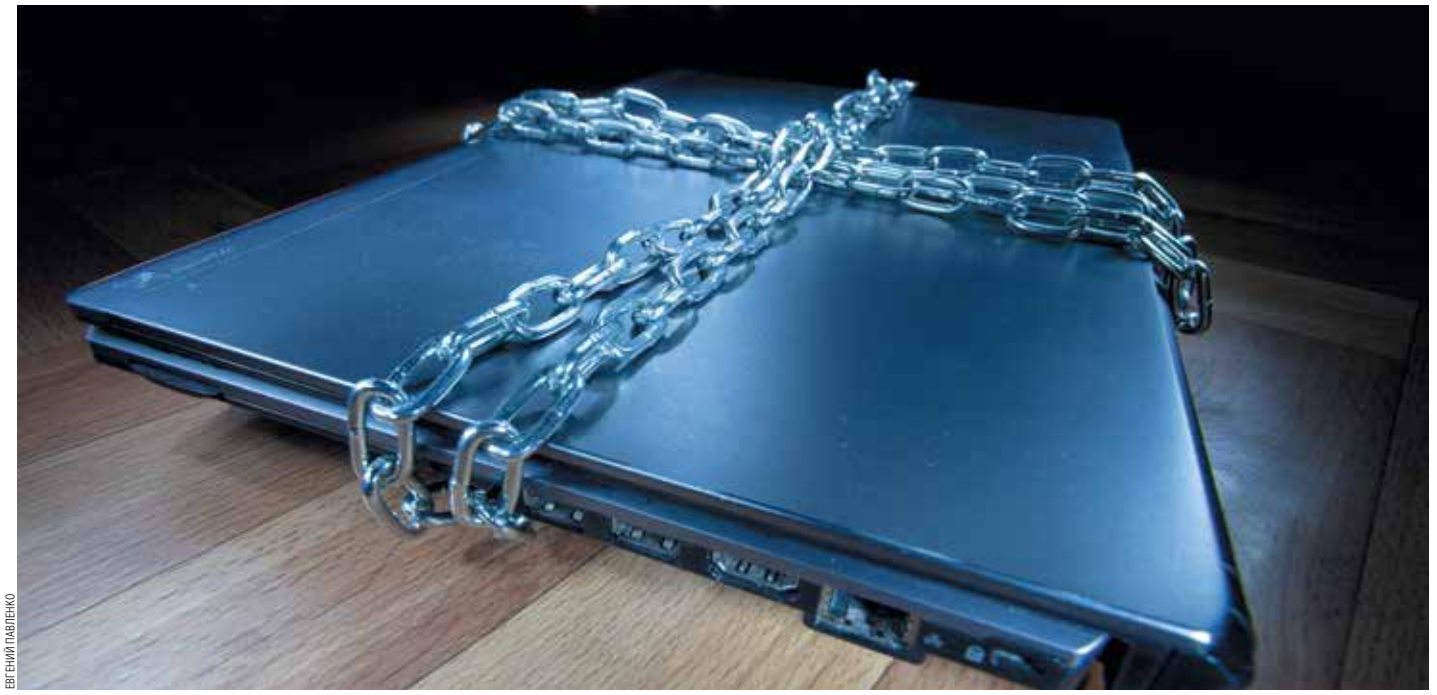
15 ➔ достигает $58 млн: это в три раза больше, чем у нефинансовых организаций. Более того, 64% опрошенных заявили, что будут вкладывать в улучшение защиты независимо от окупаемости этих инвестиций.

Рост вложений в киберзащиту имеет веские основания: в последние несколько лет количество угроз для финансовой индустрии неуклонно растет, они становятся все более сложными и чреваты серьезными последствиями. «Так, 70% банков сообщили о том, что за последний год они понесли денежные потери в результате кибермошенничества. Больше всего опасений вызывают риски, связанные с мобильным банкингом: 42% респондентов считают, что в ближайшие три года увеличится рост количества инцидентов, связанных с кражей денег через мобильные устройства. Среди других актуальных угроз для пользователей банки выделили фишинг: с ним в 2016 году сталкивались клиенты 46% компаний. Еще одна сфера повышенного риска — банкоматы. Причем всего 19% банков обеспокоены угрозой атак на них, в то время как в 2016 году объем вредоносного ПО для банкоматов вырос на 20% по сравнению с 2015 годом», — говорится в исследовании «Лаборатории Касперского».

Алексей Чалей, генеральный директор компании Cezurity, отмечает, что хакеры атакуют всех, и если банки из топ-50 могут себе позволить дорогостоящие системы киберзащиты, то небольшие кредитные организации, как правило, не готовы к кибератакам и вызывают наибольший интерес у преступников.



ЕВГЕНИЙ ПАВЛЕНКО

СРЕДНИЙ ГОДОВОЙ БЮДЖЕТ БАНКОВ НА КИБЕРБЕЗОПАСНОСТЬ ОБЫЧНО В ТРИ РАЗА БОЛЬШЕ, ЧЕМ У НЕФИНАНСОВЫХ ОРГАНИЗАЦИЙ

АТАКИ ВНЕ ПЕРИМЕТРА По словам Дениса Камзеева, директора отдела информационной безопасности Райффайзенбанка, можно выделить следующие топ-5 угроз: Advanced Persistent Threat (APT) — целевые атаки на платежную инфраструктуру банков, SWIFT, логические атаки на банкоматы, включая BlackBox, атаки типа «отказ в обслуживании» (DDoS, инсайд и утечка данных), а также мошенничество в системах дистанционного банковского обслуживания.

Марк Гойхман, ведущий аналитик ГК TeleTrade, отмечает, что в последнее время наблюдается переход на атаки в целом на базу банков и хищения не с индивидуальных, а с корпоративных счетов. «Взламывается защитная оболочка. Для этого могут использоваться вирусы, „зараженные“ электронные сообщения, программы, спецаппаратура с применением электромагнитного излучения», — говорит господин Гойхман.

Большая часть успешных крупных компьютерных атак за последние три года начиналась не со взлома периметра защиты компаний, а с атак на обычных пользователей с использованием методов социальной инженерии, считает Андрей Янкин, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет».

«Примером успешного использования социальной инженерии являются несколько взломов, начавшихся с того, что работникам банков пришли письма, в которых говорилось, что ЦБ РФ рассмотрел их резюме и хочет пригласить их на работу. Процент успешности атаки оказался удивительно высоким: несмотря на то, что работники нигде не публиковали свои резюме, любопытство оказалось сильнее здравого смысла. Урон от таких атак зачастую может превышать миллиард рублей», — рассказывает господин Янкин.

ЧУЖОЙ СРЕДИ СВОИХ Особую опасность для банков представляет утечка информации из внутренних каналов. Ущерб от инсайдов может быть довольно ощутимым и болезненным. Алексей Головченко, управляющий партнер юридической компании ЭНСО, отмечает, что российской ментальности подходит присказка «больше всего может украсть охранник, охраняющий ваш склад». В этой связи много средств уходит на реализацию контролирующих функций — обеспечение внутренней безопасности.

По оценкам Марка Гойхмана, около 80% утечки информации в сфере персональных данных и счетов клиентов — результат халатности сотрудников банков.

Александр Омельченко, начальник управления информационной безопасности Альфа-банка, уверен, что наряду с информированием и обучением персонала необходимо использовать и технические средства для выявления и предупреждения подобного рода инцидентов: систему обеспечения безопасности привилегированного доступа (PAM), систему управления событиями информационной безопасности (SIEM) и систему предотвращения утечек информации (DLP). С их помощью регистрируются, обрабатываются, контролируются и сохраняются действия пользователей, производимые на системах банка, манипуляции с данными клиентов банка, перемещение данных по сети банка и передача их наружу.

«Все это позволит вовремя выявлять неблагонадежных работников и применять соответствующие контрмеры. Также необходимо доносить до работников мысль о неотвратимости наказания в случае возникновения инцидентов», — резюмирует господин Омельченко.

БУНКЕР НЕ ПОМОЖЕТ Банки стремятся к абсолютной безопасности своей информационной среды, но цифра «100%», по мнению экспертов, является утопичной.

«Даже если организация отключится от интернета, полностью закроется, переедет в изолированный бункер где-нибудь в тайге, то вряд ли добьется стопроцентной безопасности. Бизнес такая организация неизбежно потеряет, но полностью неуязвимой все равно не станет. В реальной жизни современным банкам надо быть открытыми, грамотно лавируя между „закручиванием гаек“ и удобством пользователей», — считает Александр Санин, коммерческий директор компании «Аванпост».

По оценкам Тимофея Костина, глобального консультанта Experian в России и странах СНГ, дополнительной проблемой обеспечения полной информационной безопасности является то, что банки находятся в постоянном состоянии догоняющих: сначала выявляется новый вид мошенничества, потом начинается разработка средств и инструментов по его предотвращению.

«При этом сколько угроз еще не выявлено, сколько появится новых рисков — невозможно оценить и предсказать. Например, даже установив новейшую версию используемой DLP-системы, можно уже на следующий день обнаружить, что изменился формат передачи данных в каком-то мессенджере и DLP уже не может полноценно анализировать содержимое чата в этом мессенджере», — поясняет Ашот Оганесян, технический директор Device Lock.

По мнению Рустэма Хайретдинова, генерального директора компании «Атак Киллер», в случае с банками речь всегда идет не об абсолютной безопасности, а об эффективной. «Достаточно сделать усилия злоумышленников по взлому банковских систем более дорогими, чем возможная выгода от взлома, а риск быть пойманным — большим, и взломы станут просто неинтересными — никто не будет тратить миллион долларов, чтобы украсть тысячу», — резюмирует эксперт.

УСПЕТЬ ЗА 15 МИНУТ Риски хищений средств со счетов клиентов связаны, в том числе, с низкой осведомленностью пользователей в вопросах информационной безопасности, полагает Алексей Ершов, главный специалист по информационной безопасности банка «Александровский». И задача банков — не только обучать сотрудников, но и постоянно информировать клиентов о необходимых мерах безопасности.

Антон Казанцев, начальник службы информационной безопасности банка для предпринимателей «Точка» (финансовая группа «Открытие»), предупреждает, что обычно у человека есть 10–15 минут, пока деньги не зачислены на счет мошенников, после чего шанс их вернуть становится очень мал.

Максим Али, старший юрист юрфирмы «Максима Лигал», говорит, что если взглянуть на дела последних двух лет, которые рассматривались Санкт-Петербургским городским судом, то более чем в 85% случаев клиентам банков отказывали в возврате списанных средств.

«В таких случаях суды ссылаются на то, что все требования законодательства и условий обслуживания банковских карт были соблюдены банком, а согласие клиента на проведение операции предполагалось, поскольку от его имени был введен секретный код. Речь идет, например, о пин-коде, CVV/CVC или номере из SMS», — констатирует господин Али.

По наблюдениям Елены Потаповой, ведущего бизнес-аналитика группы компаний Custis, чаще всего кредитные организации не помогают своим же клиентам оформлять заявления в полицию, утверждая, что клиент ввел личные данные и совершил платеж добровольно. Полиция также не расположена заниматься подобными преступлениями, поскольку нет четкого описания в законодательстве.

Павел Савицкий, руководитель практики «Интеллектуальная собственность и информационные технологии» петербургского офиса юридической фирмы «Борениус», приводит в пример интересное судебное решение, которое может стать прецедентным: «В январе 2017 года Верховный суд РФ принял важное решение, которое может существенно повлиять на практику нижестоящих судов по возврату средств, похищенных у клиентов банков. Согласно позиции суда, именно банк несет риск ответственности за последствия исполнения поручений, выданных неуполномоченными лицами посредством дистанционных сервисов. При этом суд не исключил, что банк может предъявить иск к клиенту о возмещении убытков, причиненных действиями клиента, из-за которых произошло хищение его денежных средств с использованием дистанционных сервисов». ■