Информационная безопасность в банковском секторе

В мероприятии приняли участие более 60 человек, среди которых руководители управлений и служб ИБ в банках, представители компаний-интеграторов, независимые эксперты

Активное участие в обсуждении различных вопросов приняли следующие спикеры: управляющий директор блока «Технологии» Сбербанка РФ и ПАО Сбербанк **Владислав КОНТОРОВИЧ**; начальник управления информационной безопасности АО «Интерпрогрессбанк» **Алексей СВИРИДЕНКО**; советник Банка «ФК Открытие» **Михаил ЛЕВАШОВ**; советник председателя правления «МТИ-Банк» (АО) **Александр ВИЛЬДМАН**; эксперт Ассоциации российских банков **Константин МАРКЕЛОВ**; советник Российского национального коммерческого банка (РНКБ) **Сергей НИКИТИН**; директор по развитию бизнеса компании Group-IB **Кирилл КЕРЦЕНБАУМ**; начальник отдела ИБ НС Банка, заместитель руководителя службы финансового мониторинга ВТБ 24 **Алексей ТИМОШКИН**; директор по развитию бизнеса Россия, СНГ и Монголия SWIFT **Екатерина КАЛИНИНА**; директор по развитию бизнеса банковский сектор Россия, СНГ и Монголия, SWIFT **Павел ПРОКУДИН** и др.

Организатор: **Национальный Банковский Журнал (NBJ)** при содействии Ассоциации российских банков.
Модератор: начальник управления информационной безопасности АО КБ «Златкомбанк» **Александр ВИНОГРАДОВ.**

NBJ: Тема информационной безопасности продолжает оставаться злободневной, и ее актуальность постоянно растет, что неудивительно, если учитывать количество хакерских атак и объемы клиентских средств и персональных данных, которые оказываются под ударом. Поэтому, наверное, никого не удивляет то, что Национальный Банковский Журнал NBJ регулярно проводит тематические круглые столы, посвященные проблемам, связанным с ИБ. И первый вопрос, который мы хотели бы адресовать аудитории в рамках очередного такого круглого стола, сформулирован следующим образом: каковы, по вашему мнению, главные тенденции, превалирующие в сфере ИБ в наше время?

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

А. СВИРИДЕНКО (Интерпрогрессбанк): Сама формулировка вопроса подразумевает, что каждый из нас должен поделиться своими знаниями и опытом организации, в которой он работает. Лично я больше всего сталкиваюсь с тем, что растет объем работ по информационной безопасности. Это и пентесты, и «нормативка». Привычные механизмы защиты уже не действуют, и мы понимаем, что в силу этого часть хакерских атак может оказаться успешной. В такой ситуации наша главная задача – сделать так, чтобы они не нанесли критического урона организациям, которые являются мишенью атак. Если киберпреступность представляет собой основной тренд, то другой не менее важной тенденцией является создание киберустойчивости.

А. ВИНОГРАДОВ (Златкомбанк): Действительно, вопросом на злобу дня является появление новых угроз, с которыми пока нельзя справиться, поскольку еще не созданы средства противостояния им. Должен сказать, что одну из таких угроз мы нашли в части ДБО. Мы поставили в известность об этом FinCert и разработчиков решений в сфере ИБ и уведомили и тех, и других, что данная угроза настолько серьезна, что мы не можем придать гласности ее механизм, рассказать даже в общем о ее характерных признаках. Причина проста. Если мы это сделаем, то завтра 60 % банковского рынка будет однозначно подвергнуто хакерским атакам. А адекватно защититься от этого нападения мы, как я уже сказал, не сможем.

А. ВИЛЬДМАН (МТИ-Банк): Озвучивать действительно не стоит, раз не существует соответствующих средств и способов борьбы. Если же говорить о разработчиках, то общение с ними преимущественно заканчивается печально, потому что они обычно говорят, что не отвечают за безопасность. Иными словами, что обеспечение ИБ – на стороне банков, а не их дело.

М. ЛЕВАШОВ (Банк «ФК Открытие»): Современный подход к безопасности подразумевает, что мы уже живем и будем жить в эпоху практически непрерывных атак вредоносного ПО (ВПО), которое различными путями будет пытаться проникать в наши информационные системы. И здесь должна быть обеспечена эшелонированная оборона, которая начинается с обучения персонала (социальная инженерия) и продолжается на всех возможных рубежах, которые пытается преодолеть ВПО. Это и решения класса NGFW, и различного рода испытательные полигоны («песочницы»), и многофакторность и многоканальность защиты... Получается своего рода многослойный бронежилет, в котором злоумышленнику для преодоления каждого слоя требуется все возрастающее количество усилий и времени.

А. ВИЛЬДМАН (МТИ-Банк): Вполне очевидно, что под ваше описание в первую очередь подходит уязвимость в системе ДБО. К сожалению, если злоумышленник использует ее, он попадет в самую точку. Что бы мы ни строили, как бы мы ни защищали периметр – без разницы. Можно защититься только антивирусом, и то надо отдавать себе отчет в том, что даже самый лучший антивирус ловит примерно 25% всех «печалей».

А. СВИРИДЕНКО (Интерпрогрессбанк): Почта, интернет – это все средства недоверенной доставки, и мы их однозначно проверяем. ДБО у нас всегда

Алексей СВИРИДЕНКО,
начальник управления информационной безопасности АО «Интерпрогрессбанк

Александр ВИЛЬДМАН,
советник председателя правления «МТИ-Банк» (АО)

идет как средство доверенной доставки сообщений. Они приходят на компьютер операциониста, который коммуницирует с тем или иным клиентом. Самое простое, что можно в этом случае сделать, – это работать с персоналом. Пришел файл с указанным расширением – зови айтишников, кидай полученный файл в «песочницу», где его будут проверять специалисты на наличие различных угроз для ИБ.

К. МАРКЕЛОВ (АРБ): Все мы не раз летали на самолетах, поэтому знаем, что такое чистая зона аэропорта. Но при этом всегда есть вероятность того, что в здание аэропорта будет внесен некий пакет, на котором будет написано «дипломатическая почта». Его нельзя проверять, просвечивать и т.д., и эта вещь приходит в чистую зону аэропорта, а там оказывается бомба. С моей точки зрения, это сравнение подходит к той ситуации, которую мы обсуждаем. И тут можно предложить только один вариант решения проблемы. Каждый пришедший снаружи пакет должен вскрываться, независимо от того, является ли он обычным или «дипломатическим».

NBJ: Для того чтобы отправить вредоносное письмо, надо владеть клиент-банком, т.е. надо иметь доступ к конкретному ДБО юридического или физического лица. Насколько часто обнаруживается, что у злоумышленников он есть, несмотря на наличие систем многофакторной аутентификации и других средств защиты?

А. ВИЛЬДМАН: Все уязвимости 99% в периоде) ДБО находятся на стороне клиента, потому что убедить его что-то соблюдать – задача априори неблагодарная. В результате таких случаев великое множество и в малом, и в крупном бизнесе. Сейчас уже, наверное, меньше «зловредов», которые берут компьютер под управление, но если у тебя есть цель «повалить» банк, то это сделать можно.

А. ВИНОГРАДОВ (Златкомбанк): В банки очень часто приходит письмо о том, что им прислано дополнительное соглашение к договору о клиентском обслуживании. В 99 % случаев, сколько ни обучай сотрудников, они все равно открывают его. Хотя первое, что мы им говорим при обучении, – это о необходимости проверки, есть ли у банка такой клиент.

К. КЕРЦЕНБАУМ (Group-IB): Нельзя забывать о том, что такое письмо можно отправить также из системы ДБО физлиц, необязательно из ДБО юрлиц. У физлиц нет трехфакторной аутентификации, в лучшем случае двухфакторная. Я знаю банки, у которых реализация системы ДБО допускает, что в ней можно зарегистрироваться даже без карты: то есть вы просто совершаете регистрацию в личном кабинете, а потом уже делаете запрос на карту. Система информационного обмена изначально предусматривает отправку некоего скана, которым, как правило, является PDF-документ, а это один из самых уязвимых форматов, что необходимо учитывать.

Хотелось бы также добавить несколько слов по поводу сотрудников, встав на их защиту. Обучать

Константин МАРКЕЛОВ,
эксперт Ассоциации российских банков

персонал, конечно, надо. Как в автомобиле, так и в информационной системе самое уязвимое – это промежуточное звено между монитором и сиденьем, то есть человек. Но технологии не стоят на месте: модифицируется фишинг, распространяется фарминг (процедура скрытного перенаправления жертвы на ложный IP-адрес. – Прим. ред.). Представьте, что вам приходит письмо от вашего руководителя или подчиненного с почтового сервера вашей компании. Заподозрите ли вы неладное? Скорее всего, нет. Люди далеко не всегда виноваты в том, что такие атаки становятся возможными.

А. ВИНОГРАДОВ (Златкомбанк): Мы все время говорим: клиент, клиент. Мы думаем, что они все хорошие, но они бывают разными, и давайте мы не будем забывать о том, что среди них есть и те, которые специально приходят, чтобы заразить наши компьютеры или нанести банку еще какой-то вред, используя при этом ИТ-технологии.

М. ЛЕВАШОВ (Банк «ФК Открытие»): Мы говорим о том, что действительно есть некие бэкдоры, письма, сообщения, которые проходят первоначальную

Кирилл КЕРЦЕНБАУМ,
директор по развитию бизнеса компании Group-IB

процедуру контроля и попадают в информационную систему банка. Что дальше? Для того чтобы вирус начал действовать, должны быть определенные условия. Он не может начать работать, если ему не позволяет это делать система защиты на следующем этапе. Если вирус уже перешел в активную фазу, то его отлавливают по нестандартному поведению в системе. Вот здесь как раз и заключается самый актуальный на сегодняшний день вопрос – поиск аномалий в контенте системы, в том числе и в больших данных. Это огромный пласт, здесь можно применять новые идеи и разработки, включая различные методы машинного обучения. Задача заключается в том, чтобы выявить аномалии в сети, определить их причину (имеет ли место нарушение ИБ) и дальше при наличии ВПО принять меры к его локализации и уничтожению. Сейчас на рынке имеются современные и эффективные решения, достаточно успешно решающие эти задачи. Они позволили предотвратить и последние вирусные атаки, которые натворили немало бед.

В. КОНТОРОВИЧ (Сбербанк): Мы затронули одну из наиболее проблемных и актуальных тем – защиту клиентов от социальной инженерии. В связи с этим хотел бы выступить, что называется, адвокатом бренда нашего банка, потому что Сбербанк уже давно и плотно занимается этим вопросом. У нас создана высокотехнологичная система фрод-мониторинга, которая постоянно совершенствуется и технически, и организационно. Но на 100% защитить клиентов от последствий воздействия социальных инженеров, насколько мне известно, пока не получается ни у кого. Поэтому руководство банка приняло решение разработать специальные продукты для защиты от мошенников клиентов, которые не в состоянии обеспечить на своей стороне защиту аутентификационных данных для удаленного доступа к своим счетам. Эти продукты предполагают работу с клиентскими счетами, включая использование хорошо известных с давних времен сберкнижек, только при личном присутствии клиента в банковском офисе. Об этом сообщил заместитель председателя правления Сбербанка Станислав Константинович Кузнецов во время Всемирного фестиваля молодежи и студентов в Сочи в октябре этого года.

М. ЛЕВАШОВ (Банк «ФК Открытие»): Я тоже являюсь клиентом Сбербанка и хочу поддержать некоторые тезисы выступления представителя этой финансово-кредитной организации. Недавно, участвуя в качестве эксперта в курируемом Сбербанком кластере ИБ программы цифровой экономики, я общался со специалистами этого банка, занимающимися вопросам кибербезопасности. Сбербанк действительно внедряет в этой области передовые идеи и технологии, которые позволяют добиться хороших результатов.

А. ВИНОГРАДОВ (Златкомбанк): Фактически мы плавно переходим с вами к теме кибербезопасности в условиях цифровой экономики.

К. КЕРЦЕНБАУМ (Group-IB): В банковской среде вопрос дальнейшей победы

Михаил ЛЕВАШОВ,
советник Банка «ФК Открытие»

«цифры» над аналогом – это развитие цифровых услуг, перевод своего бизнеса в цифровой офис. На рынке уже есть примеры, демонстрирующие жизнеспособность этой стратегии. Все стремятся к сокращению издержек, при этом многие бизнес-процессы ускоряются, привлечение клиентов становится более простым. Некоторые пенсионеры уже активно пользуются онлайн-банками, а что касается молодежи, то ее уже давно не загнать в рамки банковского офиса. Для многих финансово-кредитные организации ассоциируются с отживающими свое бюрократическими структурами.

Лично я являюсь клиентом нескольких банков, и одним из главных критериев выбора обслуживающей организации для меня является система ДБО. Конечно, и безопасность тоже, но в первую очередь удобство. В одном западном банке, который представлен в России, я сокращаю количество получаемых услуг, потому что ДБО там не развивается и цифровых сервисов, предоставляемых клиентам, до сих пор очень мало. Российские же банки, напротив, увеличивают количество услуг, оказываемых через интернет, и становятся благодаря этому более привлекательными. Естественно, цифровизация

ведет к увеличению рисков, но в этом вопросе нужно видеть и другую сторону медали. Благодаря большей клиентоориентированности банки получают дополнительную прибыль, и они могут позволить себе инвестировать часть из полученных таким образом средств в информационную безопасность.

Еще один момент, который я хотел бы подчеркнуть: есть убеждение, что активные ретейл-банки с наиболее развитой цифровой составляющей чаще становятся объектами хакерских атак, чем их менее цифровизированные «коллеги по цеху». Но статистика говорит об обратном. Когда мы сокращаем штат операционистов, которых невозможно обучить правилам информационной безопасности на должном уровне, то мы таким образом сокращаем и риски, возникающие в силу человеческого фактора. Поэтому с учетом всего вышесказанного я позволю себе сформулировать следующий вывод. Цифровизация – это не вызов, а путь к сокращению рисков банка. Конечно, при одном обязательном условии – правильно организованной и поставленной работе с новыми рисками.

А. СВИРИДЕНКО (Интерпрогрессбанк): Я бы не сказал, что количество рисков в результате цифровизации будет уменьшаться. Когда бизнес придумывает новую идею, вопросы безопасности не являются приоритетными, и тема информационной защиты в этом случае однозначно отходит куда-то на второй или третий план. Главное – получить прибыль! И если она перекрыла потери и затраты, значит, все в порядке. Так что, честно говоря, весь «поход в цифру» оборачивается для сотрудников информационной безопасности дополнительной головной болью и попыткой пристроить механизмы защиты на уже набирающем обороты процессе. Многие сервисы в эпоху цифровизации, рекламируя свою скорость и доступность, особо не учитывают риски безопасности со стороны граждан. А если говорить о поколении «миллениум», то открытость жизни для них является нормой. Отправить фотографию паспорта для получения сервиса, оставить полные данные в обмен на скидочную карту (особенно если это бесплатно и предусмотрен бонус) – все это молодежь делает легко и не задумываясь о последствиях. И хочется надеяться, что последствия пренебрежения своей безопасностью не приведут для них к катастрофическим последствиям.

NBJ: Поскольку здесь речь зашла о клиентах и о соблюдении или, точнее, несоблюдении ими правил информационной безопасности, то позволим себе тоже встать на защиту клиентов, поскольку, как легко догадаться, являемся ими. Все начинается с того, как человека принимают в банке. Расхожая ситуация: мы в качестве клиента приходим в офис, и что нам говорит менеджер? Ура, вы пришли! Вот вам карта, к ней привязан вклад, вы с ней можете совершать разные операции. После непродолжительного разговора с банковским менеджером начинаешь чувствовать себя Золушкой во время встречи с доброй феей. Фея, как и положено, отправляет тебя на бал, снабжая при этом платьем, хрустальными туфельками, диадемой и попутно рассказывая тебе о твоих сияющих перспективах. О рисках утраты платья, туфелек и перспектив упоминается, как говорится, «во вторых строках», и, конечно же, ни Золушка, ни обрадованный клиент не обращают на подобные предостережения ни малейшего внимания. Потом, как известно, бьет 12-й час, и реализуются риски. На мой взгляд, при такой системе обслуживания бессмысленно упрекать клиента в том, что он чего-то не дослушал и не досмотрел. Ему, по сути, в банках ничего не объясняют и ни о чем всерьез не предостерегают. Максимум, возможно, в его договоре будет на нескольких строках прописано «а вот если ты будешь «разбрасывать» свой пароль и логин где попало...», но этого явно недостаточно.

Владислав КОНТОРОВИЧ,
управляющий директор блока «Технологии» Сбербанка РФ и ПАО Сбербанк

А. ВИЛЬДМАН (МТИ-Банк): Я подскажу и вам, и другим клиентам, как с этим бороться: верить никому вообще нельзя, если вам что-то предлагают, все нужно перепроверять.

А. СВИРИДЕНКО (Интерпрогрессбанк): Мы преимущественно люди взрослые, поэтому сами способны понять и оценить верность вашего тезиса. А что делать новому поколению? Оно публикует в соцсетях о себе все – данные, фотографии, геолокацию. Из человека таким образом можно вытащить полностью всю информацию, и нет ни малейших сомнений в том, что злоумышленники будут этим пользоваться и уже делают это.

А. ВИЛЬДМАН: Проблема в том, что нам надо соблюсти некую золотую середину между регулятором, который считает, что за любой инцидент информационной безопасности можно прижать банк к ногтю и серьезно наказать финансово-кредитную организацию, и этим самым поколением, которое не привыкло выполнять даже минимальные требования по защите информации, собственных средств, пластиковых карт и т.д. К сожалению, что бы

мы ни делали, банк все равно виноват. И мы это видим на практике. На сегодняшний день информационная безопасность – это третий способ вывода банков с рынка наряду с претензиями к качеству кредитов и, следовательно, к величине капитала, и 115-ФЗ. Количество бумаг, которые должен писать банк по ИБ, наверное, уже превышает количество документации у рисковиков. Небольшие региональные банки не могут себе позволить держать необходимых специалистов в штате.

М. ЛЕВАШОВ (Банк «ФК Открытие»): Есть аутсорсинг, поэтому не нужно держать специалистов в штате. Надо использовать профессиональные компании, которые могут предоставить практически любые услуги в области обеспечения ИБ. Необходимо использовать такие возможности.

А. ВИЛЬДМАН (МТИ-Банк): Поэтому мы и будем обсуждать стандарт по аутсорсингу. А вот вопрос об аудите систем информационной безопасности является куда более проблематичным. Все понимают, что он нужен и полезен, но официальных требований к аудитору нет. Предположим, они появятся, но еще большой вопрос, какими они будут. Представим себе следующую ситуацию: в договоре между аудитором и банком прописано, что в случае, если проверка Центрального банка после успешного аудита обнаружит недостатки и это повлечет за собой определенные последствия, аудитор должен будет их ликвидировать. Возникает вопрос: какой аудитор сможет оплатить потерю банком лицензии?

М. ЛЕВАШОВ (Банк «ФК Открытие»): Это крайний случай, фантастический!

А. ВИЛЬДМАН (МТИ-Банк): Поэтому я и говорю, что так или иначе крайним всегда будет банк. В целом же, если отвлечься от этой темы, то следует признать, что аудит возможен двух видов. Первый – это когда приглашается профессиональная компания, которая обладает рыночным опытом.

Алексей ТИМОШКИН,
начальник отдела ИБ НС Банка, заместитель руководителя службы финансового мониторинга ВТБ 24

Конечно, ценник у нее будет соответствующим, но по крайней мере по итогам аудита банк получит полезные рекомендации и адекватные решения имеющихся проблем. Второй вид – ты будешь пользоваться тем, что дешевле, и тогда есть вероятность, что к тебе придут три студента и подпишут акт, что у тебя все хорошо, получив за это три копейки. Потом придет проверка из ЦБ РФ, и дальше все понятно.

А. ВИНОГРАДОВ: Давайте перейдем к следующей теме, которая звучит так – развитие вымогательского программного обеспечения и масштабные кибератаки с использованием шифровальщиков, технические особенности атак вымогателей.

М. ЛЕВАШОВ (Банк «ФК Открытие»): Действительно, появление вирусов-шифровальщиков – это опасный тренд. Из общих отчетов компаний, которые занимаются этой проблематикой, следует, что вымогатели, беря деньги, ничего не расшифровывают. Нужно осуществлять резервное копирование информации. Если у банков построена современная эшелонированная система защиты, то такие шифровальщики не проходят. Система защиты не дает им ничего сделать.

А. СВИРИДЕНКО (Интерпрогрессбанк): Если брать первый шифровальщик – WannaCry, то он опирался на уязвимость, которую не закрывали длительное время. То есть это был первый звонок. Те, кто понял угрозу, к моменту нападения второго вируса-шифровальщика были уже готовы. Ситуацию для банков улучшило то, что первая атака шла не на них, и у финансово-кредитных организаций было время подготовиться. Естественно, что многое зависело от того, как кто реагировал на угрозу. Те, кто ее проигнорировал, попались во время «второй волны». В третий раз Bad Rabbit не затронул банковскую сферу, но при этом возникла негативная тенденция: если при первой и второй атаке эксплуатация старых уязвимостей была где-то двухмесячной давности, то последняя уязвимость в ноябре была буквально недельной давности. Атака прошла буквально через неделю после публикации уязвимостей, то есть времени на устранение обнаруженного «узкого места» было совсем мало.

К. КЕРЦЕНБАУМ (Group-IB): Я считаю, что череда шифровальщиков WannaCry, NotPetya и Bad Rabbit многому нас научила. Вопросы информационной безопасности вышли на другой уровень. Важно понимать, что шифровальщиков уже десятки тысяч. В антивирусных сигнатурах всех вендоров их очень много, они направлены в основном на консьюмеров, то есть на частников. Все три нашумевших вируса ничего не расшифровывали. Либо механизм, предназначенный для шифровки, был сломан, либо он изначально не закладывался. WannaCry, NotPetya, Bad Rabbit были направлены на наш регион – Россия, СНГ, Восточная Европа, при этом за ними стояли совершенно разные группировки. Если за WannaCry предположительно несла ответственность Северная Корея, то NotPetya и Bad Rabbit – это, скорее всего, дело рук русскоязычных

хакеров. И мы понимаем, что шифровальщики становятся также инструментом политического принуждения к определенным действиям и инструментом запугивания оппонентов или конкурентов. Это плохая тенденция.

А. ВИНОГРАДОВ (Златкомбанк): Давайте перейдем к вопросу о решениях по предотвращению утечек информации – DLP.

М. ЛЕВАШОВ (Банк «ФК Открытие»): 100% – это вещь недостижимая. Сейчас актуальность темы предотвращения утечек данных резко снизилась, и причина этого очевидна, ведь сначала надо ответить на вопрос, с кем бороться, а потом уже как это делать. Итак, с кем мы боремся? Если с высококвалифицированными ИТ-специалистами, имеющими большие права и полномочия, то это бесполезно. Они все равно вынесут все, что захотят. А с обычным пользователем справится любая DLP-система. Я не помню, чтобы на рынках продавались банковские базы данных. Там ранее появлялись только базы данных некоторых мобильных операторов.

К. КЕРЦЕНБАУМ (Group-IB): Хочу добавить по поводу DLP. Я работал в области ИБ, когда DLP еще было модно. Помните, была старая реклама, когда сын спрашивает отца: «Папа, а инопланетяне существуют?», а тот говорит: «Нет, сынок, это фантастика». То же самое можно сказать и про DLP. Эффективных систем DLP не существует, потому что ни один вендор не гарантирует вам защиту на 100% от утечек. Но в чем разница между DLP и классической ИБ? Когда у вас стоит антивирус на почте, на веб-шлюзе и т.д., все они не закрывают риски на 100 %, и мы это знаем. Если разные вендоры, зона перекрытия в зависимости от того, чьи решения вы выбрали, чуть увеличивается, но все равно остается процент пропуска. Что мы делаем? Эшелонирование. А с DLP что делать? Есть средство контроля утечек, а его вам закрыть нечем.

Екатерина КАЛИНИНА (SWIFT),
директор по развитию бизнеса Россия, СНГ и Монголия SWIFT

На мой взгляд как человека, который восемь лет назад занимался продвижением DLP, сейчас это эффективно только для двух отраслей – хайтек и научные разработки. В других отраслях DLP не дает нужной защиты. Что мы будем защищать, если вся информация есть в Facebook и других социальных сетях? Если есть такое явление, как дата-брокеры, у которых любая компания может купить информацию. В эпоху публичности эффективность DLP стремится к нулю.

А. ТИМОШКИН (ВТБ 24): Я бы предложил взглянуть на проблему с другой стороны. Все инциденты в информационной безопасности – атаки, «вредоносы», утечки персональных данных – это не абстрактные вещи, и все они делаются с какой-то целью. Как правило, она всегда одна и та же – украсть деньги. Кто в банках встречает эту угрозу, кто выступает в роли «пограничников»? Это подразделение ИБ, отдел по антифроду и финансовому мониторингу, в самой худшей ситуации юристы. Зачастую бывает так. Служба безопасности выявила атаку, украли деньги (одно юрлицо похитило деньги у другого), собираются вывести похищенное на счета в другом банке. При этом отдел финансового мониторинга говорит, что данная проблема вне зоны его компетенции, и он прав, потому что в 115-ФЗ нет конкретики для таких видов преступлений. Получается, что подобные прецеденты наши аналитические системы не ловят, потому что со стороны это выглядит как перевод средств от одного юрлица другому. Здесь проявляется некая внутренняя несогласованность, потому что все эти подразделения наблюдают один и тот же процесс, но с разных сторон. У всех локальный взгляд, все ограничены корпоративными стенами.

Это одна проблема. Вторая заключается в том, что мы стоим на пороге взрывообразного роста новых технологий (блокчейн, новые виды идентификации – биометрия и т.д.). Многие банки с интересом наблюдают за этими технологиями, которые, конечно же, несут с собой в случае своего использования много положительного, но и риски. И здесь тоже возникает проблема межпрофессиональных коммуникаций, которые зачастую отсутствуют. Я предлагаю найти точки соприкосновения, механизмы взаимодействия, чтобы с разных позиций можно было взглянуть на одну проблему.

А. ВИЛЬДМАН (МТИ-Банк): Что касается сотрудничества информбезопасности, комплаенса и т.д., то здесь все упирается в законодательство и регулирование, потому что большинство банков имеют у себя за спиной большое количество предотвращенных попыток хищений. При этом часто банки располагают абсолютно конкретными сведениями о получателе похищенных денег, они точно знают, что деньги пройдут через тех или иных физических или юридических лиц. Было бы очень хорошо, если бы регулятор дал нам возможность этими данными обмениваться, пусть не в целях запрета совершения операций с подобными счетами, а хотя бы для сведения.

Е. КАЛИНИНА (SWIFT): Тема сегодняшней встречи – информационная безопасность, для нас в SWIFT

Павел ПРОКУДИН (SWIFT),
директор по развитию бизнеса банковский сектор Россия, СНГ и Монголия, SWIFT

это приоритетная тема. Я уверена, что аудитория знакома с программой безопасности пользователей, которую SWIFT начал в 2016 году после кейса с Национальным банком Бангладеша. Сейчас SWIFT проводит аттестацию по этой программе, и каждый пользователь системы должен получить аттестацию по требованиям безопасности до конца 2017 года. В 2018 году нужно будет привести свои меры безопасности в соответствие с тем стандартом, который разработал SWIFT. Мы видим, что еще не все банки активно включились в этот процесс. По тем откликам, которые мы получаем от индустрии, это очень полезный инструмент, и мы рассчитываем на то, что те банки, которые прошли аттестацию или находятся в стадии ее завершения, будут продвигать требования стандарта среди своих контрагентов, потому что эта инициатива направлена на повышение уровня безопасности индустрии в целом.

А. ВИНОГРАДОВ (Златкомбанк): Планируете ли вы подписание с Центральным банком каких-либо договорных соглашений? Я знаю, что SWIFT не имеет отношения к 161-ФЗ, вы не оператор платежной системы, вы оператор информационных систем. И многие не понимают, на основании чего они должны проводить самоаттестацию на соответствие требованиям вашего стандарта.

Е. КАЛИНИНА (SWIFT): Нам тоже такие вопросы задают. Действительно, данное требование не закреплено в каком-то нормативном акте, и мы взаимодействуем с Банком России, в том числе и по данной теме. Я не знаю, захотят ли там какие-то положения из нашей программы имплементировать в свои требования по ИБ. Но я могу сказать, что у нас есть взаимопонимание и поддержка друг друга в этом направлении. Банк России заинтересован в статусе самоаттестации, сотрудники ЦБ РФ уже запрашивали у нас информацию о том, кто уже провел ее, а кто еще не приступал к этой работе. В начале 2018 года мы подведем итог по первому этапу самоаттестации, подадим в ЦБ РФ список тех, кто ее выполнил. Я соглашусь, что нормативным актом это не установлено, но мы исходим из того, что эта инициатива – в интересах всего сообщества, это правильные, логичные, своевременные шаги.

А. ВИНОГРАДОВ (Златкомбанк): Если бы можно было на полгода оттянуть дедлайн прохождения самоаттестации, то было бы вообще идеально.

Е. КАЛИНИНА (SWIFT): Мы пытались достичь какого-то баланса в этом вопросе, и поэтому – и я хочу особо это подчеркнуть – мы не требуем полного и немедленного соответствия нашему стандарту. Мы настаиваем на том, чтобы банки, которые являются участниками нашей системы, провели аттестацию, сами для себя осмыслили, где они находятся с точки зрения ИБ.

П. ПРОКУДИН (SWIFT): Позволю себе один небольшой комментарий или, скорее, дополнение к тому, что было сказано Екатериной (Калининой – *Прим. ред.*) Во-первых, вопрос взаимодействия с комплаенс и службой информационной безопасности. Мы много встречаемся с банками и в России, и в других странах. Мы слышим от крупных (глобальных) расчетных банков, что они уже ввели в свои комплаенс-процедуры оценку корреспондентов по критериям безопасности SWIFT. KYC Registry Security Attestation – это та платформа, на которой сейчас должна проводиться самоаттестация и самооценка, через нее банки могут давать друг другу доступ к своему профайлу, чтобы видеть, насколько твой контрагент соответствует требованию SWIFT по безопасности. И западные банки, помимо сбора общих документов, уже ввели оценку по безопасности. В настоящее время использование сервиса локальной аутентификации, или Local Authentication (LAU), является рекомендуемой опцией в рамках требований Customer Security Program SWIFT, но в обозримом будущем станет обязательной. Для использования LAU данная опция должна быть активирована на стороне интерфейса SWIFT (уже имеется у всех пользователей и не требует никаких дополнительных затрат), при этом она также должна быть реализована на стороне автоматизированной банковской системы и других банковских систем, взаимодействующих с интерфейсом SWIFT. К сожалению, в настоящее время еще далеко не все вендоры банковского ПО поддерживают LAU в своих системах, в связи с чем мы рекомендуем уточнять у них возможность использования данной опции.

NBJ: Коллеги, большое спасибо всем, кто принял участие в нашем круглом столе. Очевидно, что мы не можем в течение ограниченного времени обсудить весь спектр вопросов по ИБ, но также очевидно и то, что такие круглые столы стали хорошей площадкой для обмена мнениями и опытом. Поэтому мы уверены, что скоро встретимся вновь, и будем надеяться на то, что нам придется обсуждать не столько успешные атаки злоумышленников, сколько эффективные методы и инструменты борьбы с ними. NBJ