УДК 004:336.7

А.И. Пилипенко[1], С.В. Пилипенко[2]

[1]*Луганский государственный институт культуры и искусств, Луганск*
[2]*Луганский филиал АБ «Брокбизнесбанк», Луганск*

КОНСАЛТИНГ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЛАТЕЖНЫХ СИСТЕМ

Выявлены особенности консалтинга в области информационной безопасности платежных систем. Это способствует взаимодействию с международными платежными системами в части выполнения требований по приведению платежных систем организаций в соответствие требованиям стандарта PCI DSS. Ист. 4, табл. 1.

Ключевые слова: *консалтинг, информационная безопасность, платежная система, стандарт.*

Введение

Постановка проблемы. В последние годы, наиболее значимой угрозой для бизнеса является утечка конфиденциальной информации. При этом главные факторы риска в 80% случаев находятся внутри самой компании, в лице нелояльных сотрудников [1]. Решение этой проблемой требует соблюдения украинских, международных и отраслевых стандартов. Таким образом, банки должны соответствовать PCI DSS (Payment Card Industry Data Security Standard), который выдвигает жесткие требования к защите данных владельцев платежных карт [2]. После принятия закона *«Про захист персональних даних»* актуальность защиты информации от утечек, прежде всего в государственном секторе, существенно возрастает, более того, требуется обеспечить качественно новый уровень безопасности [3].

В последних исследованиях и публикациях отмечено, что лидеры практически всех сегментов рынка с каждым годом вынуждены увеличивать свои расходы на обеспечение информационной безопасности. Это связано как с появлением новых угроз, так и с тем фактом, что ранее вопросы защиты информации редко относились к числу приоритетных и, соответственно, финансировались по остаточному принципу. В настоящий момент многие компании уже вышли на уровень консолидации систем безопасности и оптимизации их работы. То есть все базовые системы (антивирусы, межсетевые экраны, системы предотвращения вторжений и т.д.) используются уже давно, но из-за несистемного подхода, применявшегося при организации защиты, они зачастую либо малоэффективны, либо слабоуправляемы.

Выделение нерешенных ранее частей общей проблемы. В последнее время существует четкая тенденция к увеличению консалтинговой составляющей в сложных и комплексных проектах. Консалтинг в области информационной безопасности (ИБ) представляет собой комплекс услуг, оказываемых компанией-консультантом заказчику. С этой целью необходимо решить ряд задач, а именно определить:

текущий уровень обеспечения ИБ в организации, в соответствии с лучшими мировыми практиками по обеспечению ИБ, отраслевыми требованиями, а также с точки зрения эффективности противодействия существующим угрозам ИБ;

направление развития ИБ, цели и решаемые задачи с учетом стратегических целей развития организации;

конкретные действия, необходимые для продвижения по выбранному направлению и достижения поставленных целей и задач.

Целью данной статьи является выявление особенностей консалтинга в области информационной безопасности платежных систем для взаимодействия с международными платежными системами VISA и Master Card в части выполнения требований по приведению платежных систем организаций в соответствие требованиям стандарта PCI DSS.

Основной материал исследования

Консалтинг – это, прежде всего, вид интеллектуальной деятельности. Его основная задача заключается в анализе и обосновании перспектив развития, а также в использовании научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента. Консалтинг решает вопросы управленческой, экономической, финансовой, инвестиционной деятельности организаций, стратегического планирования, оптимизации общего функционирования компании, ведения бизнеса, исследования и прогнозирования рынков сбыта, движения цен и т. д.

Обращение в консалтинговую компанию происходит в следующих *случаях*:

Во-первых, это происходит тогда, когда организация не знает, на каком уровне развития находится

информационная безопасность ее ресурсов, отвечает ли она потребностям бизнеса и внешним требованиям (законодательство, отраслевые, регулирующие требования, требования заказчиков и т.п.), нет полного понимания, какие действия необходимо предпринимать и нужны ли они вообще. При этом в штате организации отсутствуют квалифицированные специалисты, способные решить вышеперечисленные задачи.

Во-вторых, когда существующая система ИБ построена и функционирует неэффективно, и это сказывается на текущей деятельности. В такой организации часто возникают инциденты информационной безопасности, приводящие к значительным ущербам, остаются высокие риски реализации угроз ИБ из-за отсутствия или малой результативности отдельных мер по ее обеспечению. При этом в организации не хватает необходимого опыта и внутренних ресурсов для выстраивания эффективных защитных мер, а также обеспечения адекватной и своевременной реакции на возникающие инциденты ИБ.

В-третьих, когда существует явная необходимость привести имеющиеся механизмы обеспечения ИБ в соответствие с внешними требованиями в области информационной безопасности. В основном это относится к требованиям различных регуляторов в той отрасли, в которой работает организация. Сюда же можно отнести и выполнение требований законодательства.

В-четвертых, когда организация, достигнув нового, более высокого уровня развития, понимает, что существующий уровень обеспечения ИБ не только не удовлетворяет текущим потребностям, но и является сдерживающим фактором для дальнейшего развития. В данном случае необходимо выстроить процессы управления ИБ, тесно взаимоувязанные со существующими бизнес-процессами, что позволит перевести на более высокую ступень развития и управления ИБ в организации. Это, в свою очередь, поможет добиться прозрачности и ясности вопросов обеспечения информационной безопасности как для высшего руководства организации и существующих акционеров, так и для потенциальных инвесторов. Такой консалтинг заключается в построении системы управления ИБ в соответствии с лучшими мировыми практиками и, при необходимости, в подготовке системы управления к сертификации по международным стандартам в области ИБ. Вопросы сертификации в большинстве случаев связаны с планируемым привлечением инвестиций, с выходом организации на IPO, с упрочнением позиции на рынке, созданием необходимого имиджа в глазах потенциальных партнеров и повышением доверия со стороны клиентов.

Инициаторами приобретения услуг консалтинга в сфере информационной безопасности, как правило, являются:

– руководство организации, если оно хочет разобраться в том, на каком уровне находится ИБ в организации, сделать ее эффективной с точки зрения затрат и, соответственно, адекватной угрозам, что необходимо предпринять, чтобы улучшить состояние процессов обеспечения защиты информации. При этом руководство осознает, что собственных ресурсов для решения такой задачи недостаточно. В некоторых случаях руководство может быть инициатором приглашения внешнего консультанта, если хочет составить для себя объективную картину того, насколько качественно службы, ответственные за выполнение задач по обеспечению ИБ, выполняют их;

– служба автоматизации или служба информационной безопасности, когда существующий уровень компетенций сотрудников в части ИБ в целом недостаточен для решения поставленных задач по построению эффективной системы информационной безопасности;

– служба информационной безопасности в случаях, когда перед ней ставятся новые задачи, выходящие за рамки установленных обязанностей и компетенций (периодические работы, требующие высокой квалификации сотрудников, внедрение новых систем и технологий и т.п.). В данном случае внешние высококвалифицированные специалисты привлекаются для решения данных специализированных задач, в то время как штатные сотрудники службы могут сконцентрироваться на решении профильных повседневных вопросов.

Каждый консалтинговый проект в области ИБ сам по себе уникален. Однако можно выделить основные *виды* услуг, предоставляемых консалтинговыми компаниями:

– аналитическая деятельность (анализ и оценка деятельности организации по защите информационных ресурсов, включая анализ эффективности применяемых средств и методов защиты информации, экспертизу ведущихся проектов в части ИБ, сравнительные исследования с показателями по отрасли и т. д.);

– прогнозирование (на основе проведенного анализа и используемых консультантом методик – составление прогнозов по указанным выше направлениям);

– консультации с выдачей рекомендаций по самому широкому кругу вопросов, касающихся защиты бизнес-процессов и ресурсов организации, разработки и внедрения мероприятий и систем защиты;

– стратегическое планирование деятельности организации в области ИБ и решение совокупности проблем, связанных с организацией управления ин-

формационной безопасностью.

Формы предоставления услуг также могут быть различными в зависимости от сложности проекта и пожеланий заказчика:

– консультации с периодическими выездами на площадку заказчика для сбора исходных данных, согласования результатов анализа и выдаваемых рекомендаций;

– удаленные консультации без выезда на площадку заказчика;

– постоянное присутствие на площадке заказчика определенного числа консультантов в течении всего срока проекта (аутстаффинг).

Объектом консалтинга в информационной безопасности платежных систем являются:

– процессы, связанные с автоматизированными банковскими системами;

– процессы, связанные с автоматизированными платежными системами (процессинг);

– процессы, связанные с автоматизированными системами межбанковского взаимодействия;

– другие.

В зависимости от задач, стоящих перед кредитно-финансовой организацией, обследование состояния ИБ может включать в себя различные виды работ и критерии оценки, которые согласуются с исполнителем перед началом консалтингового проекта. В целом, все работы в ходе обследования выполняются в три этапа (табл. 1).

Таблица 1

Этапы обследования состояния информационной безопасности с разработкой рекомендаций

1. Информационное обследование	1.1. Сбор данных об информационной системе кредитно-финансовой организации
	1.2. Сбор информации о процессах обеспечения информационной безопасности
	1.3. Сбор информации о защищенности информационной системы
2. Анализ полученной в ходе обследования информации	2.1. Экспертная оценка эффективности используемых средств и методов защиты информационных ресурсов ИС
	2.2. Построение модели угроз информационной безопасности в отношении ресурсов ИС кредитно-финансовой организации
3. Разработка и согласование рекомендаций по повышению уровня информационной безопасности организации	3.1. Принятие первоочередных мер по усилению информационной безопасности ИС заказчика
	3.2. Внесение в нормативно-распорядительную документацию необходимых изменений или дополнений
	3.3. Доработка существующих механизмов защиты данных в ИС
	3.4. Внедрение дополнительных механизмов защиты информации

Для минимизации рисков утечки информации и компрометации платежных карт разработана система межбанковского обмена информацией *"Exchange-OnLine"* [4]. Она позволяет банкам обмениваться сведениями касательно фактов несанкционированного использования платежных карточек, компрометации данных, и иной необходимой информацией. Оперативный обмен сведениями посредством системы межбанковского обмена информацией "Exchange-OnLine" касательно фактов компрометации данных платежных карт клиентов украинских банков позволяет банкам-пользователям системы оперативно принимать меры по прекращению использования скомпрометированных карт (путем блокировки, перевыпуска карточек, установления лимитов на операции и т.д.) и предотвращать возможные убытки вследствие мошеннического использования платежных карт.

Одним из основных принципов законодательства в области ИБ является приоритет норм международного права над государственным законодательством (если эти нормы не противоречат Конституции Украины). Это позволяет применять международные нормативно-правовые акты, которые относятся к лучшим мировым практикам, и таким образом покрывать недостатки и пробелы в украинском законодательстве. Примером такой практики является применение в Украине *стандарта Payment Card Industry Data Security Standard (PCI DSS).*

Стандарт Payment Card Industry Data Security Standard (PCI DSS) разработан международными платежными организациями American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., объединившимися в консорциум PCI Security Standard Council (PCI SSC). Стандарт определяет требования к состоянию защищенности платежных систем кредитно-финансовых организаций, которые обрабатывают, хранят или передают информацию о держателях платежных карт. Такие структуры должны ежегодно подтверждать соответствие защищенности своих платежных систем требованиям стандарта PCI DSS путем прохождения сертификационного аудита, который могут выполнять только специализирован-

ные компании, обладающие соответствующим статусом:

– Qualified Security Assessor (QSA) – проведение сертификационного аудита;

– Approved Scanning Vendor (ASV) – внутреннее и внешнее сканирование платежных систем организации.

Консорциум PCI SSC постепенно вводит систему штрафов, которые будут взыскиваться с финансовых организаций, если защищенность их платежной системы не соответствует требованиям стандарта PCI DSS.

Одним из основных факторов, влияющих на выбор компании, оказывающей услуги по консалтингу в области информационной безопасности, является уровень доверия к консультанту. Это объясняется тем, что в большинстве случаев компании-консультанту предоставляется доступ к конфиденциальной информации заказчика, поэтому к ней предъявляются повышенные требования. Такой уровень доверия может быть обеспечен не только заключением соответствующих договоров о конфиденциальности и неразглашении сведений, которые станут известными консультанту в ходе работ по консалтингу, но и наличием необходимых лицензий государственных и регулирующих органов, предоставляющих право осуществлять работы в области информационной безопасности.

Компания, оказывающая услуги консалтинга в области ИБ, должна иметь соответствующие партнерские статусы от ведущих вендоров на рынке информационной безопасности. При этом данный статус должен определять возможности компании не только по дистрибуции средств защиты, но и способности консультанта по внедрению и технической поддержке данных средств.

Выводы

Преимуществом компании-консультанта является наличие тесного взаимодействия с различными ассоциациями, органами по сертификации, разработчиками стандартов и требований в области ИБ. Это позволяет консультантам быть в курсе последних изменений и тенденций в области информационной безопасности, что соответственно повышает уровень их компетенций в вопросах информационной безопасности.

Взаимодействие со стороны компании-консультанта с кредитно-финансовой организацией может быть в любой форме, в том числе и в форме аккредитации консалтинговой компании в качестве органа по сертификации по стандарту PCI DSS. Такая аккредитация, помимо права на проведение сертификационного аудита, позволяет понимать видение разработчиков стандарта и предлагать качественные услуги по консалтингу в данной области.

Список литературы

1. Фисун Р. Безопасность: «ничего особенного» / Р. Фисун, Э. Савушкин // Компьютерное обозрение. – 2008. – № 12 (629). – [Электронный ресурс]. – Режим доступа к журн.: http://ko-online.com.ua/node/ 35152.

2. Стандарт безопасности данных индустрии платежных карт (PCI DSS). – Версия 1.1. – 2006. – [Электронный ресурс]. – Режим доступа к ресурсу: http://dsec.ru/consult/pcidss/PCI_DSS_v1-1_rus.pdf.

3. Проект закону України «Про захист персональних даних». – БНТИ. – [Электронный ресурс]. – Режим доступа к ресурсу: http://gska2.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=32124.

4. Украинская межбанковская ассоциация членов платежных систем «ЕМА». – БНТИ. – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ema.com.ua.

Поступила в редколлегию 18.02.2009

Рецензент: д-р техн. наук, проф. В.А. Рач, Восточно-украинский национальный университет им. Владимира Даля, Луганск.

КОНСАЛТИНГ В ОБЛАСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ

А.І. Пилипенко, С.В. Пилипенко

Виявлені особливості консалтингу щодо взаємодії кредитно-фінансових організацій з міжнародними платіжними системами з питань виконання вимог стандарту PCI DSS.

Ключові слова: *консалтинг, інформаційна безпека, платіжна система, стандарт*

CONSULTING IN PAYMENT SYSTEM INFORMATION SECURITY

A.I. Pilipenko, S.V. Pilipenko

The consulting peculiarities connected with credit-financial organizations and international payment systems interaction considering completion the PCI DSS standard.

Keywords*: consulting, information safety, payment system, standard.*