PCWEEK Безопасность

Информационная безопасность в банках: тратить нельзя терпеть

Автор: Александр Бодрик

05.06.2017

Информационная безопасность как свойство бизнеса не живет в отрыве от бизнеса, поэтому информационную безопасность банков вместе с банковской отраслью штормит уже несколько лет. Однако есть и уверенно чувствующие себя банки, в частности об инвестициях в ИБ активно рапортуют «Тинькофф» и Сбербанк, что вкупе с общим сокращением количества банков создает впечатление нового «неравенства» в банковской ИБ, где сверхактивные финансовые институты как будто существуют в параллельной реальности с сотнями небольших да еще и активно сокращаемых ЦБ региональных банков.

В данном обзоре мы планировали сверить свои впечатления с мнением широкого круга участников рынка и попытаться выявить консенсус-тренды в этом волатильном, но активно развивающемся сегменте рынка ИБ. К сожалению, ряд приглашенных экспертов — представителей известных в мире ИБ компаний не сочли возможным ответить на наши вполне конкретные и острые вопросы. Поэтому сверить впечатления и выработать консенсус получилось только с в некотором роде интеллектуальной элитой участников рынка банковской ИБ.

Зачистка банковского сектора и ИБ-сегмента

Отзыв десятков и сотен лицензий у банков фундаментально меняет ландшафт банковской отрасли: становится меньше клиентов, отменяются бюджетированные проекты, консолидируются банковские доходы, затраты и в конечном итоге бюджеты, освобождаются для работы в других банках десятки профессионалов в области ИБ.

Однако наши эксперты не согласны с таким видением полностью, в частности директор центра ИБ компании «Инфосистемы Джет» Алексей Гришин говорит о возможности лишь косвенного влияния: «Банки стали серьезнее относиться к требованиям ЦБ, в том числе и по информационной безопасности». Но Дмитрий Тирский, менеджер по развитию кибербезопасности в финансовых и торговых организациях ИБ-департамента ГК Softline, согласился с тем, что отзывы лицензий влияют на распределение ИБ-бюджетов между банковскими организациями (по сути в пользу оставшихся).

А вот Дмитрий Огородников, директор центра компетенций по ИБ компании «Техносерв», отметил: «Количество банков с уставным капиталом более 10 млрд. руб. стабильно растет. В 2010 г. таких банков было двадцать один, а в 2017-м их уже тридцать три. Именно эти банки и определяют развитие информационных технологий и информационной безопасности в банковском секторе, являясь основными заказчиками». Он не нашел корреляции между отзывами лицензий и уровнем ИБ банков, подчеркнув: «Наиболее активное сокращение количества банков в России началось в 2014 г., и с тех пор было отозвано свыше трёхсот лицензий. Но в том же 2014-м была проведена крупнейшая в истории атака группы Carbanak, в результате которой злоумышленникам удалось украсть более миллиарда долларов с банковских счетов по всему миру, и после этого вопросы кибербезопасности в банках стали заметно

актуальнее». (От себя отмечу, что эти факты не учитывают параметра времени: подготовка к операциям группой Carbanak очевидно началась до 2013-го, а влияние отзывов лицензий на ИБ банков проявилось никак не раньше 2015-го ввиду стандартного корпоративного цикла планирования и бюджетирования.)

Есть ли ИБ-жизнь в банках ниже ТОП-50?

С другой стороны — отзывы лицензий затронули в основном некрупные банки, не вошедшие в ТОП-50, в которых, вероятно, и так с ИБ-бюджетами было не густо. Все наши эксперты согласились, что финансовые возможности у таких банков весьма ограниченны, однако причины внимания к ИБ и особенности реализации проектов все же разнятся.

Так, Николай Зенин, главный инженер проектов информационной безопасности ГК «Компьюлинк», обратил внимание на то, что основным драйвером ИБ в некрупных банках является комплаенс, подчеркнув: «Небольшие банки как раз больше других обеспокоены обеспечением соответствия стандарту регулятора». Василий Хасанов, эксперт в области решений Data Security и противодействия финансовым преступлениям компании DIS Group, посетовал: «Зачастую выбор и внедрение решений в таких банках сопряжены с условиями жесткой экономии, что в ряде случаев может оказывать негативное влияние на качество».

Алексей Андрияшин, руководитель системных инженеров Fortinet, предложил банкам в целях оптимизации и гибкого управления TCO ИБ-решений обратить внимание на продукты с гибкой системой лицензирования и облачными сервисами, а также на широкую линейку виртуализированных решений (VM appliance).

Дмитрий Романченко, директор практики информационной безопасности IBS, отметил специфичный опыт взаимодействия с некрупными банками, искавшими «серебряную пулю» от угроз ИБ, которой, считает он, объективно не существует. Эксперт полагает, что период поиска «серебряной пули» прошел, но, как видим, ее апологеты еще остались.

Наконец, Алексей Гришин и Дмитрий Огородников сошлись во мнении, что в отличие от более крупных банков небольшие финансовые институты во многом реализуют проекты своими силами, а также активно используют Open Source (Алексей Гришин) и реализуют ИБ как часть ИТ-проектов (Дмитрий Огородников).

Региональная специфика банковской ИБ

Вопрос о региональной и международной специфике банковской ИБ не получил сильного отклика у экспертов, часть из них не нашла что ответить, а представители компаний «Инфосистемы Джет» и Softline согласились друг с другом, что внутри России таковой нет, однако были и другие мнения.

К примеру, Дмитрий Романченко выделил унаследованные проблемы в области ИБ у подразделений федеральных банков с региональной сетью: «Часто филиальная сеть у таких структур создавалась путем поглощения региональных банков, поэтому уровни обеспечения ИБ в центре и в регионах существенно различаются — даже если в центре делают инвестиции в ИБ, в филиалах ИБ-поддержка может быть недостаточной. Если учесть интегрированность информационных систем банков, такая ситуация весьма опасна — атака может быть направлена как на центральную инфраструктуру и поражать более слабые региональные сегменты, так и на региональный сегмент и дальше в центр уже по сетям банка». Надо сказать, что автор настоящего обзора неоднократно сталкивался с более низким уровнем ИБ в регионах. Так, в ходе аудита ИБ одной из крупнейших государственных корпораций общий неплохой уровень серьезно подпортило отделение в Самаре, а некоторые крупные оперативные центры

информационной безопасности (Security Operations Center, SOC) де-факто ограничивают свою деятельность московскими подразделениями (такие примеры есть не только в банковском секторе, но и в телекоме, нефтегазовом и государственном секторах).

Специфику обеспечения ИБ в банках с иностранным головным офисом подметил Денис Горчаков, руководитель группы исследования и анализа мошенничества Kaspersky Fraud Prevention. В частности, он считает, что такие финансовые организации «практикуют несколько отличный от российского подход, более прагматичный в плане обеспечения ИБ, больше задумываются над экономической целесообразностью того или иного решения, меньше готовы экспериментировать, зато лучше принимают уже прижившиеся в Европе практики».

Информационная безопасность бизнес-направлений банков

ИБ банков часто вращается вокруг темы обеспечения безопасности банковской инфраструктуры, а ведь инфраструктура для банков — всего лишь средство для функционирования бизнес-приложений, специфика и архитектура работы которых прямо завязаны на конкретные бизнес-направления (line of business, LoB): розничный и корпоративный, инвестиционный и управления активами, наконец модный сейчас цифровой. Многие эксперты не согласились с существованием специфики в обеспечении ИБ LoB, но и реальные примеры такой специфики приведены тоже были.

Так, Дмитрий Романченко поделился опытом обеспечения безопасности розничного банка, где по его мнению фокус делается на достоверную идентификацию и аутентификацию клиента. Эксперт считает, что классические методы аутентификации по логину и паролю с добавлением SMS-сообщения не являются полностью надежными, так как может быть скомпрометирован канал передачи, компьютер или смартфон пользователя, в результате чего реквизиты могут попасть к злоумышленнику. Поэтому он советует использовать цифровые сертификаты и ключевые носители с криптографией на борту, антифрод-системы, нацеленные на персональную и групповую поведенческую модель клиента, а также задуматься об идентификации по биометрическим атрибутам (отпечатки пальцев, скан радужки глаза, 3D-модель лица, тепловая карта сосудов ладони), которые могут быть применены во фронтальном сегменте розничного банка.

Заочно поспорили Алексей Гришин, который отмел наличие специфики в обеспечении ИБ различных бизнес-направлений банков («угрозы для разных банкингов примерно одинаковы»), и Дмитрий Огородников, приведший примеры специфичных проблем для многих направлений. Так, для розничного банкинга он считает актуальными вопросы защиты банкоматов и частных транзакций физических лиц при использовании терминала оплаты или смартфона, поскольку именно на эти устройства направлено подавляющее число атак. А для цифрового банкинга эксперт видит уязвимое место в клиент-банковских приложениях и системах ДБО. Упомянул он и угрозы для инвестиционного банкинга и управления активами, где основными угрозами считает доступ к инсайдерской информации об эмитентах, акциях, планируемых финансовых действиях на рынке и совершении сделок на основе этих данных — так называемый инсайдерский трейдинг. Автор добавил бы вероятные проблемы с ошибочным раскрытием информации о лимитах, остатках и рисках, ведь галопирующая в последние два-три года цифровизация работы брокерских и private banking-организаций создает предпосылки для ошибок в создании и применении ролевых моделей в цифровом канале инвестбанка. В отличие от традиционного коммерческого банка инвестиционный банк оперирует на порядки большим количеством лимитов, рисков и продуктов, а значит, сложность, вероятность ошибок в реализации и потенциальная уязвимость подсистем управления доступом здесь на порядки выше.

Бизнес информационной безопасности

Что касается развития банками своего бизнеса по обеспечению ИБ, то можно сделать вывод об актуальных запросах заказчиков и ещё один, опосредованный вывод, насколько им соответствует представление вендора. Ведь игрок, который не понимает своего клиента, вряд ли вырастет или хотя бы сохранит бизнес на том же уровне. Из ответов на наши вопросы сложилась следующая картина.

«Компьюлинк» делает ставку на последовательное создание и сопровождение SOC в организациях.

Fortinet продвигает концепцию интегрированной системы ИБ, но отмечает, что пока наибольший интерес со стороны заказчиков вызывают решения, способные противостоять целенаправленным атакам (APT), обязательным компонентом которых является «песочница», где можно в изолированной среде без риска для корпоративной сети анализировать поведение подозрительных файлов.

Рост ИБ-бизнеса «Инфосистем Джет» сейчас идёт в основном не за счет продажи ИБ-продуктов, а за счет ИБ-услуг. В компании как наиболее быстро растущее направление отмечают борьбу с мошенничеством. А среди будущих драйверов бизнеса видит развитие собственных антифрод- и анти-APT-решений.

«Техносерв» ощущает повышенный спрос на средства защиты информации с функциями поведенческого анализа и регистрацией подозрительной активности процессов или пользователей. К числу таких решений относятся специализированные IDS/IPS-комплексы, модули, реализующие функционал «песочниц», различные анализаторы сетевого трафика. Маржинальность компании по этим решениям примерно одинаковая, но большой вклад в бизнес дают сопутствующие услуги (вероятно, по сравнению с не-ИБ-решениями. — *Прим. автора*).

DIS Group видит рост интереса к решениям в области Data Security, помогающим обеспечить безопасность информационных потоков.

Единственным участником нашего обзора, который упомянул аудиты ИБ как важное направление деятельности, стала IBS. Однако в качестве драйверов ИБ-бизнеса представитель компании назвал еще SIEM, SOC, IDM, DLP, антифрод, анти-APT.

Безопасность цифровизации банков

Цифровизация банков идет уже не первый год и, похоже, только набирает обороты. В этой связи все наши эксперты были скорее пессимистичны насчет сопутствующих рисков ИБ, в частности Алексей Гришин рассказал о грустной реальности корпоративной ИБ-жизни: «ИБ всегда идет следом за ИТ, а ИТ — следом за бизнесом. Даже когда бизнес тесно связан с ИТ, как в банковском секторе, безопасность отстает. Потребность в защите новых финансовых сервисов безусловно существует, спрос есть, но нужных ИБ-решений просто может еще не быть. Поэтому используются классические средства защиты, условно говоря, средства вчерашнего дня для защиты от угроз дня сегодняшнего. Понятно, что вскоре появятся новые инструменты, направленные на решение конкретных задач. Но появятся и новые сервисы, идеи, бизнес-направления, для которых существующих средств защиты опять же будет недостаточно. К сожалению, при запуске новых решений для бизнеса организации редко задумываются о безопасности». Он также спрогнозировал рост интереса к системам защиты от мошенничества и средствам защиты, интегрированным непосредственно в системы обработки больших данных.

А Денис Горчаков отметил и иной аспект галопирующей цифровизации: сложно защитить безнадёжно устаревающую банковскую инфраструктуру и технологии — приложения, оборудование. (Отмечу, что каждый специалист, хоть раз выполнявший крупный аудит безопасности региональных бизнес-приложений, не может не согласиться с экспертом: устаревшего и унаследованного ПО хватает даже в самых обеспеченных организациях, а ведь там гораздо скуднее набор механизмов безопасности, проблемы с обновлениями и сделанная «на коленке» архитектура скорее норма, чем исключение.)

Дмитрий Романченко и Дмитрий Огородников сошлись на том, что необходима ИБ-поддержка трансформации традиционного банкинга в цифровой, в том числе требует решения ИБ-задача идентификации и аутентификации и доверия к цифровому банкингу в широком смысле. При этом Дмитрий Романченко отметил актуальность антифрод-систем, а Дмитрий Огородников — открытой аутентификации, блокчейна и UEBA (User and Entity Behavior Analytics).

В свою очередь, Алексей Андрияшин подчеркнул практические проблемы мобильного канала цифрового банкинга: «Многие клиенты, использующие SSL/TLS на Android, могут быть подвержены атаке „человек посередине“. Соответственно разработчики новых банковских продуктов должны тщательно продумывать вопросы ИБ предоставления сервисов, вовремя исключать известные уязвимости и стремиться к превентивному исправлению любых недостатков в клиентском ПО».

Банки под атакой

Историческая дискуссия, есть ли специфические банковские угрозы (стандартное мнение банкиров) или нет (мнение многих представителей других отраслей), не стихает до сих пор. Наши эксперты сошлись во мнении о существовании специфических банковских угроз: угрозы ДБО, вмешательства в межбанковские платежи (атаки на АРМ КБР), кражи персональных данных (в банках, платежных системах и сопутствующих сервисах), атаки на SWIFT и на сети банкоматов и т. д., при этом банки становятся неким агентом ИБ-влияния (иногда негативного) на смежные отрасли. Так, Дмитрий Романченко рассказал, что попытки атак на инфраструктуру телеком-операторов предпринимаются в том числе с целью кражи персональных данных клиентов банков.

А вот Дмитрий Тирский считает, что специфики банковских угроз не существует. Однако он полагает, что «...атаки на банки легко монетизируются и на банках обкатываются новые тактики и стратегии таргетированных атак. В итоге полученные в результате таких атак деньги — это понятный индикатор успешности какой-то конкретной новой тактики и стратегии, что в свою очередь становится сигналом для злоумышленников — данную таргетированную атаку можно переносить в другой сектор. Один из примеров — фишинговая активность, которая распространилась далеко за пределы банковской сферы». (Отмечу, что вышедшие сейчас в публичное поле фишинговые рассылки блокировщиков-вымогателей имели место в России еще в 2011 г.: в то время было проще вывести деньги через различные платные мобильные номера.)

Николай Зенин подчеркнул актуальность комплаенс-рисков в сфере ИБ: любое несоответствие требованиям регулятора усугубляет риск отзыва лицензии на осуществление банковских операций. Однако с точки зрения эксперта наиболее актуальной угрозой для банковской сферы была и остается угроза проведения кибератак, целью которых является вывод денежных средств клиентов без их согласия, в частности с недавнего времени получили распространение атаки на российские банки через систему межбанковских коммуникаций SWIFT.

Экономия в банковском стиле

На рынок банковской ИБ цифровизация может влиять и негативно: ИТ становятся основным средством в банках, а значит, у них повышаются требования к экономической эффективности вложений в ИТ/ИБ — снижается маржинальность проектов (в отличие, например, от нефтегазовой отрасли, где затраты на ИБ часто невозможно рассмотреть в бюджете организаций и с лупой, хотя это сотни миллионов рублей). Это особенно актуально для розничных банков, маржинальность бизнеса которых может быть меньше маржинальности их контрагентов. Однако контрагенты не привязаны к розничным банкам и могут вполне прохладно относиться к идее дополнительных скидок, поэтому для банков могут быть актуальными такие стратегии оптимизации затрат, как использование Open Source, импортозамещение (многие российские продукты не стоят на месте), аутсорсинг. Оценить эти стратегии и предложить свои мы попросили наших экспертов.

Дмитрий Романченко указал на использование Open Source как один из вариантов «первого выбора» при оптимизации затрат, но подчеркнул, что есть нюансы: «При этом возникает очевидный вопрос центра ответственности за систему, построенную на СПО, — все риски получает банк, и разделить их не с кем. В итоге использование Open Source лишь частично способствует снижению TCO информационных систем». Он также описал свое видение импортозамещения в банковском секторе: «Импортозамещение следует рассматривать скорее в контексте снижения стратегических рисков банка, а не как непосредственный инструмент снижения стоимости ИТ/ИБ. Переход на отечественные решения — это способ снижения страновых и санкционных рисков, а также переход на работу с более управляемыми и лояльными локальными поставщиками. Данный подход в том числе делает возможной полную проверку исходного кода программных продуктов на предмет безопасности и отсутствия уязвимостей».

Алексей Гришин упомянул, что при всей актуальности для банковского сектора тематики оптимизации затрат банки в первую очередь смотрят на эффективность средств защиты: «Экономия на безопасности может обойтись себе дороже». (Отмечу, что такую точку зрения — «Cost effectiveness is not a first priority in Security IT» — разделяет и ряд ведущих мировых глобальных банков.)

Денис Горчаков признал, что немало западных продуктов по-прежнему превосходят российские разработки, при этом стоят дешевле и работают надёжнее, значит, есть куда стремиться. Но он видит преимущество российских продуктов в лучшем понимании специфики рынка, и считает, что у России много общего со странами БРИКС и Ближним Востоком, поэтому высококачественные российские продукты успешны и там.

С ним де-факто согласился Дмитрий Огородников, подчеркнув, что несмотря на явные проблемы с документированием собственных решений и оказанием технической поддержки, по функциональным возможностям многие отечественные продукты класса DLP, IDM, антивирусной защиты и др. заметно обгоняют иностранных конкурентов. Помимо этого эксперт выделил целый ряд стратегий оптимизации затрат на ИБ — в частности свободное ПО, аутсорсинговые услуги по обслуживанию инфраструктуры, облачные технологии и онлайн-сервисы, контейнерные разработки и в целом смещение бюджетов из CAPEX в OPEX. Но указал он и на нюансы регулирования банковской отрасли: «В ИБ банков очень много конкретных требований по реализации тех или иных организационных и технических процедур, так что при использовании СПО или облачных услуг к этому вопросу нужно подходить очень аккуратно, учитывая требования соответствующих положений Банка России и федерального законодательства».

«Царь горы» банковской ИБ

Банковская сфера ИБ сложнее многих других ИБ-секторов — в ней есть отдельный регулятор, ее одной из первых атакуют киберпреступники, ИТ-ландшафт банков сложнее в сравнении с иными отраслями (поспорить здесь, пожалуй, могут лишь телеком и ИТ). Кто же вносит наибольший вклад в ИБ банковской системы — вендор, консультант, регулятор, правоохранительные органы или сами банки?

Дмитрий Романченко и Дмитрий Тирский отметили ключевую роль регуляторов, при этом первый подчеркнул необходимость вклада каждого участника для эффективной работы системы в целом, а г-н Тирский поставил на второе место банки и лишь за ними — вендоров и консультантов.

Алексей Гришин и Денис Горчаков вышли из парадигмы вопроса и отметили ключевой «вклад» киберпреступности в развитие банковской ИБ, а г-н Гришин даже описал целую последовательность значимости «вклада» в развитие ИБ: киберпреступность, регуляторы, консультанты, производители. Замыкают цепочку банки, но среди них иногда бывают и передовики, обгоняющие всю индустрию, отметил он.

А Дмитрий Огородников не стал однозначно определять ключевого игрока, назвав ландшафт ИБ банков весьма сложным, где у каждого игрока «свои роли и задачи». Он, в частности, упомянул прецедент, когда собственная команда разработчиков банка создала продукт для внутреннего использования, но со временем трансформировалась в независимую компанию-вендора с продуктом класса IDM, который вполне успешно продвигается на нашем рынке. (Отмечу, что чуть ли не каждый российский ИБ-продукт был создан на деньги заказчика, ведь уровень процентных ставок банковских кредитов и неразвитость венчурной индустрии оставляет мало выбора вендорам.)

Тратить? Нельзя терпеть?

Все наши эксперты сходятся в том, что спрос на разнообразные ИБ-проекты со стороны банков есть. На кадровых ресурсах можно найти ИБ-вакансии участников рынка, видно, как они переманивают людей, выбирают новые офисы в центре и активно инвестируют маркетинг. Эти деньги не берутся из воздуха, они приходят из реальных проектов реальных банков, которые инвестируют ИБ каждый день, понимая, что часть сэкономленных за счет цифровизации средств на привлечение и обслуживание клиентов придется направить на обеспечение должного уровня ИБ.

В противном случае менеджменту и акционерам банков не стоит надеяться на стабильное и качественное обслуживание клиентов, а тем более на рост доходов и стоимости бизнеса, прироста клиентской базы и уровня лояльности клиентов и партнеров.

Впрочем, банки всегда могут выбрать развитие партнерской сети и сети агентов, ведь 100%-ная цифровизация всей банковской отрасли вряд ли достижима — всегда останется какой-то уровень спроса клиентов на физическое обслуживание.

Автор статьи — сертифицированный специалист по управлению информационной безопасностью корпоративных и облачных ИТ-ландшафтов, член ISACA, ASIS, ACFE.