Кокутин С.А. Аутсорсинг – как технология повышения качества ИТ-безопасности предприятия [Электронный ресурс] // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал. 2013. – № 5(15). Режим доступа http://iea.gostinfo.ru/files/2013_05/2013_05_13.pdf

УДК 338.49

АУТСОРСИНГ – КАК ТЕХНОЛОГИЯ ПОВЫШЕНИЯ КАЧЕСТВА ИТ-БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кокутин С.А. ФГУП «Российский научно-технический центр информации по стандартизации, метрологии и оценке соответствия» (ФГУП «СТАНДАРТИНФОРМ»)

В статье рассматриваются вопросы внедрения аутсорсинга информационной безопасности в компаниях, организациях, на предприятиях, как бизнес-технологии, способствующей качественному обслуживанию и управлению системой безопасности.

Ключевые слова: аутсорсинг, информационная безопасность, качество.

UDC 338.49

OUTSOURCING – HOW TECHNOLOGY IMPROVING THE QUALITY OF THE ENTERPRISE IT-SECURITY

Kokutin S.A. FGUP «Russian Research and Development Information Center on Standartization, Metrology and Compliance Check» (FGUP «STANDARTINFORM»)

The article deals with the implementation of outsourcing information security in companies, organizations, enterprises as the business-technology conducive quality service and security system management.

Keywords: outsourcing, information security, quality.

Век информационных технологий предъявляет особые требования к информационной безопасности корпораций, предприятий, организаций. Их стремительно развивающаяся инфраструктура включает не десятки устройств, а сотни, а порой и тысячи. В ведущих компаниях вопросам информационной безопасности уделяется серьезное внимание, при этом они

не исчерпываются лишь защитой компьютерных сетей, а включают совокупность организационно-технических мероприятий, проводимых по разным направлениям, имеющих целью обеспечить непрерывность ведения бизнес-процессов. Отсюда вытекает закономерность, что эффективное функционирование системы информационной безопасности требует надежного управления.

Информационная безопасность для подавляющего большинства крупных и многих средних компаний, которые прошли период массового внедрения ИТ, вышла на уровень бизнеса-процессов. В ИТ-системе стали храниться и обрабатываться действительно важнейшие данные, необходимые для существования и выживания бизнеса. В результате для многих компаний вопрос сохранения информации и поддержания целостности ИТ-систем и ИТ-инфраструктуры из второстепенных задач превратился в первостепенную, требующий достаточных финансовых затрат. Другим важным показателем повышения значимости ИБ является серьезное увеличение числа компаний, где выделен ИБ-отдел или отдельный сотрудник, ответственный за ИБ (по данным компании LETA, среди компаний с парком ПК более 200, уже у 70% есть выделенные специалисты по ИБ).

Но в тоже время, по оценкам отечественных специалистов в области информационной безопасности, ее уровень в российских компаниях на сегодняшний день, не достаточно высок. Однако, темпы развития данной области вселяют определенный оптимизм. Это обусловлено не только принятыми новыми нормативными актами и законами, среди которых особое место занимают Федеральный Закон РФ № 152-ФЗ, PCI DSS, СТО БР [1], но и осознанием со стороны руководства того, что проблемами информационной безопасности следует заниматься целенаправленно и систематично. В противном случае риск потери инфраструктурных элементов достаточно велик, что впоследствии, непременно приведет к реальным финансовым убыткам.

За примерами ходить далеко не следует, так, в 2010 г. наиболее распространенными угрозами стали, направленные атаки на финансовый сектор – количество таких преступлений увеличилось на 115 %, о чем заявлял FinCEN (Департамент Казначейства США по борьбе с финансовыми преступлениями в сети). При этом самым опасным признано мошенничество в системах дистанционного банковского обслуживания, в связи с растущей динамикой использования систем интернет-банкинга и интернет-платежей. Достаточно высоки угрозы корпоративным брендам в глобальной компьютерной сети Интернет. Рост корпоративного присутствия компаний в интернете привело к появлению нового типа киберугроз. Проявляется он в целенаправленных атаках на корпоративный бренд, заключающихся в массовых рассылках спама, резком росте количества фишинговых сайтов, неправомерном использовании узнаваемого бренда и др. [2]

Важным аспектом является и то, что при приобретении компанией различных средств защиты информации проблемы не исчезают, а прибавляются. Помимо решения комплексной задачи – защиты от угроз, необходимо данные средства развернуть и в последующем эффективно ими управлять. При этом, следует понимать, что чем крупнее и сложнее сетевая инфраструктура, тем больше она уязвима к атакам.

Постоянное развитие информационных систем, динамичное внедрение новых средств и технологий в сфере информационной безопасности требуют дополнительных ресурсов и повышения квалификации специалистов, способных решать возникающие задачи и поддерживать корпоративную информационную систему безопасности на должном уровне.

Практика свидетельствует о том, что собственные отделы информационной безопасности в большей степени выполняют проекты по базовым требованиям безопасности, не всегда эффективно реагируя на возникающие угрозы.

По нашему мнению, решению этих вопросов способствует аутсорсинг, как бизнес-технология, предусматривающая передачу стороннему

подрядчику ряда внутренних услуг и внутренних сервисов компании-заказчика, в том числе на основе использования его лицензий, программных продуктов, приложений, технических средств и фрагментов инфраструктуры. Его суть предполагает наличие длительного процесса взаимоотношений между заказчиком и исполнителем, в отличие от оказания разовых услуг отдельными организациями. Важным аспектом, влияющим на принятие решения об использовании аутсорсинга, являются возможность его органичного встраивания в бизнес-процессы компании, экономическая эффективность и минимизация потенциальных рисков его внедрения.

Так, например, в настоящее время компании аутсорсеры широко практикуют обслуживание ИТ-инфраструктуры предприятий и организаций, включающей программное и аппаратное обеспечение Microsoft, Citrix, Symantec. Тем самым обеспечивают удаленную диагностику сбоев, консультации различного уровня по используемому программному обеспечению, моделирование заявленных проблем, выезд инженеров на площадку заказчика, как в рабочее, так и нерабочее время. К наиболее востребованным услугам относят мониторинг IDS, работоспособность серверов и средств защиты, а также резервное копирование и восстановление.

Аутсорсинг информационной безопасности получил широкое распространение в западноевропейских странах уже давно, подобные услуги носят название Managed Security Services (MSS). Одним из лидеров предоставления подобных услуг является компания IBM ISS. В ее арсенале более 2200 клиентов по всему миру и свыше 12 тыс. поддерживаемых устройств. [3]

Особо следует подчеркнуть, что важной особенностью современного ведения бизнеса является массовое применение сотрудниками корпораций личных устройств – смартфонов, ноутбуков, планшетов, что, несомненно, имеет свои преимущества, но в тоже время возлагает дополнительную нагрузку на ИТ-департаменты. В опросе, проведенном аналитиками

Dimensional Research по заказу Dell, 82 % сотрудников и руководителей ИТ-служб подчеркнули, что использование личных устройств в корпоративной сети представляет серьезную проблему. Чаще всего упоминается опасность нарушения безопасности сети – на это указало 62 % опрошенных, 50 % отмечают возможность потери контроля над данными клиентов, 48 % опасаются кражи интеллектуальной собственности, а 43 % указывают на проблемы с соблюдением законов. [4]

Как показала практика, в настоящее время аутсорсинг в сфере информационной безопасности в большинстве случаев используется крупными российскими компаниями с развитыми корпоративными сетями, имеющими множество территориально распределенных филиалов, дополнительных офисов и др.

Но в тоже время, хотелось бы заметить, что внедрение аутсорсинга вызывает со стороны руководства компаний определенные опасения. Среди них особое место занимает – недоверие к внешнему исполнителю, заключающееся в боязни потери контроля над собственными информационными ресурсами и системами, именно это становиться основным движителем создания моделей самостоятельного внедрения политик ИБ и технических средств. Безусловно, это в свою очередь неминуемо ведет к сокращению расходов, повышению компетенций собственного персонала, а также появлению более удобных программных продуктов, не требующих длительного внедрения.

Мнения специалистов по аутсорсингу ИБ далеко не однозначно. Одни считают, что на специалистов компании аутсорсера следует возложить удаленный мониторинг, защиту и управление системой ИБ и другие трудоемкие задачи по обеспечению информационной безопасности. Тем самым круглосуточный режим работы аутсорсера в совокупности с высокой скоростью защитной реакции и опытом специалистов дает возможность вовремя выявлять значимые события ИБ и молниеносно реагировать на них. Все это непременно приводит к максимальной оптимизации затраты на ИБ;

повышению качества услуг, а в целом способствует повышению эффективности обеспечения ИБ. Аутсорсеры для создания комплекса защиты данных от утечки предлагают различные решения, включающие в себя систему перехвата сообщений, систему инспекции файловых ресурсов, систему активного контроля, систему архивирования и анализа и др. Они всецело осознают, что в целом архитектура должна быть настолько гибкой и масштабируемой, чтобы в соответствии с политикой использования Интернет-ресурсов, внутренних информационных ресурсов и размеров конкретной организации обеспечивать ее информационную безопасность.

Так, специалисты ЗАО «НПО “Эшелон”» проведя исследования приводят следующие данные, что применение аутсорсинга в области ИБ ведет к снижению единовременных затрат на 20-30 %, а регулярных – до 40 %.

Другие же наоборот, занимают иную позицию, единую с руководителями компаний и организаций. Аутсорсинг они связывают, прежде всего, с рисками заказчика, к которым причисляют: уровень профессионализма сотрудников аутсорсинговой компании может оказаться недостаточным для выполнения работ или оказания услуг на высоком уровне; наличие рисков нарушения безопасности и утечки сведений конфиденциального характера, в результате предоставления нерегулируемого доступа к документам, данным и материальным ценностям предприятия; недостаточность рычагов управляющего воздействия, что может привести к снижению эффективности процессов, высокая стоимость услуг, слабая проработка юридических вопросов, низкий уровень подготовки инфраструктуры регионов и др.

Именно поэтому в своих высказываниях респонденты отрицательным образом высказываются по вопросу внедрения в своих компаниях аутсорсинга ИБ (см. рис. 1).

В связи с этим, необходимо четкое понимание и разграничение сведений, которые не являются критичными, от информации, имеющей

высокую степень конфиденциальности. Следует выделить и основные бизнес-процессы, передаваемые на аутсорсинг:

– лицензирование деятельности (аттестация объекта информатизации, обучение специалистов компании, приобретение контрольно-измерительных средств);

– проектирование и реализация системы обеспечения информационной безопасности (предпроектное обследование, проектирование системы обеспечение ИБ, макетирование, реализация);

– поддержка системы обеспечения ИБ (техническая поддержка, мониторинг системы, реагирование на инциденты).

Рис. 1. Данные опроса респондентов о внедрении аутсорсинга ИБ на предприятиях [5]

При построении системы контроля услуг аутсорсинга важно осознавать, что она должна охватывать как свои (внутренние) процессы, так и сервисы, являющиеся смежными, переданными на поддержание аутсорсеру. Необходимо не только отображать текущее состояние процессов и сервисов, но и прогнозировать развитие ситуации хотя бы в краткосрочной перспективе.

Хотелось бы подчеркнуть, что передать компании-аутсорсеру только систему информационной безопасности практически невозможно – она тесно интегрирована с самой ИТ-системой предприятия. Но в тоже время, отдельные подсистемы ИБ такие как:

– управление межсетевыми экранами;

– управление системами обнаружения и предотвращения вторжений;

– управление системами внутренней безопасности;

– анализ уязвимостей и тестирование системы (включая проведение тестов на проникновение);

– управление антивирусными системами;

– управление системами аутентификации и авторизации;

– управление криптографическими системами, включая построение виртуальных частных сетей и инфраструктуры открытых ключей и др. всецело можно передавать на аутсорсинг.

Таким образом, аутсорсинг в сфере информационной безопасности непременно должен иметь положительную тенденцию [6, 7], прежде всего, с точки зрения экономической целесообразности, направленной на сокращение расходов, на обслуживание и управление системой безопасности. Потому что, решение вопросов информационной безопасности собственными силами требует наличия узкоспециализированных высокооплачиваемых сотрудников, содержания дорогостоящего оборудования, а также различных программных средств.

Контроль защищенных коммуникаций также одна из важнейших задач для большинства подразделений информационной безопасности. Задача одновременно обеспечить бизнесу сохранность информации и свободу коммуникации может быть решена только при наличии специальных средств. Поэтому сторонняя организация, имеющая в своем арсенале передовые ИТ-технологии и инструменты способна предоставить высокое качество услуг, способна обеспечить сетевую коммуникацию различной сложности, ее настройку и конфигурацию, создать надежную, отказоустойчивую систему.

Список использованных источников и литературы

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ) // www.base.consultant.ru; PCI Security Standards Council // www.pcisecuritystandards.org; Стандарт Банка России СТО БР ИББС-1.0-2010. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации (принят и введен в действие Распоряжением Банка России от 21.06.2010 № Р-705) и др. // www.base.consultant.ru.

2. Рынок информационной безопасности 2010: New Generation // www.cnews.ru.

3. Зосимовская Н. Аутсорсинг информационной безопасности // CIO. 2008. № 4.

4. Беды от смартфонов // Computerworld Россия. 2011. № 3.

5. Бугримов С., Зенкин Д., Борисов К. Служба безопасности – надежная опора бизнеса // Управление персоналом. 2009. № 7.

6. Коновалов В.А., Ломакин М.И. Модель оптимальной реализации аутсорсинговых резервов качества ИТ-услуг // Транспортное дело России. 2012. № 6-1. С. 162-164.

7. Ершов А.С. Безопасность интеллектуального капитала малых инновационных предприятий // Экономические и гуманитарные науки, 2012. – № 6.