Содержание

Приложение 1

Предисловие

В настоящее время *организация режима информационной безопасности* становится критически важным *стратегическим фактором* развития любой отечественной компании. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей российской нормативно-методической базы в области защиты информации. Вместе с тем многие ведущие отечественные компании сегодня используют некоторые *дополнительные инициативы*, направленные на *обеспечение устойчивости и стабильности функционирования корпоративных информационных систем для поддержания непрерывности бизнеса* в целом. В чем сущность этих инициатив и насколько они могут быть полезными для вашей компании? Давайте посмотрим вместе. Для этого сначала вспомним основные успехи развития российской нормативно-методической базы в области защиты информации в 2001–2003 гг., а затем остановимся на некоторых инициативах ведущих отечественных компаний.

В 2002 году в рамках деятельности Гостехкомиссии при Президенте РФ подготовлены и согласованы специальные требования и рекомендации по защите конфиденциальной информации, а также соответствующие методики. Летом 2002 года был утвержден ГОСТ Р ИСО/МЭК 15408-2002 (части 1, 2, 3) «Критерии оценки безопасности информационных технологий» на основе прямого применения международного стандарта ИСО/МЭК 15408-99. Продолжается работа над следующими нормативными документами по стандартизации (РД Гостехкомиссии):

- Руководство по разработке профилей защиты и заданий по информационной безопасности;
- Руководство по регистрации профилей защиты;
- Методика оценки профилей защиты и заданий по информационной безопасности;
- Автоматизированный комплекс разработки профилей защиты и заданий по информационной безопасности.

Кроме того, разрабатывается шесть профилей защиты для конкретных систем и средства информационных технологий, в том числе для некоторых операционных систем, межсетевых экранов и других компонент информационных технологий. В дальнейшем планируется создание более 20 профилей защиты.

В январе 2002 года в рамках деятельности ФАПСИ принят Федеральный закон «Об электронной цифровой подписи». С 1 июля 2002 года введена в действие новая версия стандарта ЭЦП ГОСТ РЗИ.10-01 на основе операций в группе точек эллиптических кривых. Новый стандарт по своим характеристикам, например криптостойкости и скорости, существенно превосходит предыдущий стандарт

ЭЦП. Продолжается подготовка отечественных нормативных документов для создания национальной инфраструктуры с открытым распределением ключей (Public Key Infrastructure – PKI) и национальной иерархической системы удостоверяющих центров.

Дополнительные инициативы отечественных компаний в области защиты конфиденциальной информации обусловлены ростом интереса со стороны директоров служб автоматизации (CIO), служб безопасности (CISO), а также исполнительных директоров (CEO) ведущих отечественных компаний к постановке и решению следующих задач:

- анализа информационных рисков компании и управления ими;
- оценки непрерывности бизнеса организации;
- оценки экономической эффективности корпоративных систем защиты информации;
- оценки совокупной стоимости владения (TCO) системы защиты информации;
- оценки возврата инвестиций (ROI) компании в информационную безопасность (ИБ);
- планирования и управления бюджетом на ИБ.

Основной из перечисленных задач является *анализ и управление информационными рисками*. Действительно, большинство руководителей, ответственных за организацию режима информационной безопасности, наверняка задавалось вопросом: «Как оценить уровень безопасности корпоративной информационной системы нашего предприятия для управления им в целом и определения перспектив его развития?». Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Российской Федерации. Поэтому выбор методов оценки уровня безопасности корпоративной информационной системы обязательно требует ответа на следующие вопросы: в соответствии с какими критериями и показателями производить оценку эффективности системы защиты информации, и в том числе – как оценить и/или переоценить информационные риски предприятия? Вот почему в дополнение к имеющимся требованиям, рекомендациям и руководящим документам Гостехкомисии при Президенте РФ и ФАПСИ приходится адаптировать к российским условиям и применять на практике методики международных стандартов (ISO 17799, ISO 9001, ISO 15408, BSI и пр.), а также использовать внутренние корпоративные методики количественного анализа информационных рисков и оценивания экономической эффективности инвестиций в защиту информации, например, методики совокупной стоимости владения (TCO) и возврата инвестиций (ROI).

Современные технологии анализа рисков позволяют оценить существующий уровень остаточных информационных рисков в отечественных компаниях. Подобная оценка особенно важна в тех случаях, когда к информационной системе предприятия предъявляются повышенные требования в области информационной безопасности. Сегодня есть ряд методик анализа информационных рисков, в том числе с привлечением CASE-средств, адаптированных к применению в отечественных

условиях. Существенно, что квалифицированно выполненный анализ информационных рисков позволяет:

- провести сравнительную оценку по критерию «эффективность–стоимость» различных вариантов защиты информации;
- выбрать адекватные контрмеры для защиты информации;
- оценить уровень остаточных информационных рисков компании.

Кроме того, инструментальные средства анализа рисков, основанные на современных базах данных и знаний в области защиты информации, дают возможность построить:

- структурные и объектно-ориентированные модели современных корпоративных информационных систем;
- модели угроз и модели рисков, связанных с отдельными составляющими элементами КИС, и таким образом выявлять те сегменты и объекты информационных систем, риск нарушения безопасности которых является критическим, то есть неприемлемым;
- различные модели защиты информационных систем, а также сравнивать между собой по критерию «эффективность–стоимость» варианты мер по защите (контрмер) и также вести контроль выполнения требований к организации режима информационной безопасности на предприятии.

По мнению авторов, настоящая книга является *первым полным русскоязычным практическим руководством по вопросам анализа информационных рисков и управления ими*. Основное отличие этой книги от других источников, преимущественно изданных за рубежом, заключается в том, что в ней последовательно изложены все основные идеи, методы и способы практического решения задач анализа информационных рисков и управления ими в различных государственных и коммерческих организациях и структурах.

Эта книга может быть полезна следующим основным группам читателей:

- руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), ответственным за организацию режима информационной безопасности, адекватного текущим целям и задачам бизнеса компании;
- внутренним и внешним аудиторам (CISA), которым приходится комплексно оценивать текущее состояние организации режима информационной безопасности компании на соответствие некоторым требованиям корпоративных, национальных и международных стандартов, например ISO 15408, ISO 17799, BSI, COBIT и пр.;
- менеджерам высшего эшелона управления компанией (TOP-менеджерам), занимающимся оценкой информационных рисков компании и их управлением.

Книгу могут также использовать в качестве учебного пособия студенты и аспиранты соответствующих технических специальностей, тем более что материалы многих глав основаны на опыте преподавания авторов в Московском и Санкт-Петербургском госуниверситетах.

Книга состоит из семи глав:

- Анализ рисков в области защиты информации;
- Управление рисками и международные стандарты;
- Технологии анализа рисков;
- Инструментальные средства анализа рисков;
- Аудит безопасности и анализ рисков;
- Анализ защищенности информационной системы;
- Выявление атак и управление рисками.

В первой главе показана роль и задачи анализа рисков и управления ими при организации режима информационной безопасности российских компаний. Подробно рассмотрена международная концепция обеспечения информационной безопасности компаний, а также различные подходы и рекомендации по решению задач анализа рисков и управления ими.

Во второй главе приведен обзор основных стандартов в области защиты информации и управления рисками: ISO 17799, ISO 15408, BSI, NIST, MITRE. Отмечены главные достоинства и недостатки существующих подходов к анализу информационных рисков и управлению ими.

Третья глава содержит описание основных технологий анализа рисков, возможных проблем и их решений, а также примеры разработки корпоративных методик анализа рисков. Кроме того, здесь представлен положительный практический опыт работы в данной предметной области.

В четвертой главе обсуждаются инструментальные средства для анализа рисков (COBRA, CRAMM, MethodWare, RiskWatch, Авангард). Даны рекомендации по использованию указанных средств при анализе рисков информационных систем.

Пятая, шестая и седьмая главы посвящены практике решения задач анализа защищенности и выявления атак. Показана взаимосвязь с задачей анализа рисков и управления ими, а также роль «активного аудита» и обнаружения вторжений для оптимизации рисков. Рассмотрены технология работ аудита безопасности и оценки эффективности обеспечения информационной безопасности в отечественных компаниях. Имеется пример построения корпоративной системы защиты информации на основе решений Symantec.

Книга написана кандидатом технических наук Петренко С. А. (CISO) и кандидатом технических наук Симоновым С. В., за исключением следующих ее частей:

- раздел 1.1 – совместно с Березиным А. С. (Элвис+);
- раздел 1.2 – совместно с Муравьевой И. В. (Конфидент);
- разделы 1.3.1, 3.2.4 – совместно с Нестеровым С. А. (СПбПГУ);
- раздел 3.2 – совместно со Шпак В. Ф. (СЗО РАН);
- главы 6 и 7 – соавтор Астахов А. (CISA, Вимм–Билль–Данн);
- приложение 1 – © KPMG, Российский член KPMG International, Швейцарская ассоциация, перевод 2002 г.;
- приложение 2 – © Эрнст энд Янг (СНГ) Лимитед, перевод 2002 г.;
- приложение 7 – совместно с Кисловым Р. И. (Конфидент) и Поповым Ю. И. (компания АйТи).

Авторы выражают особую благодарность докторам технических наук профессорам А. Д. Хомоненко, Ю. И. Рыжикову, В. Н. Кустову, Б. Н. Соколову, А. Г. Ломако и кандидату технических наук профессору В. В. Ковалеву за ценные советы и замечания по рукописи, которые помогли улучшить ее качество. Авторы благодарят кандидата технических наук А. А. Кононова за предоставленные материалы по экспертной системе «Авангард» и активное обсуждение глав книги.

Благодарим также центр GIAC и институт SANS в лице Стивена Нортката (Stephen Northcutt)) и Эрика Коула (Eric Cole), общество ISC [2] в лице CISSP Дмитрия Шепелявого, CISSP Чарльза Крессона Вуда (Charles Cresson Wood) и CISSP Шон Харрис (Shon Harris), ассоциацию ISACA в лице президента Лондонского отделения CISA Чарльза Мансура (Charles Mansour), CISA Андрея Дроздова (KPMG) и CISA Александра Астахова, а также компании «Эрнст энд Янг» (СНГ) в лице Мишель Мур и Cisco Systems в лице CCIE Максима Мамаева, CCIE Михаила Кадера, CCIE Мерике Кэо (Merike Kaeo).

Будем признательны всем читателям, которые готовы сообщить свое мнение о данной книге. Вы можете направлять письма в компанию АйТи по адресу: itpress@it.ru.

Глава 1

Анализ рисков в области защиты информации

1.1. Информационная безопасность бизнеса

В настоящее время проблемы обеспечения информационной безопасности корпоративных информационных систем (КИС) все чаще и чаще обсуждаются на страницах различных компьютерных изданий. При этом, как правило, значительное внимание уделяется описанию различных технических решений, анализу преимуществ и недостатков известных аппаратных и программных средств и технологий защиты информации. В меньшей степени затрагиваются вопросы и меры организационного обеспечения ИБ компании – стратегия и тактика защиты информации, концепция и политика безопасности, планы защиты информационных ресурсов компании в штатных и внештатных условиях функционирования КИС. При этом считается само собой разумеющимся, что данная проблема безусловно актуальна для представителей отечественного бизнеса. Однако за кадром остается вопрос: а каковы, собственно, интересы представителей отечественного бизнеса в решении этой проблемы? Ведь стандартных слов о том, что критичная для бизнеса информация должна быть *доступной, целостной и конфиденциальной*, здесь явно недостаточно, поскольку информация – понятие достаточно абстрактное; угрозы ее безопасности носят вероятностный характер (как известно, пока гром не грянет, никто ничего делать не будет), к тому же технические и организационные решения по безопасности стоят немалых денег!

Видимо, объяснение указанному явлению кроется в том, что обсуждается данная проблема в основном в среде технических специалистов или специалистов, имеющих явные «технические корни». Однако с уровня бизнес-управления компанией существование потенциальных угроз для информационных ресурсов компании и наличие критичных технических уязвимостей КИС «не видны», поэтому проблема обеспечения информационной безопасности КИС представляется весьма туманной. Зато вполне понятна такая постановка проблемы: стоит ли тратить деньги на корпоративную систему защиты информации, полезность которой для бизнеса далеко не очевидна? Более того, часто можно услышать такой вопрос: «А зачем нам вообще нужна информационная безопасность? На этом же нельзя заработать!» Или, если говорить на языке бизнеса, – зачем нам создавать еще один затратный центр? Их у нас и так слишком много! И с этими аргументами достаточно

трудно спорить. Особенно, если не владеть контраргументами, понятными для представителей отечественного бизнеса. К сожалению, часто российские директора и начальники служб автоматизации (CIO), исполнительные директора (CEO), начальники служб информационной безопасности (CISO) таких контраргументов не имеют, хотя интуитивно абсолютно уверены в необходимости решения данной задачи. Итак, что же нужно сделать, чтобы информационная безопасность воспринималась как один из корпоративных бизнес-процессов? Другими словами, как представить ИБ с точки зрения бизнеса?

Очевидно, для этого надо сначала попробовать определить бизнес-задачу ИБ. Одним из основных двигателей рынка автоматизации бизнеса является стремление самого бизнеса стать более эффективным и конкурентоспособным за счет использования современных информационных технологий и совершенствования своей собственной модели. Такое стремление вполне понятно: не так уж много осталось реальных механизмов повышения конкурентоспособности, и все они в основном уже исчерпаны, а информационные технологии предлагают поистине неограниченные возможности. В том, что в автоматизации бизнеса заложен огромный потенциал для его динамического развития, не сомневается сегодня, наверное, уже никто. Достаточно сравнить эффективность и оперативность работы, например, корпоративной электронной почты с эффективностью и оперативностью многочисленной армии секретарей и машинисток, качество и сроки разработки сложных технических систем посредством CAD/CAM/CAE-систем и с помощью традиционного кульмана и др. Можно сказать, что бизнес-задача КИС, как и любой другой технической системы, состоит в том, чтобы упростить, ускорить или сделать более удобными ранее рутинные и потому медленные и изобилующие ошибками бизнес-процессы. Или, если говорить более строго, любая действующая в интересах бизнеса техническая система в принципе должна предоставлять бизнесу какой-то тип сервиса. Сервис может быть самым разнообразным: доменная печь «оказывает услуги», выплавляя сталь, транспортный цех – транспортируя грузы, заводская столовая – обеспечивая питание сотрудников и т.д. Также и КИС, будучи сугубо технической системой, предлагает бизнесу свой тип сервиса – в данном случае сервис информационный. И этот сервис заключается в предоставлении бизнесу необходимой *для принятия решений* информации нужного качества, в нужное время и в нужном месте, то есть информации для *управления самим бизнесом*.

По своей сути информация постепенно становится одним из ключевых элементов бизнеса. Ведь что такое информация с точки зрения бизнеса? В сущности, это не что иное, как некий набор формализованных (в смысле структурированных, разложенных по полочкам и имеющих средства для поиска и представления) знаний бизнеса *о самом себе*. При этом под информацией можно понимать не только какие-то статичные информационные ресурсы, например бухгалтерский баланс за прошедший год или текущие настройки какого-либо оборудования, но и динамические информационные процессы обработки знаний в виде запрограммированной бизнес-логики работы компании в среде таких популярных приложений, как электронный документооборот, ERP, CRM, службы каталогов и др.

Времена Генри Форда, когда управляющий компанией самостоятельно привинчивал гайки на конвейере, давно миновали. Сегодня высшее руководство любой компании по существу имеет дело только с информацией – и на ее основе принимает решения. Понятно, что эту самую информацию готовят множество нижестоящих слоев достаточно сложной организационной системы, которая называется современным предприятием. И нижние слои этой системы вообще могут не иметь понятия о том, что они производят не только какую-то продукцию или услугу, но и информацию для руководства. По нашему мнению, глубинный смысл автоматизации бизнеса заключается как раз в том, чтобы ускорить и упорядочить информационные потоки между функциональными уровнями и слоями этой системы и представить руководству компании лишь самую *необходимую, достоверную и структурированную* в удобной для принятия решения форме информацию.

Заметим, информацию *достоверную*! Отсюда нетрудно сделать вывод, что ключевой бизнес-задачей корпоративной системы ИБ является обеспечение гарантий *достоверности* информации, или, говоря другими словами, гарантий *доверительности* информационного сервиса КИС.

Попробуем спросить любого представителя отечественного бизнеса, готов ли он потратить, скажем, сто тысяч долларов на закупку, например, пяти межсетевых экранов и ста лицензий на антивирусное ПО. А потом зададим тот же самый вопрос по-другому: готов ли он потратить сто тысяч долларов на защиту информации о самом себе и на защиту сервиса, на котором основано управление компанией? Скорее всего, ответ в первом случае будет таким: либо традиционное для России «Денег нет», либо, как в Одессе, вопросом на вопрос: «А зачем?». Во втором случае вариантов ответов больше: «В какие сроки управимся? А где вы были раньше?». И даже: «А почему так мало? Разве мой бизнес так мало стоит?».

Кроме того, по всей видимости, здесь последует другой интересный вопрос: «А почему именно сто тысяч, а не пятьдесят или, скажем, четыреста семьдесят пять?». И в таком случае CIO, CEO, CISO просто необходимо предоставить понятный для бизнеса ответ, аргументированный соответствующими экономическими выкладками. То есть по сути предложить обоснование стоимости системы ИБ для бизнеса.

Можно ли провести такой анализ и обосновать стоимость корпоративной системы защиты информации? Внимательный читатель, наверное, уже заметил, что в последнее время в печати все чаще и чаще появляются новые для ИБ темы: анализ угроз ИБ, анализ информационных рисков, оценка совокупной стоимости владения системой безопасности, оценка возврата инвестиций от такой системы и т.д. Все это в виде метрики и меры информационной безопасности представляет собой некий экономический инструментарий, преломленный в область ИБ, который и позволяет ответить на вопрос: «А почему сто тысяч?». И еще – это яркий показатель того, что наиболее «продвинутые» российские CIO, CEO, CISO уже пытаются на него ответить.

Посмотрим, как можно обосновать стоимость корпоративной системы защиты информации. По нашему мнению, таких подходов как минимум два.

Первый подход – назовем его наукообразным – заключается в том, чтобы освоить, а затем применить на практике необходимый инструментарий получения метрики и меры безопасности, а для этого привлечь руководство компании (как ее собственника) к оценке стоимости защищаемой информации, определению вероятностей потенциальных угроз и уязвимостей, а также потенциального ущерба. В этом случае от результатов таких оценок будет во многом зависеть дальнейшая деятельность CIO и CISO в области ИБ. Если информация не стоит ничего, существенных угроз для информационных активов компании нет, а потенциальный ущерб минимален – и руководство это *подтверждает* (!) – проблемой ИБ можно, наверное, не заниматься. Если же информация стоит определенных денег, угрозы и потенциальный ущерб ясны, то понятны и рамки бюджета на корпоративную систему ИБ. Существенно, что при этом становится возможным привлечь руководство компании к осознанию проблем ИБ и построению корпоративной системы защиты информации и заручиться его поддержкой.

Второй подход (назовем его практическим) состоит в следующем: можно попробовать найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования некоторая общая оценка разумной стоимости такой услуги, как страхование собственного автомобиля, составляет от 5 до 15% его рыночной цены – в зависимости от локальных условий эксплуатации, культуры и опыта вождения водителя, интенсивности движения, состояния дорог и т.д.

По аналогии с автострахованием можно вообще не заниматься ИБ в компании, и не исключен вариант, что принятый риск себя вполне оправдает. А можно потратить на создание корпоративной системы защиты информации немало денег, и все равно останется некоторая уязвимость, что рано или поздно приведет к утечке или хищению конфиденциальной информации. Поэтому эксперты-практики в области защиты информации нашли некий оптимум, позволяющий чувствовать себя относительно уверенно, – стоимость системы ИБ должна составлять примерно 10–20% от стоимости КИС – в зависимости от уровня конфиденциальности информации. Это и есть та самая оценка на основе практического опыта (best practice), на которую можно положиться. И на вопрос «А почему для создания адекватной целям и задачам бизнеса корпоративной системы защиты информации требуется сто тысяч долларов?» отвечать «Потому что на сегодняшний день стоимость нашей КИС составила один миллион долларов!».

Очевидно, что второй подход не лишен недостатков. Здесь, скорее всего, не удастся заставить руководство глубоко осознать проблемы ИБ. Но зато можно смело прогнозировать объем бюджета на ИБ и существенно сэкономить на услугах внешних консультантов.

1.2. Развитие службы информационной безопасности

Вместе с развитием любой отечественной компании (и ростом стоимости ее информационных активов) в той же мере развивается и служба информационной безопасности. При этом определение стратегии и тактики работы службы информационной безопасности становится одной из основных функций TOP-менеджмента компании. Действительно, сегодня успех реализации политики информационной безопасности компании зависит не только от организационных и технических решений в области защиты информации, но и от квалификации и компетентности соответствующих кадров. Вспомним известный тезис: «Кадры решают все!».

Покажем роль и место службы информационной безопасности в организационной структуре компании, а также попробуем сформулировать современные квалификационные требования к сотрудникам этой службы.

Возможная организационная структура TOP-менеджмента компании, ответственного за организацию режима информационной безопасности, представлена на рис. 1.1.

Согласно исследованию KPMG за 2002 год (см. приложение 1) в наиболее благополучных с точки зрения ИБ западных компаниях функцией обеспечения информационной безопасности занимается отдельное подразделение, наделенное полномочиями и имеющее поддержку высшего руководства компании. При этом почти в половине «успешных» компаний ответственность за ИБ закреплена за советом директоров, что наиболее характерно для финансового сектора. Действительно, непосредственное участие TOP-менеджмента организации требуется для корректного определения и постановки «правильных» целей и задач в области ИБ, позволяющих без ущерба для бизнеса компании обеспечивать информационную безопасность. Кроме того, как правило, только руководство компании способно поддержать обеспечение безопасности надлежащим уровнем инвестирования и другими необходимыми ресурсами.

В российских компаниях в настоящее время наблюдаются следующие основные тенденции развития службы ИБ:

- ранее (а зачастую и сейчас) в большинстве российских компаний проблемой информационной безопасности организации занимались отделы и службы автоматизации. Сегодня ведущие отечественные компании идут путем выделения подразделения информационной безопасности в отдельную службу с соответствующими организационными, кадровыми и финансовыми изменениями. При этом создаются две ключевые позиции специалистов, ответственных за информационную безопасность: CISO (Chief Information Security Officer) –