Тема № 9 «Обеспечение информационной безопасности участников финансового рынка»

1. Наиболее опасные угрозы информационной безопасности.
2. Риски информационной безопасности финансового рынка.
3. Политика ЦБ в сфере защиты информации.

1. Наиболее опасные угрозы информационной безопасности.

Угрозы информационной безопасности, характерные для финансовых систем

На Всемирном экономическом форуме по глобальным рискам 2018 года кибератаки признали составной частью единого базового глобального технологического риска.

Выявлен мировой тренд, в котором компьютерные нападения на финансовую систему преследуют две цели:

- увеличение денежных потерь экономики в целом;
- нарушение целостности и непрерывности функционирования банковской системы.

Атаки на банковский сектор составляют 17 % от всего объема хакерских атак в мире. Характер хакерских атак на российские банки за последний год изменился. Основным риском признается несанкционированная операция по переводу денежных средств или списание средств с карты или счета клиента. Причинами такой операции могут быть действия хакеров или инсайдеров. По данным ФинЦЕРТ, в 2018 году объем средств, незаконно списанных со счетов юридических лиц, составил 1,469 миллиарда рублей. Но в сравнении с тем, что в 2015 году эта цифра составляла 3,7 миллиарда, можно говорить о существенном улучшении ситуации с информационной безопасностью в банковской системе. Для сравнения: количество денежных средств, потерянных клиентами банков в результате несанкционированных списаний с банковских карт, в 2018 году составило 1,384 миллиарда рублей, а в 2015-м – 1,14 миллиарда рублей.

Такую диспропорцию, когда при усилении мер безопасности объемы списания со счетов компаний уменьшаются, а со счетов граждан увеличиваются, можно объяснить двумя причинами:

- общим увеличением числа банковских карт;
- недостаточной экономической грамотностью населения.

Но более опасны системные сбои в работе банковской организации, способные затормозить или остановить экономическую деятельность клиентов на неопределенное время. Ключевыми рисками информационной безопасности, требующими внимания и устранения, в этой ситуации становятся:

- потери клиентов кредитных организаций (в том числе граждан, разово пользующихся банковскими услугами, например, банкоматом или системой переводов), подрывающие доверие к финансовой системе в целом, современным информационным технологиям и государству как регулятору;
- потери участников банковско-кредитного рынка как в части собственных средств, так и в части средств клиентов, способные негативно повлиять на их устойчивость и привести к банкротству;
- нарушение непрерывности операционного цикла оказания банковских услуг, что наносит ущерб репутации участников рынка и создает социальное напряжение в обществе. Социальная напряженность вызывается минимальным сбоем в работе банкоматов или систем онлайн-банкинга;
- системный кризис в отдельных секторах банковского рынка, спровоцированный систематическими и массированными кибератаками.

Для понимания, является ли вмешательство хакеров в операционную деятельность банковской организации проблемным, OSCO (международной организацией – регулятором денежных рынков) выработала критерии надлежащего функционирования системы:

- возможность восстановить операционную деятельность и осуществлять финансовые трансакции уже через два часа после инцидента информационной безопасности, нарушившего работоспособность системы;

- любой платеж должен быть осуществлен по наступлении определенного срока его завершения, например, платежное поручение исполняется банком не позднее следующего дня, а платеж по кредиту должен быть зачислен в оговоренные в договоре сроки, их нарушение по вине банка грозит убытками для клиента, возместить которые должен банк.

Если информационная система кредитной организации соответствует этим требованиям, значит, она надежна. Банки обязаны заботиться об информационной безопасности больше, чем обычные организации, так как они рискуют не только своими активами, но и средствами клиентов. Это порождает необходимость дополнительного регулирования соблюдения требований информационной безопасности в банковской и финансовой системе со стороны государства.

Кроме средств клиентов и банков, хакеров могут интересовать:

- персональные данные;
- программные коды и алгоритмы работы банковских продуктов;
- конфиденциальная информация, связанная с планами, стратегией, политикой кредитной организации.

Защита этих массивов информации осуществляется в соответствии с требованиями регуляторов (ФСТЭК, ФСБ, ЦБ РФ) и по собственным технологиям финансовой организации.

Типы массовых атак на компании банковско-кредитного сектора мало отличаются от атак на компании, работающие в других секторах экономики, это:

- DDoS-атаки (им подвергается каждое четвертое учреждение кредитно-финансовой сферы);
- фишинг (21 %);
- взлом систем (17 %);
- 20 % – инциденты прочего характера.

АБС (автоматизированные банковские системы) защищены в достаточной степени, наибольший объем атак приходится на клиентские

мобильные приложения. Часто хакеры используют такие приложения для внедрения вредоносного ПО – шифровальщиков, кодирующих данные на мобильном устройстве и предлагающих раскодировать их за выкуп. Сообщается, что приложения мобильного банкинга 50 из 100 крупнейших мировых банков содержат уязвимости, страдают ими и другие front-end-системы, предлагающие мобильный банкинг для предприятий. В последние годы крупнейшие финансовые организации внедряют в систему «Клиент-Банк» фрод-модули, но риск несанкционированных трансакций в полной мере пока не снят.

Помимо классических хакерских атак, в последние годы для финансовых организаций возник новый тип рисков. Банковские бизнес-процессы уязвимы, и опытные мошенники могут перенастроить информационную систему таким образом, чтобы изменить течение процесса и сконцентрировать основную прибыль у себя. Business Process Compromise (BPC), так называется этот вид мошенничества, в банковском бизнесе чаще всего выражается в подложных поручениях на перевод средств. Ущерб от этого вида мошенничества по миру уже превысил несколько миллиардов долларов. Например, у Банка Бангладеша таким образом было похищено около 80 миллионов долларов.

2. Риски информационной безопасности финансового рынка.

РИСКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

При подготовке этого документа мы исходили из очевидной необходимости минимизировать те риски, которые наряду с многочисленными преимуществами создает цифровая трансформация.

В кредитно-финансовой сфере к ним относятся:

- финансовые потери клиентов и финансовых организаций;
- нарушение операционной надежности и непрерывности работы финансовых организаций, и как следствие — репутационный ущерб и социальная напряженность;

- развитие системного кризиса вследствие кибератак в значимых для рынка организациях.

В этой связи стоит сказать о том, что повышает значимость информационной безопасности финансового рынка Российской Федерации.

Во-первых, это скорость развития новых финансовых технологий, в том числе, обусловленная активной поддержкой создания цифровой экосистемы руководством страны.

Во-вторых, необходимость защиты потребителей финансовых услуг от потерь и, как следствие, поддержания доверия к финансовой системе России.

В-третьих — задача по интеграции показателей киберрисков в состав основных рисков финансовых организаций.

С УЧЕТОМ ТРЕНДОВ

Развитие цифровой среды — это непрерывное появление и внедрение новых цифровых технологий. Это как многочисленные прорывные разработки финтех-стартапов, так и крупные инфраструктурные цифровые проекты. В отношении некоторых из них Банк России уже устанавливает требования по информационной безопасности. Это единая биометрическая система, система быстрых платежей и платформа Маркетплейс.

В будущем требования к киберустойчивости финансовой экосистемы мы будем формулировать с учетом глобальных трендов развития финтеха. В первую очередь, таких как использование технологий распределенного реестра, развитие удаленного доступа, BigData, искусственного интеллекта и «Интернета вещей» как элемента платежного пространства.

ЗАДАЧИ СЕГОДНЯ

Однако это нам пока только предстоит. Вернемся в сегодняшний день, когда нашей приоритетной задачей является реализация информационной безопасности финансовых организаций на следующих уровнях:

- безопасность инфраструктуры, или инфраструктурный уровень;
- безопасность прикладного программного обеспечения, или уровень приложений;

- безопасность технологий обработки данных, или уровень технологий обработки данных;
- а также протоколирование действий и операций (транзакций).

НОРМАТИВНАЯ БАЗА

Практическую реализацию стратегии мы начали в прошлом году с разработки необходимой нормативной базы.

Мы исходили из того, что правовой механизм обеспечения информационной безопасности на финансовом рынке должен гарантировать предсказуемость реализации Банком России своих полномочий, предсказуемость надзора за исполнением требований участниками финансового рынка и в конечном итоге обеспечивать выполнение ключевого показателя эффективности обеспечения информационной безопасности в финансовой сфере. Напомню, им является доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, не превышающая 0,005 %

Могу сказать, что Банк России провел беспрецедентную по своему масштабу работу по нормативному закреплению полномочий и механизмов противодействия информационным угрозам в кредитно-финансовой сфере.

Начиная с 2016 года сотрудники Банка России участвовали в разработке принятого в 2018 году Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» (далее — Федеральный закон № 167-ФЗ). В дальнейшем в дополнение к нему был издан ряд конкретизирующих и уточняющих нормативных актов. Указанные документы позволили:

- создать механизм противодействия переводам денежных средств без согласия клиента, предусматривающий как обязательные требования к защите информации, формируемой кредитными организациями, так и процедуры управления рисками, разрабатываемые кредитными организациями на основе анализа характера, параметров и объема

совершаемых их клиентами операций (осуществляемой клиентами деятельности);

- организовать информационное взаимодействие кредитных организаций с Банком России по обмену информацией об инцидентах защиты информации, о случаях и попытках осуществления переводов денежных средств без согласия клиента, включая формирование и ведение Банком России базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента;
- обеспечить реализацию кредитными организациями в целях противодействия осуществлению переводов денежных средств без согласия клиента в рамках осуществляемой ими банковской деятельности, некредитными финансовыми организациями в целях противодействия незаконным финансовым операциям в рамках осуществляемой ими деятельности в сфере финансовых рынков уровня защиты информации, соответствующего потенциальным угрозам безопасности с учетом пропорционального метода регулирования.

Помимо этого, Банком России в течении 2016–2018 гг. были изданы следующие нормативные акты:

Указание № 4793-У [1], устанавливающее требования к прикладному программному обеспечению (в части сертификации, анализа уязвимостей, ежегодного тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, применения раздельных технологий), к обеспечению защиты информации с помощью средств криптографической защиты информации, к порядку информирования Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;

Указание № 4753-У [2], которое устанавливает обязанность операторов по переводу денежных средств и операторов услуг платежной инфраструктуры по предоставлению в Банк России отчетности по форме

0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» (далее — отчетность по форме 0403203) на ежеквартальной и полугодовой [3] основе.

АСОИ

В целях противодействия осуществлению денежных переводов без согласия клиентов кредитных организаций, противодействия осуществлению незаконных финансовых операций Банк России ведет сбор и обработку поступающей от кредитных и некредитных финансовых организаций информации о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, а также о планируемых мероприятиях в отношении инцидентов защиты информации.

Информацию об угрозах информационной безопасности Банк России получает как от поднадзорных финансовых организаций, так и от компаний-интеграторов, разработчиков антивирусного программного обеспечения, иностранных финансовых организаций и регуляторов, групп реагирования на инциденты (в том числе иностранных), провайдеров и операторов связи, а также правоохранительных, иных государственных органов, наделенных полномочиями в области информационной безопасности.

Для упрощения процесса информационного обмена, а также повышения оперативности и уровня его защищенности используется автоматизированная система обработки инцидентов (далее - АСОИ), к которой в настоящий момент подключены все кредитные организации Российской Федерации. Также осуществляется подключение страховых организаций и иных участников информационного обмена. Всего к АСОИ подключено 826 организаций. Число участников информационного обмена из категории «некредитные финансовые организации» (НФО) по сравнению с периодом 2017–2018 гг. увеличилось более чем на 100 организаций. Также участниками информационного обмена стали более 20 вендоров защитных решений, разработчиков банковского программного обеспечения, операторов связи, провайдеров хостинга и иных заинтересованных организаций.

Взаимодействие с вышеуказанными организациями осуществляется на безвозмездной основе в соответствии с соглашениями о взаимодействии по вопросу предупреждения и противодействия компьютерным атакам (в 2018 г. заключено 21 такое соглашение). За период с сентября 2018 года по настоящее время количество активных участников информационного обмена, регулярно передающих информацию о выявленных угрозах и уязвимостях, увеличилось на 48 % (с 315 до 465). Данное обстоятельство связано в том числе с активной реализацией участниками информационного обмена стандарта Банка России СТО БР БФБО-1.5–2018.

Функционал АСОИ позволяет автоматизировать следующие процессы между участниками информационного обмена и Банком России:

- получение данных от участника (информация об инцидентах в организации, выявленных уязвимостях, угрозах, данных о раскрытии информации, запросах);
- передача участнику данных об актуальных угрозах информационной безопасности в кредитно-финансовой сфере (в том числе из 589 выпущенных Банком России бюллетеней);
- оперативное взаимодействие между участником и Банком России по инцидентам и запросам;
- мониторинг информационных атак на организации кредитно-финансовой сферы и поддержка взаимодействия Банка России с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов.

КПЭ

Доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, в 2019 г. составила 0,0023 % (в 2018 г. — 0,0018 %). Указанные значения не превышают установленный Банком России целевой показатель доли таких операций в общем объеме операций, совершенных с использованием платежных карт. Повторюсь, этот показатель установлен на уровне 0,005 %.

Наблюдаемое в отчетном периоде изменение нисходящей динамики 2015–2017 гг., а также качественно более высокие показатели операционной отчетности указывают на имевшую место реальную необходимость повышения прозрачности предоставляемых банками данных и подтверждают правильность разработки и внедрения мер по минимизации риска осуществления операций без согласия клиентов, принимаемых участниками рынка и Банком России, а также необходимость их дальнейшего развития.

ПРОВЕРКИ

Основой эффективной деятельности в сфере обеспечения информационной безопасности является применение подхода, основанного на оценке кибер-риска, или, другими словами, риск-ориентированный подход. Банк России планируют сформировать профиль риска, а также определять операционную надежность и киберустойчивость каждой поднадзорной организации на основе данных, которые мы получаем в ходе анализа поступаемой отчётности, сообщений участников информационного обмена об инцидентах, а также проверок соблюдения требований по информационной безопасности. В 2019 году мы провели порядка 170 таких проверок как в кредитных организациях, так и в некредитных финансовых организациях.

КИБЕРУЧЕНИЯ

По направлению киберучений осуществляются следующие мероприятия:

1. Формирование риск-ориентированного задания на киберучения на основе:

- информации об инцидентах, характерных для вида деятельности;
- информации об инцидентах, характерных для технологических участков;
- информации о проведенных ранее проверках/киберучениях в поднадзорной организации;
- информации об актуальных атаках.

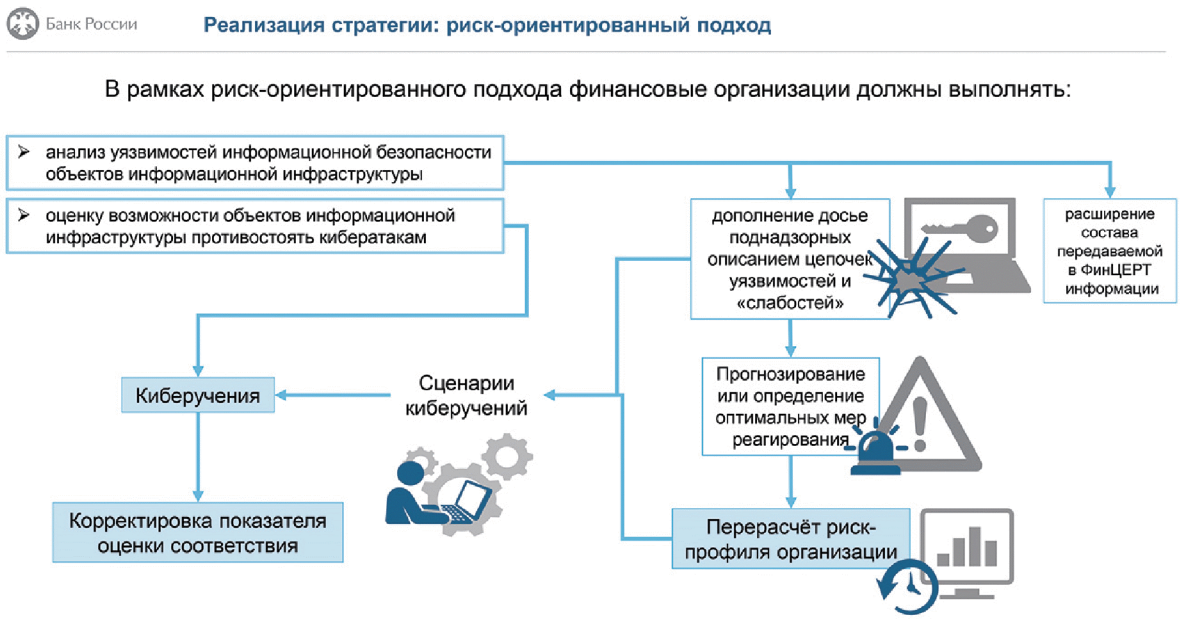
2. Проведение киберучений на площадке поднадзорной организации:

- анализ инфраструктуры, актуализация CPE;
- определение актуальных слабостей (CWE);
- определение актуальных атак (CAPEC);
- определение актуальных инцидентов;
- определение максимально возможных финансовых потерь.

3. Подготовка отчетного документа по результатам киберучений:

- корректировка показателя оценки соответствия;
- определение и применение мер воздействия[4];
- направление в профильные департаменты информации для учета показателей информационной безопасности при применении мер воздействия.

Организацией и проведением киберучений в рамках надзорных мероприятий занимается Департамент информационной безопасности Банка России.



В рамках управления киберрисками задачами каждой финансовой организации в первую очередь будут являться:

- обеспечение соответствия фактических потерь в результате инцидентов защиты информации допустимым потерям;
- формирование финансового резерва на покрытие потенциальных финансовых потерь либо страхования такого риска;

- своевременное восстановление непрерывности технологических и бизнес-процессов;
- и в целом защита интересов клиентов и соблюдение требований законодательства Российской Федерации в области защиты информации.

3. Политика ЦБ в сфере защиты информации

Полномочия ЦБ РФ как регулятора банковской деятельности, определяющего в том числе требования к информационной безопасности, установлены законом «О центральном банке». Ему предписано обеспечивать стабильность банковской и финансовой системы, и в этом качестве он вправе издавать документы, описывающие требования к информационной безопасности, обязательные для исполнения банками.

Центробанк издал основополагающее Постановление № 683-П от 17.04.19, устанавливающее обязательные требования к защите информации с целью исключения несанкционированных переводов.

Также за последние несколько лет в рамках усиления информационной безопасности в кредитной и финансовой сфере:

- приняты нормативные акты, согласно которым банки и финансовые организации обязаны уведомлять ЦБ РФ о выявленных инцидентах информационной безопасности;
- выпущены стандарты СТО БР БФБО-1.5-2018 об управлении инцидентами информационной безопасности и СТО БР ИББС-1.0-2014, освещающий общие вопросы информационной безопасности в финансовой и кредитной сферах;
- изданы разъяснения о порядке выполнения нормативных актов.

Это привело к заметному снижению числа инцидентов. ЦБ РФ устанавливает наиболее жесткие требования по информационной безопасности к следующим программным модулям:

- платформа удаленной идентификации в Единой биометрической системе (не в последнюю очередь из-за обработки биометрических персональных данных);
- системы быстрых платежей;
- платформы, обслуживающие маркетплейсы;
- цифровой профиль клиента.

Здесь требования регулятора могут быть жестче, чем соответствующие требования ФСТЭК РФ, связанные с защитой ПД.

В дальнейшем планируется доработать требования, связанные с:

- использованием Интернета вещей как новой угрозы;
- применением искусственного интеллекта и Big Data;
- применением технологии распределенных ресурсов и изменением архитектуры ИС.

ФинЦЕРТ

Существенную долю ответственности за обеспечение безопасности в банковской сфере взял на себя Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). Организация существует более четырех лет, и за этот период ей удалось систематизировать накопленный опыт в сфере информационной безопасности и снизить частоту нападений на банки и средний размер ущерба, причиняемого одной хакерской атакой. ФинЦЕРТ разработал собственную автоматизированную систему обработки информационных инцидентов. Подключиться к системе ФинЦЕРТ могут банки и небанковские кредитные организации.

ФинЦЕРТ вправе проводить проверки соблюдения требований информационной безопасности в банковской сфере. Во время 122 проверок, проведенных в 2019 году, выявлено около 700 нарушений требований, которые привели или могли привести к риску возникновения компьютерного инцидента и хищения денег клиентов.

Особенности систем информационной безопасности в банках

Большинство банков самостоятельно разрабатывают программное обеспечение – от общих систем до мобильных приложений. ЦБ РФ внес инициативу обязательной сертификации всех программ и обновлений, но она встретила сопротивление в финансовом сообществе. Банки отметили, что иногда обновление должно быть сделано в течение 1-2 недель после выявления ошибок в приложении, а сертификация замедлит его выход на рынок на месяцы. Сейчас в практической деятельности банков с целью предотвращения хищения средств клиентов при помощи компьютерных технологий используются следующие программные и технические средства осуществления информационной безопасности:

- программные средства защиты от внутреннего и внешнего фрода или мошенничества в сфере электронной коммерции;
- системы многофакторной аутентификации клиентов при онлайн-пользовании услугами банка;
- системы мониторинга информационных сетей и удаленных устройств, способных выявлять и реагировать на инциденты информационной безопасности;
- средства защиты банкоматов, исключающие несанкционированный доступ на физическом или информационном уровнях.

Стандартные программные средства защиты, предписанные регуляторами, ЦБ РФ, ФСТЭК, ФСБ, выбираются согласно классу системы, в которой обрабатываются персональные данные клиентов. Они обеспечивают уровень защиты информации, предписанный регулятором, но, если банк предполагает наличие риска целевых атак, защита должна быть усилена.

Пока в России не было хакерских атак на банковскую систему настолько интенсивных, чтобы была нарушена ее нормальная жизнедеятельность. Но регулярные сбои в работе банкоматов и онлайн-приложений создают напряженность в обществе, что побуждает уделять еще большее внимание информационной безопасности в финансовых системах.