информационная безопасность в финансовом секторе

в мероприятии приняли участие более 90 человек, среди которых были топ-менеджеры финансово-кредитных организаций, руководители управлений и служб информационной безопасности банков, представители компаний-интеграторов, а также независимые эксперты в области ИБ

В числе активных участников круглого стола были: советник банка «ФК Открытие» **Михаил ЛЕВАШОВ**; директор по развитию компании «Актив» **Владимир ИВАНОВ**; член комитета по финансовым рынкам и кредитным организациям Торгово-промышленной палаты РФ **Тимур АИТОВ**; коммерческий директор ГК «Инфосекьюрити» **Александр ДВОРЯНСКИЙ**; заместитель генерального директора компании «Аладдин Р.Д.» **Алексей САБАНОВ**; генеральный директор компании SafeTech **Денис КАЛЕМБЕРГ**; советник председателя правления МТИ-Банка **Александр ВИЛЬДМАН**; менеджер проектов по информационной безопасности Тинькофф Банка **Алла ФИЛОНЕНКО**; начальник отдела информационной безопасности АО «ГЛОБЭКСБАНК» **Валерий ЕСТЕХИН**; начальник отдела информационно-технической безопасности ПАО «АктивКапитал Банк» **Дмитрий БУРЯ**; региональный директор компании RADWARE **Михаил СУКОННИК**; директор по развитию продуктовых решений ITD Group **Александр САКСАГАНСКИЙ**; начальник отдела информационной безопасности АО «Нижневолжский коммерческий банк» **Александр СМЕРДОВ**; руководитель отдела безопасности банковских систем Positive Technologies **Тимур ЮНУСОВ**; начальник службы информационной безопасности АО «РФК-банк» **Денис ГРАЧЕВ** и др.

Организатор: **Национальный Банковский Журнал (NBJ)** при содействии Ассоциации российских банков
Модераторы: начальник управления информационной безопасности АО КБ «Златкомбанк» **Александр ВИНОГРАДОВ**, генеральный директор Национального Банковского Журнала **Елена ЕЛИСЕЕНКОВА**

А. ВИНОГРАДОВ: Все участники нашего мероприятия, безусловно, были не на одном симпозиуме, не на одной конференции, в рамках которых речь шла о проблемах обеспечения ИБ в финансовом секторе. Поэтому я предлагаю не обсуждать общие темы, поскольку они всем нам хорошо известны, а сосредоточиться на действительно острых практических вопросах и проблемах. Одна из таких проблем – Положение Банка России № 552-П «О требованиях к защите информации в платежной системе Банка России». Документ полностью вступает в силу с 1 июля текущего года, согласно ему банкам надо будет привести в соответствие требованиям регулятора свои нормативные документы, а также провести некоторые мероприятия.

В прошлом месяце я общался с создателями данного положения, было поднято много вопросов, сделано много уточнений. Сейчас ведется работа по написанию совместно с ЦБ РФ методички, однако возникает вопрос о дальнейшем согласовании и утверждении этого документа на уровне регулятора.

Еще одной больной темой является видеонаблюдение. Не прописано, в каком качестве, с какой периодичностью записывать данные рабочего места и где их затем хранить. Все, что есть, – это указание на то, что хранить информацию требуется в течение трех лет. При этом существует Положение Банка России № 242-П (приложение 5, которое устанавливает требования к Плану ОНиВД), в соответствии с которым надо будет делать резервное копирование, причем результаты этого копирования должны храниться не в самом банке, а в другом месте.

Думаю, ни для кого не секрет, что в декабре этого года нам надо будет сделать самооценку по Положению Банка России 382-П (202 форму отчетности).

Это основные назревшие к данному моменту вопросы. Со своей стороны, я хотел бы предоставить первое слово Алексею Сабанову, чтобы он рассказал о существующих проблемах доверия к результатам идентификации и аутентификации и способах их решения.

Александр ВИНОГРАДОВ,
начальник управления информационной безопасности АО КБ «Златкомбанк»

А. САБАНОВ: Проблема в данном случае заключается в том, что пока нет принятых стандартов. Первое и второе чтение проекта прошло, эксперты озвучили свои за и против, далее предстоит общественное обсуждение, и окончательно первый стандарт будет принят в конце года. Далее планируется разработка стандарта, который будет регулировать уровень доверия к результатам идентификации, и аналогичного стандарта по аутентификации.

В чем же проблема? В том, что идентификация по биометрическим характеристикам – это очень удобная вещь, но она очень ненадежная, небезопасная и дорогая. Если вы хотите снизить риски совершения ошибок первого и второго уровня, то вам придется существенно потратиться. И уж тем более ни в какие ворота не лезет то, что некоторые эксперты настаивают на возможности использования биометрии для первичной идентификации. Мировой опыт показывает, что для того, чтобы получать хоть какую-то юридическую значимость в итоге, нам надо очень тщательно проводить идентификацию с опорой не только на биометрические данные, но и на стандартные документы – паспорт, СНИЛС и т.д. Потому что вал мошенничества в сфере биометрии уже ожидается, и риски у банков возрастут.

Кто пробовал ставить хорошие камеры, тот знает: эти камеры очень плохо работают с фотографиями. Если, напротив, поставить камеры похуже, которые хорошо работают с фотографиями, то возрастают ошибки первого и второго рода. Исследования независимых лабораторий показывают, что полностью радужную оболочку глаза рассмотреть невозможно, максимум на 60–70%. То же самое можно сказать и о голосовой идентификации.

Суть моего выступления сводится к следующему: стандартов по идентификации пока нет, проблемы доверия к результатам идентификации есть, но эти проблемы должны решаться не наскоком, а взвешенно и с тщательным учетом возможных рисков.

А. ВИНОГРАДОВ: Я хотел бы задать вопрос по биометрической идентификации. Знаю, что клиенты одного банка хотят идентифицироваться в мобильном банкинге, используя свое фотоизображение. Сейчас нет четкого понимания, можно ли рассматривать этот способ как биометрическую идентификацию или нет. И в каком качестве он может использоваться в банках – как основной метод идентификации или как дополнительный.

А. САБАНОВ: Биометрия, конечно, очень удобная вещь, поскольку не надо носить с собой никаких ключей, смарт-карт и т.д. Но надо понимать, что надежность идентификации по селфи – 60–70%, а может, и ниже, поскольку фотографии будут делать сами клиенты. Моя позиция такова: подобные подходы годятся только для малорисковых операций – если на счетах клиентов, например, лежит 10 тыс. рублей, пусть развлекаются.

Но, собственно говоря, дело не в этом: прежде чем человек станет клиен-

том банка, его нужно четко идентифицировать. Одной биометрии здесь явно недостаточно, и я бы по примеру некоторых стран запретил на законодательном уровне ее использование в качестве единственного метода идентификации. Посмотрите сами: только-только банки вздохнули и хоть немного привели в порядок ситуацию с фродами, как появилась проблема с идентификацией клиентов. Бизнес, конечно, настаивает на своем: надо делать так, чтобы клиентам было максимально удобно пользоваться услугами, это позволит банкам существенно увеличить продажи и повысить свою конкурентоспособность. Это весомый аргумент, но сразу же возникает вопрос: а кто будет нести ответственность в случае, если в ЕСИА от банков будут поступать недостоверные персональные данные или если эти данные просто украдут из базы? Когда задаешь этот вопрос, то понимаешь: у нас не коллективная ответственность, а коллективная безответственность.

М. ЛЕВАШОВ: Конечно, мы, как специалисты в сфере ИБ, не можем стоять на пути бизнеса. Банки неизбежно будут внедрять новые, востребованные клиентами услуги и продукты, делая при этом максимально удобными для клиентов способы их получения. Но, как справедливо отметил Алексей Сабанов, главный вопрос, который возникает в этом случае, – кто будет отвечать за возможные клиентские потери, вызванные мошенническими действиями злоумышленников? Кто будет платить, когда клиенты начнут массово жаловаться на то, что у них несанкционированно списывают средства со счетов? Согласен я с коллегой и по вопросу идентификации по биометрии. Если вы ее используете, то всегда надо оставлять открытой back door – запасную дверь – в виде классических способов идентификации, например по паспорту, СНИЛС и т. д.

Т. АИТОВ: Надо сказать, что в части биометрической идентификации сектор розничной торговли уже явно опередил банковский сектор. Предприятия, работающие в этом секторе, поступают следующим образом: вас незаметно фотографируют в то время, когда вы посещаете торговый центр, потом идентифицируют по социальным сетям и дают таргетированную рекламу. А мы же знаем, что банковский сектор во всем, что касается работы с клиентами, копирует торговлю. И что может произойти? Один банк поставит у входа в офис другого банка свою машину и будет фотографировать входящих клиентов. Думаю, не надо уточнять, с какой целью. Этот риск тоже надо учитывать, когда мы говорим о биометрической идентификации.

В. ИВАНОВ: Первый момент: маркетинговый шум, который поднят вокруг биометрии, опасен, поскольку маркетинговыми методами нам пытаются продать идентификацию вместо аутентификации. Биометрия – неплохой способ идентификации, но аутентификация и авторизация операций – это совсем другое дело.

Во-вторых, когда вы подменяете аутентификацию идентификацией, не забывайте, что сменить идентификатор в данном случае практически невозможно. В случае компрометации биометрических данных вы серьезно испортите жизнь многих людей.

Третий момент: злоумышленникам малоинтересно проводить атаки с использованием несовершенств биометрии на счета с малыми суммами. А вот когда речь зайдет об операциях с крупными счетами и авторизации с помощью биометрических данных, то ситуация изменится, и тогда вам следует быть

Владимир ИВАНОВ,
директор по развитию компании «Актив»

Бизнес-подразделения банков стремятся привлечь новых клиентов и повысить лояльность старых. Для этого они хотят заполучить новые «фишки», которые отличали бы их от конкурентов. Биометрическая идентификация по селфи и голосу – это модная технология, которая, однако, не доказала свою безопасность.

Представители сферы информационной безопасности сформировали свое мнение относительно биометрической идентификации, но им достаточно сложно убедить бизнес в том, что технология еще сырая и приемлемого уровня защиты не обеспечивает. Существует дефицит информации и результатов серьезных исследований. Бизнес же основывается в основном на маркетинговых заявлениях вендоров биометрических решений.

Поэтому перед ИБ-специалистами стоит задача по оценке рисков внедрения новых технологий идентификации, связанных с возможными инцидентами ИБ, репутационными потерями и реакцией регулятора на возникновение инцидентов. На них же лежит ответственность за принятие решений, связанных с внедрением биометрической идентификации.

Оправдает ли внедрение новой дорогостоящей технологии ожидания бизнеса? Вложения в биометрию велики, и вопрос возврата инвестиций нуждается в серьезной проработке. Задача ИБ-специалистов состоит в том, чтобы найти безопасные способы применения новых технологий, изучить мировой опыт, не испортить жизнь клиентам банка.

готовыми к активизации мошенников. Причем злоумышленникам, если говорить о голосовой идентификации, даже не надо будет записывать пароль: они смогут смоделировать вашим голосом любую необходимую фразу.

Огромные успехи сегодня делает индустрия 3D-визуализации, поэтому идентификация по лицу тоже скоро окажется под большим вопросом. Вы не ходите в парандже и в перчатках, вы всюду оставляете свои следы. Снять вас с любого ракурса злоумышленникам не составит никакого труда. А затем на базе этих снимков смоделировать ваше изображение в 3D.

Д. КАЛЕМБЕРГ: Я согласен с тем, что именно маркетинг двигает тему биометрии, и бизнес-подразделения банков действительно очень настаивают на применении этой технологии для идентификации и аутентификации клиентов. И я, как и выступавшие передо мной спикеры, тоже предупреждаю банкиров: сегодня вы «ведетесь» на новую и действительно удобную и для вас, и для клиентов технологию, но вы должны быть готовы к тому, что через два-три года вы столкнетесь с резким ростом рисков в этой сфере. И я согласен с тем, что можно прибегать к этому методу, когда речь идет о небольших операциях, например по оплате счетов мобильных телефонов.

Я хотел бы затронуть еще одну тему: сейчас появилось такое активно развивающееся направление, как мобильный банкинг юридических лиц. Очень многие банки стали подтверждать операции таких клиентов с помощью СМС. Это очень рискованная технология, и я думаю, что в рамках нашего круглого стола как раз следует обсудить то, какими методами банкам лучше пользоваться в данном случае.

В. ЕСТЕХИН: Вопрос, кто виноват, плавно перетекает в вопрос отсутствия нормативной базы. Как мы будем внедрять биометрию, как можно наказывать кого-то за преступления в сфере идентификации, если нет необходимых законов и

Александр ВИЛЬДМАН,
советник председателя правления МТИ-Банка

нормативов? Без всего этого данная тема фактически подвисает в воздухе.

А. САБАНОВ: По правде говоря, в этом вопросе я пессимист. Если будет разработан проект стандартов по идентификации и аутентификации, то его будут очень долго согласовывать различные ведомства. Специалистов в этой сфере недостаточно, так что ожидать чуда в данном случае не приходится. Тем не менее вы совершенно правильно говорите о том, что какие-то стандарты нужны – хотя бы для того, чтобы появилась всеми принятая терминология, описывающая соответствующие процессы.

А. ВИЛЬДМАН: Я, честно признаться, не понимаю высказанного здесь пренебрежительного отношения к счетам с небольшими суммами. Любое такое событие – это инцидент в сфере информационной безопасности, и будьте уверены, он не останется без внимания нашего регулятора. Вам что же, хочется, чтобы вам «прилетали» оттуда требования увеличить резервы? Думаю, нет, поэтому мы все должны понимать, что наше стремление подарить клиенту красивый фантик в виде, например, авторизации операций с помощью фотографии может закончиться очень печально и для самого клиента, и для банка, в котором этот клиент обслуживается. Будем честны друг с другом: такую роскошь могут позволить себе только крупнейшие игроки сектора, а всем остальным рекомендуется быть осторожными в данном вопросе.

Д. БУРЯ: Коллеги, вы обсуждаете биометрическую идентификацию в банковской сфере, и в связи с этим я хотел бы задать вопрос: смотрел ли кто-либо из вас статистику идентификации личности по биометрическим данным при раскрытии и расследовании преступлений? Может ли кто-нибудь из вас озвучить показатели достоверности результатов, например, по распознаванию лиц в информационных системах правоохранительных служб? А ведь результаты идентификации личности по биометрическим данным далеки от совершенства и для повышения достоверности требуют привлечения экспертов. Я даже не говорю о случаях мошенничества с умышленным изменением внешности, речь идет исключительно об ошибках идентификационных систем при обычных условиях. Исходя из этого, очевидно, что использование данных систем в банковской сфере в качестве единственного инструмента идентификации и аутентификации, учитывая расходы на обеспечение их работы, на данном этапе неэффективно. Кроме того, появляется проблема хранения биометрических данных, а это тяжелые файлы – готовы ли банки нести расходы на содержание больших собственных ЦОДов или платить аутсорсерам, чтобы они содержали этот массив на стороне? А если эти данные «утекут», то на ком опять же будет лежать ответственность за этот прецедент? И еще один вопрос, который был задан совершенно справедливо, – кто должен платить за все это при принятии решения об обременении банков данными сервисами?

С учетом всего этого и ряда других проблемных вопросов по той же теме мой вывод таков: на данном этапе

использование биометрии в качестве единственного инструмента идентификации и аутентификации нецелесообразно и с экономической точки зрения, и с точки зрения исключения рисков в сфере обеспечения безопасности платежей.

Вместе с тем при наличии у банка ресурсов для реализации данных сервисов их использование в качестве дополнительного идентификатора в процессе совершения транзакций при дистанционном банковском обслуживании вполне оправданно. Представьте себе ситуацию: банку со смартфона клиента (или иного технического средства) приходит запрос на совершение той или иной операции по счету, на номер телефона клиента отправляется код подтверждения, и он его вводит, при этом банк не знает, кто в данный момент держит этот телефон в руках и нажимает на кнопки. Другое дело, если вместе с запросом вы получаете онлайновое изображение клиента, транслируемое устройством, с которого и производится запрос на совершение операции: данное изображение сопоставляется с изображением, хранящимся в базе данных банка, и тогда определение достоверности совершения операции именно клиентом, а не третьим лицом, возрастает. Более того, предлагаемые в настоящее время подобные решения (они уже существуют на рынке) осуществляют данную процедуру в интерактивном режиме, предлагая клиенту совершить активные действия, которые фиксируются камерой, – например, подмигнуть либо улыбнуться – что в еще большей степени повышает достоверность идентификации клиента, а также дает возможность упрощения процедуры разрешения инцидентов в случае их возникновения.

Алексей САБАНОВ,
заместитель генерального директора компании «Аладдин Р.Д.»

Однако хотелось бы еще раз подчеркнуть, что вопрос приобретения данных систем должен быть добровольным для кредитно-финансовых организаций и не являться навязанным обременением, которое может отразиться на состоятельности данных организаций.

М. СУКОННИК: Правильно замечено, что для использования в качестве единственного средства идентификации все упомянутые здесь современные средства еще слишком сыры и непонятны. Они могут служить дополнительным средством, дополнительной ступенью при проведении проверок, не отметая существующие помимо них средства. Вообще у безопасников есть убеждение: невозможно остановить преступника, если у него достаточно времени и денег, чтобы преодолевать преграды, которые вы выставляете на его пути. Решение проблемы заключается в том, чтобы выставлять как можно больше препятствий, истощая либо его время, либо его деньги.

М. ЛЕВАШОВ: Проблема-то как раз в том, что определенная группа клиентов, которую мы очень условно назы-

Александр ВОРОЖИЩЕВ,
директор по развитию бизнеса компании «Андэк»

Клиенты банков становятся более требовательными к качеству и скорости оказываемых им услуг, а конкурентная борьба между банками становится все более острой. И выиграют в этой борьбе те участники рынка, которые будут полностью соответствовать пожеланиям клиентов, в том числе пожеланию, чтобы идентификация пользователей и аутентификация их операций осуществлялась максимально быстро.

На первый взгляд может показаться, что такой способ есть. Благодаря современным мобильным устройствам клиент может сделать свою фотографию и отослать ее в банк, чтобы там с помощью биометрических технологий его идентифицировали. Но это только на первый взгляд. При более внимательном рассмотрении мы обнаруживаем целый ряд уязвимостей такого подхода. В результате этого операции, осуществляемые клиентом, могут оказаться скомпрометированными. Я хотел бы особо подчеркнуть следующее: безусловно, биометрические технологии могут и должны использоваться, но не как основной, а как дополнительный метод идентификации клиента и аутентификации запрашиваемых им операций. Возможно, со временем наступит момент, когда эти технологии будут уже достаточно апробированы и будут выработаны средства противодействия злоумышленникам. Но пока этот момент точно еще не наступил.

ваем студентами, не хотят использовать биометрическую идентификацию только как дополнительный механизм. Они хотят видеть ее в качестве основного инструмента аутентификации и подтверждения своих запросов. Они не желают вводить логины, пароли, это, с их точки зрения, скучно и трудно. Надо ли отвечать на эти их запросы? Да, но при этом нужно предупреждать клиентов о том, что некоторые их желания – например, чтобы им выдавали деньги только по фотографиям их лиц, – чреваты серьезными рисками для клиентских средств. Потому что если банк этого не делает, это означает только одно: он берет на себя ответственность за денежные потери клиентов, возникшие в результате мошеннических действий злоумышленников.

А. ДВОРЯНСКИЙ: В последние годы фиксируется устойчивая тенденция: увеличивается количество атак на счета физлиц, в том числе и те, на которых хранятся небольшие суммы. Тут вступает в дело старый принцип «десять старушек – это уже целый рубль», то есть злоумышленники рассчитывают на эффект масштаба. У нас в стране миллионы людей имеют на счетах относительно небольшие суммы, и все отчетливо понимают, чем может обернуться целенаправленная атака против них – тогда счет может пойти уже на миллиарды рублей.

А. ВИЛЬДМАН: Структура нашего рынка такова, что есть банки, которые легко могут перенести и финансовые потери, и репутационные издержки, возникающие в случае успешных атак на счета их клиентов. Но для любого другого участника сектора инцидент в сфере ИБ – это в первую очередь удар по репутации и практически неизбежные негативные регуляторные последствия.

А. ВИНОГРАДОВ: Честно признаюсь, что я даже не ожидал, что тема идентификации и аутентификации вызовет такое бурное обсуждение. Давайте все же

Михаил СУКОННИК,
региональный директор компании RADWARE

перейдем к еще одному вопросу, который мы предлагаем поднять в рамках нашего круглого стола, – о таргетированных атаках.

М. СУКОННИК: Обратите внимание на то, что происходит с внешними атаками на банковские системы. Во-первых, количество и продолжительность таких атак растет, о чем свидетельствует статистика и за рубежом, и в нашей стране. Во-вторых, меняется такой параметр, как качество атак: с каждым годом они становятся все сложнее, каждая из них включает в себя минимум пять векторов. Но самое интересное заключается в том, что год за годом под воздействием одних и тех же атак устойчивость работы приложений в одних и тех же банках нарушается. Чаще всего речь не идет о том, что системы полностью «ложатся», банки продолжают осуществлять обслуживание клиентов, но качество сервиса заметно ухудшается, поскольку приложения начинают тормозить. И есть сезонный фактор – замечательный месяц ноябрь, когда мы все становимся свидетелями того, как крупнейшие банки «ложатся» из-за не самых сложных видов атак.

Что в связи с этим хотелось бы обсудить? FinCert выпустил рекомендации по идентификации атак и противодействию им. Мы видели очень похожий документ, выпущенный в США, аналогичные документы готовятся и в европейских странах. Так вот, главный посыл состоит в следующем: необходимо бороться не с DDoS-атаками, а за то, чтобы клиенты могли продолжать работать. Я всегда говорю: побороть DDoS-атаку просто – отключите интернет, выбросьте кабель, и все! А вот как сделать, чтобы клиенты банка при этом не пострадали, чтобы они продолжали обслуживаться в обычном для себя режиме, – это действительно очень актуальный вопрос.

Второй момент, на который я хотел бы обратить внимание участников нашего мероприятия: необходимо отражать атаку, идущую по всем векторам. Иными словами, нет повода для радости и ликования, если вы отразите атаку на 95%, оставшиеся 5% все равно «положат» сервера и системы. Поэтому руководство банков справедливо не интересуют наши рапорты о том, что мы 95% атак отразили, – их куда больше волнует, что банк не может продолжать обслуживание клиентов в нормальном режиме из-за «прорвавшихся» 5%.

Специфика нынешней ситуации состоит в том, что большие атаки банки и провайдеры более или менее научились отбивать. А вот с маленькими дело обстоит гораздо хуже. СМИ обращают внимание именно на большие сетевые атаки. Дело не в их размерах, а в том, готовы ли на другой стороне к их отражению.

И третья важная характеристика – скорость отражения атак. Необходимо это делать быстрее, чем могут поменять тактику атакующие, то есть в считанные секунды и единицы минут. Сделать это вручную не представляется возможным – нужны автоматические системы.

А. САКСАГАНСКИЙ: Все, что связано с сетевыми атаками, становится более многообразным и требует достаточно быстрого реагирования, внедрения новых средств в инфраструктуру. И я хотел бы обратить внимание всех участников круглого стола на то, что появились средства, которые используют подходы к моделированию и профилю поведения, типичного для нормальных клиентов банков. Проще говоря, современные вычислительные мощности позволяют вырабатывать решения, которые дают возможность отражать многие виды атак. Я не хотел бы подробно вдаваться в техническую сторону вопроса, но мы видим, что использование подобных решений дает очень интересные результаты.

Такие решения хорошо работают после небольшого обучения на реальном трафике, которое они производят автоматически. После начала DDoS-атаки система автоматически начинает фильтровать трафик, при этом скорость реакции составляет не более 20 секунд с начала атаки. Это позволяет серьезно снизить нагрузку на специалистов дежурной смены.

Т. ЮНУСОВ: За год наши эксперты исследуют как минимум двадцать различных бизнес-приложений (в том числе ДБО и пр.). И как минимум 2–3 раза в год мы сталкиваемся с ситуацией, при которой буквально одним запросом можно «положить» все приложение. Банки уверены, что на повестке дня, по сути, вопрос о силе и времени – насколько у них хватит и того, и другого, чтобы справиться с DDoS-атакой. Но это только одна сторона проблемы. А другая заключается в наличии банковских приложений, часто настолько непрофессионально (буквально на коленке) сделанных, что «положить» их за считанные минуты – это задача, решить которую способен злоумышленник, не обладающий сколько-нибудь высоким уровнем квалификации (любитель). А об их устойчивости к атакам со стороны профессиональных хакеров и вовсе говорить не приходится.

В. ИВАНОВ: Мы опять наблюдаем подмену понятий и игру в слова. Нам пытаются продать защиту от банального флуда, выдавая ее за защиту от DDoS. Давайте вспомним, что DoS или DDoS – это цель атаки, и неважно, сколько трафика было израсходовано. Давайте все-таки применять знания, полученные нами в институтах, и не будем позволять маркетологам обманывать себя в очередной раз.

М. СУКОННИК: Защититься нужно и от флуда, и от DDoS-атак, причем делать это необходимо одновременно.

А. ДВОРЯНСКИЙ: Можно долго ранжировать риски, но у каждого банка своя клиентская стратегия, свое понимание рисков и свой подход к решению проблем в сфере ИБ. Поэтому, на мой взгляд, ответ может быть только одним: какой-либо панацеи не существует, необходим комплексный подход к решению вопроса обеспечения ИБ.

А. САКСАГАНСКИЙ: Очень актуальна сейчас тема атак, совершаемых с помощью социальной инженерии. Один из наших партнеров – крупный банк, обладающий разветвленной филиальной сетью, – жаловался нам на то, что атаки на его системы в регионах идут как раз со стороны злоумышленников, которые используют механизмы социаль-

Алексей САБАНОВ,
заместитель генерального директора компании «Аладдин Р.Д.»

Биометрическая идентификация клиентов может служить дополнительным (не основным) фактором идентификации и аутентификации в части доказательства принадлежности смарт-карты или токена, содержащих аутентификационную информацию, конкретному физическому лицу. Стандарт США FIPS PUB 201-2 рекомендует применять биометрию только для разблокирования смарт-карты, содержащей сертификат доступа и закрытый ключ. Однако служить основным средством первичной идентификации (различия одного из многих) ни одна биометрическая характеристика не способна по своей природе.

Биометрическая идентификация граждан основана на методах математической статистики и характеризуется ошибками первого (FAR – False Accept Rate, злоумышленник идентифицирован вместо легального пользователя) и второго (FRR – False Reject Rate, отказ в идентификации легальному пользователю) рода. Согласно научным исследованиям, из десятимиллионной выборки (аналог – население Москвы) по крайней мере 10 тыс. человек имеют схожие параметры при применении одного из самых точных механизмов – анализа радужной оболочки глаза. Другие методы дают значительно больше ошибок, или стоимость их внедрения не вписывается в бюджет даже самых крупных банков.

Таким образом, идентификация клиентов и требования к ее организации в банках должны соответствовать рискам. Для операций с низким уровнем рисков применение методов идентификации с низким уровнем доверия, к которым относится и биометрия, возможно. При этом модели трансляции идентификации, обсуждаемые в последнее время, требуют внимательного рассмотрения с точки зрения неизбежных потерь доверия при передаче от одного кредитно-финансового учреждения другому.

ной инженерии. Не нужно делать никаких поддельных сим-карт или писать сложное программное обеспечение – достаточно организовать обзвон клиентов или общение с ними в социальных сетях, и они сами обо всем расскажут.

Но я хотел бы сказать еще об одном. Когда мы выстраиваем периметр безопасности в банках, то, конечно, в рамках таких проектов идут тренинги. Сотрудникам, например, приходят фишинговые сообщения: люди, открывающие их, просматривают ролик или мультфильм о том, какие последствия может иметь вскрытие такого письма. У меня в связи с этим возникает вопрос к коллегам: как вы думаете, имеет ли смысл проводить такие же тренинги среди клиентов?

Т. ЮНУСОВ: Знаете, давайте не будем переходить на удобную для нас сторону, а перейдем к вопросу, который является наиболее острым. По моему личному опыту, устроив обзвон сотрудников банка, даже тех, кого уже обучали правилам безопасности, можно собрать до 30% учетных записей! Это очень большая цифра. И мне кажется, что вот как раз с этим ничего не поменяется, если всерьез не взяться за обучение сотрудников. А с другой стороны, процесс не должен быть построен так, чтобы люди приходили в банк только для того, чтобы обучаться.

А. СМЕРДОВ: Вопрос обучения сотрудников является довольно острым. Да, мы можем слать по 10, 20 и даже 50 писем о том, что вот так делать надо, а вот так – нельзя. Но мы же все знаем, что сотрудники часто меняются, и в таких условиях эффективность обучения каждый раз оказывается под вопросом. Причем самое интересное, что ошибки совершают не только новые сотрудники, но и старые. Получается, что этот процесс должен быть непрерывным.

А. ДВОРЯНСКИЙ: У нас процесс обучения и повышения осведомленности пользователей построен следующим образом:

Александр ДВОРЯНСКИЙ,
коммерческий директор
ГК «Инфосекьюрити»

каждый сотрудник, независимо от его должности и региона работы, проходит вводный инструктаж. Далее на периодической основе производится рассылка по различным тематикам: начиная от требований и рекомендаций по парольной политике и заканчивая рекомендациями по защите от потенциального фишинга, также не менее 2 раз в год проводится физический тренинг и т.д. Вопрос с ротацией кадров у нас решается как раз входным тренингом, продолжительность которого составляет порядка 40 минут. И практика показывает, что уровень осведомленности персонала в вопросах обеспечения информационной безопасности находится на достаточно высоком уровне.

А. ВОРОНЕНКО: Люди редко читают письма, которые им приходят, и уж тем более читают их внимательно. Можно, конечно, обучить их, но вся красивая картинка рушится, когда приходится иметь дело с таргетированными атаками, и в ход идет социальная инженерия, а не просто массовые рассылки. И ведь проблема в том, что современный злоумышленник – это не человек в темных очках и в надвинутой на глаза шляпе. Это может быть их же коллега, который сидит рядом или напротив, и людям очень сложно это объяснить, они просто не могут в это поверить. Соответственно, тут выход один: непосредственно начальникам надо договариваться со специалистами по ИБ, чтобы не было ситуаций, когда ИБ пугает, а непосредственно начальник бизнес-подразделения дает понять, что все эти страшилки – ерунда.

А. ВИЛЬДМАН: Никакой тренинг никогда никого не защитит ни от какой угрозы. Защитить может только постоянная и планомерная работа среди коллег, пресечение возможностей открывать ссылки, продуманная парольная политика, индивидуальный подход к сотрудникам.

В. ИВАНОВ: Мы и говорим о том, что тренинг должен быть не самоцелью, а одним из компонентов организации информационной защиты компании или банка.

Д. ГРАЧЕВ: Я считаю, что сотрудники должны не просто знать о существовании службы ИБ, но и на постоянной основе чувствовать ее присутствие. То есть надо проводить не просто формальный инструктаж или беседу, а буквально на пальцах объяснять людям, что можно делать и что нельзя. И надо показывать, что все действия сотрудников контролируются службой ИБ, поэтому давайте жить дружно.

NBJ: Как мы видим, получилась очень интересная и, что особенно ценно, многоаспектная дискуссия. Нам удалось обсудить лишь несколько острых проблем и вызовов, которые стоят сейчас перед финансово-кредитными организациями в контексте обеспечения их информационной безопасности. Круг этих проблем гораздо шире, поэтому мы твердо убеждены в том, что это не последний наш круглый стол на тему информационной безопасности в финансовом секторе. Борьба за ее обеспечение будет постоянной.