Очевидно, что большинство популярных на рынке технических средств, внедряемых в крупных по российским масштабам организациях, неприменимо для среднего и малого бизнеса. При этом Закон № 187-ФЗ, под действие которого попали все банки, не учитывает их размера. Каков минимальный набор услуг, которым может воспользоваться небольшой банк для обеспечения соответствия требованиям ИБ? Как снизить риск конфликта интересов банка и поставщика услуг?

Аутсорсинг ИБ в средних и малых банках: ищем оптимальное решение

Максим ТЕМНОВ,
компания «Информзащита», заместитель генерального директора

Поиск оптимального решения для обеспечения информационной безопасности небольших финансовых организаций непрост по многим обстоятельствам: финансовые ограничения, нехватка ресурсов, малое количество доступных решений, требования регуляторов без поправок на размер бизнеса — перечислять можно бесконечно.

Что обычно слышат от руководства ответственные за ИБ специалисты банка в ответ на предложение о внедрении средств защиты информации? «Денег нет!», «Что нам будет, если мы не станем этого делать?», «Затраты на защиту информации не дают полной защиты», «Мне проще/выгодней заплатить штраф за нарушение», «Сейчас внедришь систему, а потом нужен будет персонал для ее эксплуатации?» и т.д.

Что делать, если для обеспечения реальной безопасности банка собственных сил и аргументов не хватает? Одним из наиболее быстрых и понятных для бизнеса способов решения практически любой задачи является аутсорсинг. Однако использование внешнего помощника для решения внутренних задач помимо новых возможностей всегда влечет за собой дополнительные вопросы и действия. Тем более когда это касается такой традиционно закрытой, я бы даже сказал — «интимной», сферы организации, как информационная безопасность.

Предлагаю взглянуть на проблематику использования аутсорсинга ИБ в средних и малых учреждениях финансовой сферы с позиций

Аутсорсинг ИБ в средних и малых банках: ищем оптимальное решение

трех сторон: регулятора, поставщика услуг и самой кредитно-финансовой организации. Не зря же взгляд с трех углов формирует самую устойчивую геометрическую фигуру — треугольник. Итак…

Каким должен быть аутсорсинг ИБ с точки зрения Банка России?

Первое, что должен обеспечивать регулятор, — устойчивость отрасли к возрастающим угрозам. Особенно это касается непрерывности функционирования какой-либо платежной системы даже на региональном уровне и в вертикали какой-либо из ключевых отраслей экономики. Требования, рекомендации и имплементация Закона № 187-ФЗ[1] не всегда учитывают размер финансовой организации, попадающей под действие Закона. Почему так? Все просто: статистика последних атак на банки показала, что три из пяти атак приходятся именно на СМБ-банки. Снижение порога применимости требований приведет к ухудшению устойчивости кредитных учреждений к информационным угрозам.

Статистика последних атак на банки показала, что три из пяти атак приходятся именно на СМБ-банки.

Для тех организаций, которые не имеют достаточного уровня компетенций и ресурсов для обеспечения реальной безопасности, Банк России предложил стандарт использования аутсорсинга ИБ.

Модели усиления системы обеспечения информационной безопасности (СОИБ) за счет провайдеров услуг аутсорсинга могут применяться на краткосрочной, среднесрочной и долгосрочной основе.

К примерам краткосрочного применения аутсорсинга ИБ можно отнести разовое привлечение экспертизы (например, проведение аудита). Банк России отмечает целесообразность привлечения сервис-провайдеров тогда, когда нужно быстро выстроить сложный процесс до создания пула своих ресурсов, например процесс приведения в соответствие с требованиями положений Банка России перед проверкой. Практика долгосрочного сотрудничества с сервис-провайдерами отмечается пока только у небольших представительств зарубежных банков. В силу своей ментальности российские финансовые компании саму парадигму долгосрочного сотрудничества пока не воспринимают. А зарубежный опыт показывает, что такая тенденция сохранится в России еще несколько лет.

К основным предпосылкам использования аутсорсинга ИБ регулятор относит кадровые, экономические, технологические и вре-

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры». См.: Лукацкий А. К чему обязывает банки новый закон о безопасности критической информационной инфраструктуры? // Внутренний контроль в кредитной организации. 2018. № 1.

Максим ТЕМНОВ

менные. Так, для обеспечения круглосуточной смены мониторинга и реагирования на инциденты ИБ необходимо не менее пяти сотрудников. Это затруднительно для большинства СМБ-банков, где за информационную безопасность отвечает один или два сотрудника.

По мнению Банка России, средним и малым организациям банковской системы РФ в первую очередь нужно ориентироваться на следующие услуги аутсорсинга:

— мониторинг и анализ событий информационной безопасности для критичных систем;

— выявление атак на критичные информационные системы (в т.ч. с использованием информации, получаемой от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT));

— анализ защищенности (управление сканерами уязвимостей);

— контроль конфигураций сетевого оборудования и операционных систем;

— управление IDS/IPS;

— анализ безопасности кода приложений;

— предоставление и администрирование WAF;

— обучение и повышение осведомленности персонала.

Необходимый конкретному банку состав аутсорсинговых услуг можно выбрать, исходя из анализа рисков, как рекомендует стандарт Банка России СТО БР ИББС-1.4-2018.

Такая позиция Банка России вполне понятна. Регулятору важно, чтобы отрасль получила возможность повысить уровень информационной безопасности в сжатые сроки. Многообразие моделей решения задачи и их здоровая конкуренция — залог эффективности и доступности решений СОИБ с точки зрения регулятора.

Как выбрать оптимальный набор аутсорсинговых услуг?

Очевидно, что большинство популярных на рынке технических средств, внедряемых в крупных по российским масштабам организациях, неприменимо для среднего и малого бизнеса. Недостаток квалификации, опыта и количества сотрудников для обеспечения ИБ — благоприятная почва для продажи и реализации решений, но оптимизация бюджетов в небольших компаниях приводит к экономии на безопасности. По крайней мере, реальная и комплексная безопасность уступает по распространенности «бумажной», а также «лоскутности» используемых решений и процессов.

Для комплексного удовлетворения требований Закона № 152-ФЗ[1], а также требований по защите информации при осуществлении

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Аутсорсинг ИБ в средних и малых банках: ищем оптимальное решение

денежных переводов и при взаимодействии с платежной системой Банка России (Закон № 152-ФЗ, Положения № 382-П[1], № 552-П[2]) вполне достаточно услуг экспресс-аудита, поставки средств защиты информации на базе OpenSource, формирования комплекта документов и сопровождения основных процессов и решений ИБ. Для реализации более продвинутого подхода возможно применять уже сертифицированные и функционально наполненные решения, где оборудование может быть предоставлено в аренду или на условиях рассрочки оплаты. Наличие элементов СОИБ в банке в большинстве случаев позволяет сэкономить за счет интеграции существующих и дополнительно предлагаемых поставщиками решений. Расширять комплекс услуг можно по принципу детской игры «пирамидка»: например, в случае комплаенса требований PCI DSS или SWIFT — при помощи добавления специфичных услуг консалтинга и отчетности.

Необходимый конкретному банку состав аутсорсинговых услуг можно выбрать, исходя из анализа рисков, как рекомендует стандарт Банка России СТО БР ИББС-1.4-2018.

В частности, необходимо анализировать:

— правовые риски — риски нарушения требований административного и уголовного законодательства и требований регулятора;

— операционные риски — прерывание операционной деятельности, кража денежных средств, нарушение бизнес-процессов и появление дополнительных затрат. Из ключевых рисков при выборе аутсорсингового решения можно отметить, например, операционный риск утраты достаточно редких специфичных компетенций по решениям на базе OpenSource как в финансовой организации, так и у поставщика услуг;

— риск потери деловой репутации — отток существующих клиентов и потеря потенциальных.

Компоненты базового технического решения для большинства финансовых учреждений могут быть типовыми. Как мы уже отмечали, требования законодательства и регуляторов для всех также едины, а угрозы для большинства банков однотипные. Таким образом, логично и экономически оправданно воспользоваться готовым решением и кастомизировать его под свои нужды.

Пользование услугами аутсорсинг-провайдеров требует от специалистов по защите информации банка разрешения очевидных конфликтов интересов заказчика и поставщика услуг: бюджет, объем работ и зоны ответственности.

[1] Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

[2] Положение Банка России от 24.08.2016 № 552-П «О требованиях к защите информации в платежной системе Банка России».

Максим ТЕМНОВ

Как показали расчеты в одном из банков, фактические трудозатраты на приведение банка в соответствие с Положением № 382-П составили 1,5 человеко-года. За этот срок банком самостоятельно был разработан пакет организационно-распорядительной документации и проведена опытная эксплуатация решений по базовым мерам защиты информации. Аутсорсер может сделать эту работу за три месяца при сопоставимых или меньших затратах. При этом финансовая организация становится готова к прохождению проверок Роскомнадзора или Банка России.

Как избежать конфликта интересов?

Пользование услугами аутсорсинг-провайдеров требует от специалистов по защите информации банка разрешения очевидных конфликтов интересов заказчика и поставщика услуг: бюджет, объем работ и зоны ответственности. Те руководители, ответственные за ИБ, которые уже провели оценку рисков использования аутсорсинга согласно СТО БР ИББС-1.4-2018, применяют следующие практики:

— подробное описание каталога услуг;
— прозрачное ценообразование;
— четкое SLA;
— контроль качества по KPI;
— подписанное NDA;
— оплата по фиксированному объему оказанных услуг.

Что же дальше?

Какие дальнейшие пути использования услуг аутсорсинга ИБ могут быть востребованы в банках?

Требования Закона № 187-ФЗ, под действие которого попали все организации финансового сектора, формируют, как представляется, дорожную карту после категорирования объектов ключевой информационной инфраструктуры:

1) экспресс-оценка текущего состояния безопасности и внедрение базового решения по обеспечению ИБ;

2) подключение к FinCERT через коммерческий SOC;

3) экспертная помощь при кибератаках.

Реализуется представленный сценарий или нет — посмотрим через год-полтора. Важно отметить, что на аутсорсинг нельзя передать функцию принятия решений по защите информации банка, следовательно, значимость и востребованность эффективных менеджеров, отвечающих за ИБ в банках, резко возрастут.

Определение состава превентивных мер внутреннего контроля в отношении иностранных публичных должностных лиц во многом оставлено на усмотрение банка. Почему анкетирование клиента нельзя считать «обоснованными и доступными в сложившихся обстоятельствах мерами»? Как реализовать комплексный подход к выявлению рисков, связанных с ИПДЛ? Как определить источник происхождения денежных средств ПДЛ и его ближайшего окружения?

Внутренний контроль при обслуживании ИПДЛ: что включить в комплекс превентивных мер?

Ксения РОМАДИНА,
эксперт в области ПОД/ФТ

Закон № 115-ФЗ[1] обязывает организации, осуществляющие операции с денежными средствами или иным имуществом, принимать «обоснованные и доступные в сложившихся обстоятельствах меры» по выявлению среди физических лиц, находящихся или принимаемых на обслуживание, иностранных публичных должностных лиц.

Важнейшей особенностью, которую необходимо учитывать при реализации требований, касающихся ПДЛ, является то, что деловые отношения с членами семьи и ближайшим окружением ПДЛ несут те же репутационные риски, что и отношения с ПДЛ.

ФАТФ указывает в своих Рекомендациях 12 и 22, что потенциальные риски, связанные с положением ПДЛ, оправдывают применение дополнительных превентивных мер по ПОД/ФТ при установлении и поддержании деловых отношений с ними.

В частности, требуется обеспечить выполнение мер внутреннего контроля, направленных на предотвращение возможности ПДЛ незаконно использовать кредитные организации в своих целях. Отдельного внимания заслуживает указание ФАТФ на характер

[1] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».