

1 Рынок услуг по управлению информационной безопасностью

Развитие современных информационных технологий, рост зависимости деятельности многих предприятий и учреждений от функционирования информационных систем и постоянное нарастание объемов и сложности информационных потоков привели к тому, что задачи обеспечения информационной безопасности стали требовать использования значительных ресурсов. В частности, финансовые средства, выделяемые на обеспечение информационной безопасности, занимают все большую долю в бюджетах предприятий, а текущее и стратегическое управление защитой информации требует большего внимания не только со стороны специалистов по информационным технологиям, но и со стороны руководителей и собственников предприятий. Зачастую необходимые ресурсы и усилия руководителей в этой сфере оказываются сопоставимыми с теми ресурсами, которые тратятся на осуществление основной деятельности предприятий. Таким образом, сложились предпосылки для формирования рынка различных услуг по обеспечению информационной безопасности, которые (услуги) помогли бы не только повысить эффективность защиты информационных ресурсов, но и оптимизировать издержки предприятий и организаций. Основными факторами, которые обусловили появление у предприятий потребностей в услугах сторонних предприятий, решающих задачи обеспечения информационной безопасности, и выделение услуг по защите информационных ресурсов в самостоятельную сферу бизнеса, стали:

- усложнение и постоянное развитие современных систем обработки, хранения и передачи информации;
- усложнение программных и аппаратных средств, используемых для защиты информации, необходимость понимания сложного комплекса теоретических и методических вопросов для их эффективной эксплуатации;
- рост числа инцидентов и разнообразия видов атак на информационные системы и их интенсивности;

Тема 2.9 – Планирование и управление информационной безопасностью в условиях рынка
(Планирование и управление информационной безопасностью)

- нехватка квалифицированных специалистов в сфере информационной безопасности и рост затрат на их содержание и профессиональную подготовку.

- Причиной того, что предприятия оказываются заинтересованными в отказе от самостоятельного выполнения определенных функций и привлечения сторонних специализированных компаний для решения этих задач (в современной практике такой подход принято называть «аутсорсингом» или «передачей на аутсорсинг»), является возможность повысить эффективность процессов защиты информации, в определенной мере сократить издержки на эти процессы, а также в большей степени сконцентрироваться на управлении основной деятельностью предприятия и не отвлекать ресурсы и время руководителей на решение задач, являющихся по своей сути вторичными и вспомогательными по отношению к основным целям и задачам деятельности предприятия. Более высокая эффективность работы специализированных компаний – поставщиков услуг в сфере информационной безопасности по сравнению с самостоятельным решением этих задач самими предприятиями, как правило, связана с тем, что высокие издержки распределяются между множеством предприятий – клиентов поставщика услуг. Характерными примерами таких расходов, которые, с одной стороны, могут оказаться непозволительными для одного предприятия, но, с другой стороны, могут быть эффективно распределены между несколькими предприятиями, являются:

- найм высококвалифицированных специалистов в относительно узких дисциплинах и областях информационной безопасности (таких как использование криптографических средств, борьба с вирусами, внедрение виртуальных частных сетей и пр.);

- частое переобучение и повышение квалификации специалистов;

- постоянное отслеживание новых угроз и глубокий качественный анализ текущего состояния информационных технологий и тенденций их развития;

- приобретение специализированных программных и аппаратных средств, необходимых для защиты информации и аудита информационных систем;
- обеспечение круглосуточного дежурства служб реагирования на инциденты.

При всех преимуществах передачи отдельных задач обеспечения безопасности на аутсорсинг этот подход имеет и ряд недостатков, которые в определенной мере могут ограничивать его применение:

1) Предприятие, которое пользуется такими услугами, несколько ограничивает себя в возможностях управлять своими затратами и сокращать издержки (накладные расходы) и, таким образом, попадает в определенную зависимость от ценовой политики поставщиков услуг, а также от складывающейся конъюнктуры рынка.

2) Сотрудники компании, предоставляющей услуги, получают доступ к наиболее важной информации предприятия-клиента и его информационным системам, что потенциально может быть источником дополнительных рисков для информационной безопасности.

3) Возникают дополнительные угрозы информационной безопасности при взаимодействии между компанией-поставщиком и предприятием-клиентом в процессе оказания услуг (например, может быть перехвачена информация при удаленном администрировании информационных систем предприятия-клиента).

Основными услугами, которые могут быть переданы на аутсорсинг (как по отдельности, так и в комплексе), являются:

- услуги по проведению комплексных аудитов состояния информационной безопасности на предприятии;
- услуги по проведению аудитов (инструментальных проверок) устойчивости и надежности отдельных информационных подсистем (сетей,

программных и аппаратных платформ и пр.) и средств защиты информации, используемых предприятием;

- услуги по сертификации информационных систем, производимых программных и аппаратных средств защиты информации;

- консультационные услуги, связанные с формированием стратегии предприятия в сфере информационной безопасности и разработкой политики безопасности;

- услуги по проектированию системы защиты информации;

- консультационные услуги по выбору и адаптации отдельных технологий защиты информации (криптографии, биометрической идентификации и пр.) применительно к определенным условиям ведения бизнеса;

- услуги по внедрению системы защиты информации, а также внедрению отдельных технических (программных и аппаратных) средств и реализации организационных мероприятий;

- услуги по текущему администрированию, поддержке и сопровождению информационных систем и систем защиты информации;

- услуги по реагированию на инциденты, связанные с нарушениями информационной безопасности;

- услуги по обучению руководителей предприятия, специалистов службы информационной безопасности и ИТ-службы, а также пользователей информационной системы предприятия.

Также в конце этой главы мы рассмотрим еще два вида услуг, связанных с обеспечением информационной безопасности: услуги по страхованию информационных рисков и услуги по поддержанию инфраструктуры публичных ключей (Public Key Infrastructure, PKI).

В целом, к настоящему моменту сложно говорить о формировании полноценного рынка услуг в сфере информационной безопасности (особенно в России), так как у большинства менеджеров крупных, а особенно средних и

малых предприятий в основном не сформировались представления о необходимых мерах в этой сфере, а финансирование работ по обеспечению информационной безопасности зачастую осуществляется по остаточному принципу. Некоторые крупные российские разработчики комплексных решений в сфере информационной безопасности, хотя и функционируют достаточно активно, но при этом фактически не являются участниками открытого рынка, так как их продукция и услуги практически полностью ориентированы на определенных потребителей в государственном секторе, таких как ФСБ, Минатом и другие. Еще одной важной особенностью рынка услуг в сфере информационной безопасности является то, что оказание таких услуг иногда становится «побочным», дополнительным видом (направлением) деятельности для компаний, занимающихся поставкой аппаратных и программных средств защиты информации (так называемых «коробочных продуктов»), а также для компаний, занимающихся разработкой комплексных решений по автоматизации предприятий. Возможным недостатком такого подхода потенциально может быть то, что консультанты и аналитики оказываются жестко «привязаны» к определенным программным и аппаратным средствам (производителям, торговым маркам) и не имеют возможности гибко подбирать отдельные средства защиты и формировать наиболее эффективные комплексные решения в соответствии с потребностями каждого конкретного предприятия.

Тем не менее, несмотря на определенные недостатки в развитии рынка услуг по обеспечению информационной безопасности, неоспоримым фактом является то, что многие такие услуги уже представлены на рынке, а основные рыночные и организационные механизмы начинают отрабатываться на практике. При этом одной из рекомендаций при работе с предприятиями-поставщиками услуг в сфере информационной безопасности является правило - пользоваться услугами нескольких разных предприятий и периодически менять партнеров, обеспечивающих решение тех или иных проблем безопасности.

2 Характеристики услуг управления информационной безопасностью

Каждый вид услуг в этой сфере имеет свои специфические характеристики как с точки зрения организации работы компаний, оказывающих услуги, так и с точки зрения структуры рынка. Соответственно, для эффективной работы необходим индивидуальный подход к организации оказания таких услуг, а также организации взаимодействия между потребителями и поставщиками услуг.

1) Услуги по реагированию на инциденты (нарушения информационной безопасности), уже частично рассмотренные в одном из предыдущих разделов, являются одним из наиболее характерных примеров обоснованности и целесообразности передачи сервисов безопасности на аутсорсинг. В частности, целесообразность отказа от самостоятельного выполнения функций реагирования на инциденты и их (функций) централизации в специализирующейся на таких задачах компании связана с тем, что эта деятельность имеет следующие важные особенности:

- требует постоянного (круглосуточного) дежурства, что предполагает содержание в штате как минимум пяти специалистов;
- предполагает наличие высококвалифицированных (а следовательно, высокооплачиваемых и востребованных на рынке труда) специалистов, способных быстро предпринять эффективные меры противодействия возникающим угрозам (в том числе и применить контрмеры к нападающим в процессе длящейся атаки), а также самостоятельно принять необходимые решения в процессе отражения длящейся атаки;
- загрузка дежурных специалистов, отвечающих за реагирование на инциденты, может быть крайне неравномерной.

Таким образом, эффект от централизации функций, связанных с реагированием на инциденты, складывается из нескольких составляющих и предоставляет возможности как для сокращения затрат и повышения уровня

защищенности предприятий-клиентов, так и для получения прибыли предприятиями-поставщиками таких услуг.

При этом разграничение функций между предприятием-клиентом и компанией-поставщиком услуг может зависеть от таких факторов, как:

- уровень доверия предприятия-клиента к предприятию-поставщику услуг;
- сложившаяся практика оказания таких услуг и наличие у предприятий-поставщика необходимых специалистов с определенным уровнем квалификации;
- состав, характеристики и функциональность информационных систем предприятия-клиента;
- уровень квалификации сотрудников предприятия-клиента (как пользователей информационных систем, так и сотрудников департамента информационной безопасности);
- оценка существующих рисков (вероятности нанесения ущерба);
- оценка (в том числе и субъективная) того, насколько значимым является знание внутренней среды предприятия сотрудниками службы информационной безопасности и их способность «изнутри» координировать действия и решать проблемы в случае каких-либо инцидентов.

Кроме того, в некоторых случаях могут существовать определенные законодательные ограничения на аутсорсинг процессов безопасности (в частности, для государственных предприятий).

2) Основные вопросы проведения аудитов информационной безопасности (и, в частности, внешних аудитов) уже рассматривались нами в предыдущей лекции. Помимо уже указанных факторов, которые обуславливают необходимость проведения именно внешних аудитов, а не внутренних (более высокая квалификация специалистов, право делать заключения о соответствии международным стандартам и пр.), важным является также и то обстоятельство, что внешние аудиторы, как правило, не заинтересованы в

представлении необъективной информации (в отличие от внутренней службы информационной безопасности). В случае же, если предприятие захочет создать собственную независимую службу для проведения аудитов информационной безопасности (отдельно от департамента информационной безопасности и других подразделений предприятия), результатом могут оказаться очень большие затраты, тем более что частота проведения таких аудитов, как правило, является не очень большой.

3) Необходимость прибегать к услугам специализированных предприятий, связанным с проверкой защищенности и надежности отдельных элементов информационной инфраструктуры (серверов, сетей, межсетевых экранов и пр.), обусловлена, как правило, наличием у этих предприятий специализированных программных и аппаратных средств, необходимых для проведения таких проверок (например, специализированных сканеров уязвимостей), а также наличие специальных знаний и навыков и разностороннего опыта, накопленного в процессе практической работы при проведении подобных проверок на различных предприятиях. Приобретение подобного опыта в рамках одного предприятия, пусть даже и очень крупного, практически невозможно.

Одним из наиболее эффективных приемов при проведении такого рода проверок является пробное (тестовое) преодоление защиты, когда проверяющий имитирует определенное нападение с целью совершить нарушение (разрушить базу данных, выкрасть конфиденциальную информацию и пр.). Основными задачами проверок такого рода являются:

- оценка эффективности используемых технических (программных и аппаратных) средств защиты информации;
- оценка эффективности работы специалистов, ответственных за реагирование на инциденты;
- контроль соблюдения сотрудниками предприятия требований политики безопасности.

Для получения наиболее достоверных результатов желательно, чтобы на самом предприятии о проведении такого теста знали только несколько руководителей, ответственных за его организацию. Также важным условием проведения такой проверки является четкая договоренность о том, насколько далеко должна зайти атака и какой уровень проникновения и разрушительных действий является достаточным, для того чтобы достоверно продемонстрировать, что атакуемая (проверяемая) система является уязвимой. В любом случае вся ответственность за ущерб, нанесенный в результате осуществления такой проверки, полностью ложится на предприятие, заказавшее такую услугу.

3) Консультационные услуги, связанные с первичной постановкой системы управления информационной безопасностью (первичным анализом, формированием и внедрением политики безопасности), обычно бывают необходимы в той ситуации, когда предприятие впервые ставит для себя задачу целенаправленного систематического комплексного обеспечения информационной безопасности. В этих условиях привлечение сторонних консультантов является практически единственным способом сформировать достаточно адекватную и эффективную политику безопасности в относительно короткие сроки, так как само предприятие в такой ситуации обычно не имеет необходимых специалистов и руководителей, которые могли бы решить весь комплекс задач, связанных с оценкой рисков, инвентаризацией информационных активов, выработкой стратегии, формированием политики и организационной структуры департамента информационной безопасности.

Привлекаемая для решения всех этих задач консультационная компания должна будет провести анализ деятельности предприятия в нескольких разрезах: с точки зрения основных бизнес-процессов, с точки зрения имеющейся информационно-технологической и коммуникационной инфраструктуры, а также с точки зрения используемых приложений (программного обеспечения и баз данных). Таким образом, необходимое качество работы по обеспечению комплексной защищенности

информационных ресурсов предприятия может быть достигнуто только в том случае, если у консалтинговой компании имеются необходимые специалисты, а также опыт работы как на подобных предприятиях, так и с подобными программными и аппаратными платформами. Высокие требования к квалификации специалистов, работающих в консалтинговых компаниях, объясняются необходимостью не просто понять особенности функционирования тех или иных бизнес-процессов и информационных систем, но и достаточно быстро оценить их слабые места, существующие риски и наиболее вероятные сценарии нанесения ущерба информационным ресурсам.

4) Услуги по администрированию информационных систем и средств защиты информации могут предоставляться как в комплексе с услугами по реагированию на инциденты, так и независимо от них. Предприятия-поставщики услуг могут осуществлять администрирование таких систем, как:

- электронная почта (защита от вирусов, спама, нарушения конфиденциальности и других нарушений политики безопасности);
- сетевое оборудование (сбор и анализ информации о функционировании маршрутизаторов, серверов и других устройств);
- брандмауэры (конфигурирование и настройка доступа к сети, а также обеспечение своевременного реагирования на различные нарушения);
- системы обнаружения вторжений (отслеживание всех «подозрительных» действий в отношении сетей, серверов, приложений и баз данных).

При этом предприятие-клиент может прибегать к услугам других предприятий для контроля за тем, насколько эффективно осуществляется администрирование средств защиты информации, либо самостоятельно осуществлять такой контроль при помощи специальных сканеров.

При оказании услуг по администрированию предприятия-поставщик, как правило, не может взять на себя полную ответственность за сохранность информации (так же как и при оказании услуг по реагированию на инциденты),

однако для установления формальных отношений предприятие-клиент и предприятия-поставщик могут выработать Соглашение об уровне обслуживания, которое должно предусматривать основные параметры функционирования информационных систем и их защищенности (гарантированное время надежной работы систем, гарантированные сроки восстановления работоспособности при нарушениях и пр.).

3 Инфраструктура публичных ключей

Инфраструктура публичных ключей (Public Key Infrastructure, PKI) представляет собой сложную организационно-техническую систему, основанную на современных технологиях и развитых организационных стандартах, которая позволяет эффективно решать некоторые ключевые проблемы информационной безопасности и, в частности, проблемы защиты данных, передаваемых по сетям (как локальным, так и глобальным), и идентификации сторон, участвующих в информационном обмене (пользователей, информационных систем, программных процессов). Технология PKI является основным инструментом, при помощи которого на основе законодательной базы (в частности, на основе Федерального Закона РФ «Об электронной цифровой подписи», принятого в 2002 году) может быть создан юридически значимый документооборот, который, в свою очередь, может стать основой для активного развития электронной торговли, оказания финансовых, информационных и других услуг, а также осуществления электронных платежей через информационные сети общего пользования. Возможность использования этой технологии для осуществления платежей и хозяйственных сделок связана с тем, что ее самым важным элементом является так называемый цифровой сертификат, выдаваемый третьей стороной, которая фактически является гарантом того, что сделки, совершаемые с использованием определенного цифрового сертификата, совершаются от имени определенного лица. Таким образом, одним из ключевых элементов инфраструктуры публичных ключей являются так называемые «удостоверяющие центры»² (Certificate Authority, CA) – организационные структуры, осуществляющие

идентификацию личностей (если речь идет о выдаче сертификата для одного человека) и выдачу электронного сертификата установленного образца, однозначно и достоверно представляющего этого человека. Также эти центры решают множество дополнительных задач, связанных с обеспечением эффективной работы инфраструктуры публичных ключей: ведут списки аннулированных сертификатов, обновляют истекшие сертификаты и пр. В целом вся совокупность используемых технических и организационных решений, а также действующая юридическая база дают возможность однозначно связывать цифровой сертификат (цифровую подпись) с определенным физическим лицом и также гарантировать, что не происходит нарушения целостности передаваемых сообщений.

В настоящее время достаточно хорошо разработаны базовые технические стандарты и информационные технологии (средства криптографии, алгоритмы, реализующие хэш-функции и пр.), необходимые для построения средств защиты на основе PKI. Дальнейшие перспективы развития в данной сфере связаны, главным образом, с совершенствованием рынка услуг и организационных механизмов.

Идеология работы PKI предполагает создание сетей и иерархически взаимосвязанных структур множества различных удостоверяющих центров, работающих в рамках единой согласованной политики и опирающихся на общий «корневой» удостоверяющий центр. На практике же наиболее распространено создание самостоятельных разрозненных удостоверяющих центров, создаваемых отдельными предприятиями (например, коммерческими банками) на основе тиражируемых программных и аппаратных решений для обеспечения защищенности и придания юридической значимости создаваемым документам и транзакциям, осуществляемым в корпоративных информационных системах (таким как, например, платежные поручения) служащими, клиентами и бизнес-партнерами предприятия. В случае если предприятие самостоятельно развертывает PKI в рамках собственной информационной системы, все взаимоотношения между администрацией и

пользователями регулируются внутренней политикой, вопросы разработки которой были рассмотрены в предыдущей главе.

При этом одним из возможных подходов к внедрению технологии РКІ является передача функций, связанных с выдачей и дальнейшим обращением цифровых сертификатов, на аутсорсинг. Передача функций удостоверяющего центра сторонней специализированной компании, как правило, решает для предприятия две важных задачи:

- позволяет избежать значительных расходов, связанных с закупкой и поддержанием программных и аппаратных средств, а также наймом и обучением персонала;
- дает возможность применять цифровые сертификаты за пределами своего предприятия, а также использовать на предприятии сертификаты сотрудников других предприятий.

В свою очередь, компания, выполняющая функции удостоверяющего центра, может передать часть работ, которые связаны с проверкой документов лиц, претендующих на получение сертификата, и их консультированием, своим партнерам – так называемым «регистрационным центрам». Их основная функция заключается в упрощении и ускорении процедуры проверки документов и идентификации личности при выдаче сертификата для лиц, которые не могут лично явиться в удостоверяющий центр.

Именно на основе сетей регистрационных центров, а также взаимодействия различных удостоверяющих центров (их объединения в единую сеть) должно происходить построение универсальной общедоступной инфраструктуры публичных ключей. Предполагается, что основными пользователями – клиентами удостоверяющих центров, желающими получить цифровые сертификаты, – должны быть лица, заинтересованные в доступе к различным специализированным электронным сервисам, облегчающим взаимодействие как с различными коммерческими структурами (например, банками), так и с государственными органами. Однако на практике

продвижение технологии РКІ и ее широкое использование сильно затруднено в связи с множеством объективных и субъективных факторов, таких как:

- неготовность многих предприятий и особенно государственных органов к использованию данной технологии и, в частности, к параллельному использованию как обычных «бумажных» документов, так и электронных (заверенных электронными подписями);
- отсутствием у многих людей достаточных навыков обращения с компьютерной техникой, а также доступа в сеть Интернет;
- отсутствием у многих людей культуры использования электронных документов и электронной подписи, за которую необходимо нести ответственность;
- ограниченная совместимость некоторых средств защиты информации, используемых в России, со средствами защиты информации, применяемыми в других странах.

В результате перспективы решения важных организационных задач, таких как унификация технологий электронно-цифровой подписи и развитие общефедеральных удостоверяющих центров, оказываются неопределенными и во многом зависят от квалификации отдельных представителей профессионального сообщества и их отношения к данной проблеме.