представляются некими благородными борцами с противными толстосумами из числа представителей отечественного бизнеса. Поэтому противозаконные действия и компьютерные преступления в России, по-видимому, обречены на дальнейшее процветание. А раз так, то для поддержания и развития вашего бизнеса жизненно необходимо начать активно действовать и энергично принять действенные меры для обеспечения информационной безопасности компании. Здесь вовремя проведенный аудит безопасности вашей корпоративной системы Internet/Intranet позволит оперативно и объективно оценить текущее состояние информационной безопасности компании и своевременно принять соответствующие контрмеры на всех основных уровнях обеспечения безопасности, включая *организационно-управленческий и технический*.

ЧАСТЬ I

АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКИХ КОМПАНИЙ



Глава 1

Актуальность аудита безопасности для корпоративных пользователей

Глава 2

Практика аудита безопасности корпоративных систем Internet/Intranet

Несмотря на постоянное развитие технологий безопасности Internet/Intranet, практика обеспечения информационной безопасности в российских компаниях насыщена примерами инцидентов в этой области. Более того, число инцидентов неуклонно растет и начинает вызывать определенное беспокойство у сотрудников отечественных компаний и организаций, ответственных за организацию информационной безопасности. Сегодня можно указать как минимум три основные причины такого положения дел. Во-первых, возрастает роль информационных технологий в поддержке бизнес-процессов отечественных компаний, повышаются требования к качеству и безопасности процессов обработки, хранения и передачи данных, возрастает структурная и функциональная сложность корпоративных информационных систем, а следовательно, и возрастает цена ошибок и сбоев информационных систем. Во-вторых, эволюционное развитие Internet/Intranet-технологий приводит к появлению все бóльшего числа уязвимостей операционной среды, многочисленных служб и сервисов, а также протоколов TCP/IP, которые на практике ранее были не известны и не изучены, что в свою очередь приводит к росту уязвимости и незащищенности корпоративных информационных систем. В-третьих, постоянное усложнение компьютерных информационных систем повышает квалификационные требования к обслуживающему персоналу, приводит к усложнению процедур выбора решений и выполнения политики безопасности компании, обеспечивающих приемлемый уровень информационной безопасности при допустимом уровне затрат.

Как можно преодолеть или, по крайней мере, нейтрализовать указанные причины? Первая причина нейтрализуется способностью компании обеспечить возрастающие требования в области информационной безопасности. Вторая парируется постоянным отслеживанием и анализом выявленных уязвимостей с целью дальнейшего их оперативного устранения. Третья решается в рамках кадровой политики и определяется возможностью получения объективной информации о состоянии системы.

Давайте рассмотрим текущее состояние информационной безопасности российских компаний на всех основных уровнях обеспечения безопасности: *организационно-управленческом; технологическом; аппаратно-программном*. При этом рассмотрим сначала безопасность корпоративной системы Internet/Intranet глазами корпоративного пользователя, возможности аудита безопасности, а затем особенности проведения аудита в российских компаниях.

В заключении первой части книги дана оценка обеспечения информационной безопасности российских компаний. Показаны пути совершенствования существующих корпоративных систем защиты информации с учетом основных тенденций и перспектив развития технологий защиты информации в Internet/Intranet.

Глава 1

Актуальность аудита безопасности для корпоративных пользователей

1.1. Безопасность электронной почты

Электронная почта (наряду с FTP и Telnet) – один из самых первых сервисов, реализованных в компьютерных сетях. В настоящее время для многих компаний электронная почта является не менее важным средством связи, чем почта обычная. Давайте посмотрим, насколько безопасна работа с электронной почтой, какие подводные камни подстерегают вашу компанию при ее использовании и как их можно избежать. Мы предполагаем, что читатель знаком с организацией электронной почты на предприятии и с основами ее администрирования. Для более подробного знакомства с организацией электронной почты компании отсылаем читателя к книге и статьям [18–20].

Почта может быть опасной. Это известно еще с тех времен, когда изобрели ядовитые чернила и додумались вкладывать бомбы в посылки. Письма могут быть поддельными – это также хорошо известно. Электронная почта не представляет собой исключение, а скорее наоборот – дает злоумышленникам больше свободы для творчества. К счастью, электронные письма не взрываются и не колются отравленными шипами, но возможный экономический ущерб от атаки через электронную почту может быть весьма и весьма велик.

Безопасность электронной почты должна обеспечиваться как на уровне администратора сети, так и на уровне конечного пользователя. И если от администратора мы вправе ожидать определенного профессионализма в этой области, то ситуация с конечными пользователями гораздо сложнее. В общем случае пользователь не является специалистом по технологиям Internet и обучен работать с определенной почтовой программой без понимания деталей того, что происходит во время приема, отправки и чтения сообщений, и без способности идентифицировать и проанализировать «необычную» ситуацию. В большинстве случаев (возможно, это покажется парадоксальным) именно пользователь является агентом злоумышленника, с помощью которого последний осуществляет атаку. Поэтому служба электронной почты предприятия должна быть организована так, чтобы администратор мог перехватить как можно большее число потенциальных инцидентов еще до того, как в игру вступит пользователь. В частности, речь идет о политике

ретрансляции, способах аутентификации, сканировании вложений и других мерах, речь о которых пойдет ниже.

Сначала рассмотрим опасности электронной почты и борьбу с ними с точки зрения пользователя, а уже потом перейдем к работе администратора. Мы предполагаем, что читатель знаком с устройством и функционированием электронной почты и других технологий Internet.

1.1.1. Что подстерегает корпоративных пользователей

«Посылки с бомбами»

Поскольку опасность для компьютера пользователя могут представлять только запущенные на этом компьютере программы, пересылка текстовых сообщений совершенно безвредна, но любая программа, содержащаяся во вложении (*attachment*) к письму и неосторожно (либо автоматически) запущенная при его прочтении, может причинить компьютеру любой мыслимый вред. Такие «почтовые вирусы» получили в последнее время широкое распространение. Причиной этому является недостаточная компьютерная грамотность пользователей, о которой мы уже упоминали выше, а не какие-либо недостатки в системе электронной почты. Избежать поражения «почтовым вирусом» можно, следуя нескольким простым правилам:

- *никогда* не конфигурировать свою почтовую программу на автоматическое открытие (извлечение) приложений. Имейте в виду, что программа может быть изначально сконфигурирована в этом режиме, поэтому не поленитесь изучить настройки программы и проверить ее поведение на примерах (можете посылать письма с вложениями сами себе).
  Запомнить, что вложение в письме от *любого* корреспондента может быть вредоносной программой, даже – и особенно! – если это письмо от хорошо знакомого вам человека. Следует понимать, что письма отправляются в конечном счете не людьми, а программами, и программа, заразившая компьютер вашего друга, просто рассылает себя от его имени по всем адресам, обнаруженным в его адресной книге.
  Если ваша почтовая программа не проверяет вложения на наличие вирусов автоматически, то при получении письма с вложением его следует извлекать в отдельный файл на диске и проверять антивирусной программой. При получении письма с неизвестным вам типом файла или с неожиданным, неадекватным для данного отправителя приложением, попросите у отправителя разъяснений по поводу этого приложения (естественно, до того, как вы его откроете).
  Помнить, что не только `.exe`-файлы, но и файлы Visual Basic Script (`.vbs`), Miscrosoft Office (Word, Excel), файлы HTML, Postscript (`.ps`), Program Information File (`.pif`) в общем случае являются программами и могут содержать вредоносный код. Если вы не хотите вдаваться в подробности