ОТЧЕТ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ ДЕПАРТАМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА РОССИИ

1.09.2018 – 31.08.2019

БАНК РОССИИ

ФИНЦЕРТ

СОДЕРЖАНИЕ

Материал подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка России.

Фото на обложке: Shutterstock/FOTODOM

107016, Москва, ул. Неглинная, 12
Официальный сайт Банка России: www.cbr.ru

Список сокращений

АБС	Автоматизированная банковская система
АСОИ ФинЦЕРТ	Автоматизированная система обработки инцидентов ФинЦЕРТ
АС «Фид-АнтиФрод»	Автоматизированная система «Фид-АнтиФрод»
БПО	Банковское программное обеспечение
ВПО	Вредоносное программное обеспечение
Мобильные устройства	Абонентские устройства мобильной связи, мобильные телефоны, смартфоны, коммуникаторы и другие устройства, используемые клиентами кредитных организаций при осуществлении переводов денежных средств
Несанкционированная операция	Несанкционированная операция по переводу денежных средств
ПО	Программное обеспечение
Положение Банка России № 242-П	Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»
Положение Банка России № 382-П	Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
Положение Банка России № 471-П	Положение Банка России от 3 июня 2015 г. № 471-П «О порядке создания, ведения и хранения баз данных, содержащих информацию об имуществе, обязательствах негосударственного пенсионного фонда и их движении, а также случаях передачи на хранение в Банк России резервных копий баз данных»
Положение Банка России № 552-П	Положение Банка России от 24 августа 2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России» (утратило силу в связи с изданием Положения Банка России № 672-П)
Положение Банка России № 672-П	Положение Банка России от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России»
Положение Банка России № 683-П	Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
Положение Банка России № 684-П	Положение Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»
СКЗИ	Средство криптографической защиты информации
Стандарт Банка России СТО БР БФБО-1.5-2018	Стандарт Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации»
Стандарт Банка России СТО БР ИББС-1.0-2014	Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
Указание Банка России № 2831-У	Указание Банка России от 9 июня 2012 г. № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»

Указание Банка России № 4926-У	Указание Банка России от 8 октября 2018 г. № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»
Указание Банка России № 5039-У	Указание Банка России от 25 декабря 2018 г. № 5039-У «О формах и порядке направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств»
Федеральный закон № 161-ФЗ	Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»
Федеральный закон № 167-ФЗ	Федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств»
Федеральный закон № 187-ФЗ	Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Федеральный закон № 325-ФЗ	Федеральный закон от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»
Федеральный закон № 395-1	Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»
Фишинг	Адресуемая с использованием домена информационная система применяется для получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения этих лиц в заблуждение относительно ее принадлежности (подлинности) вследствие сходства доменных имен, оформления или содержания информации
ЭСП	Электронное средство платежа

ОБРАЩЕНИЕ ЗАМЕСТИТЕЛЯ ПРЕДСЕДАТЕЛЯ БАНКА РОССИИ Д.Г. СКОБЕЛКИНА

Уважаемые коллеги!

С момента начала работы ФинЦЕРТ прошло четыре года. За это время ФинЦЕРТ стал свидетелем и непосредственным участником множества событий, повлиявших на развитие информационной безопасности финансовой сферы. Наблюдавшиеся несколько лет назад высокий уровень объема хищений и слабая динамика снижения числа атак на банки и их клиентов обусловили необходимость законодательных и организационно-технических изменений в регулировании и надзоре в сфере обеспечения защиты информации банков и иных финансовых организаций. ФинЦЕРТ был создан для реализации этих изменений.

С 2015 г. расширился функционал и укрепился кадровый состав подразделения, оборудована лаборатория компьютерной криминалистики, введена в работу автоматизированная система обработки инцидентов (АСОИ ФинЦЕРТ), позволившая сделать информационный обмен максимально оперативным. В прошедшем году ФинЦЕРТ получил статус управления в структуре вновь созданного Департамента информационной безопасности Банка России.

Наряду с организационными преобразованиями, менялась и нормативная составляющая. Вступили в силу законодательные акты, устанавливающие обязанность кредитных и некредитных финансовых организаций[1] уведомлять Банк России о выявленных инцидентах[2], выпущен стандарт Банка России, регулирующий безопасность финансовых (банковских) операций и управление инцидентами информационной безопасности[3], подготовлен ряд конкретизирующих их нормативных документов Банка России.

Совместная работа с банками начала приносить плоды. Повысилась прозрачность данных о хищениях, и наряду с этим возрос уровень доверия клиентов банков к используемым ими услугам с точки зрения их информационной безопасности. Хочу отметить, что таких результатов мы вряд ли смогли бы добиться без скоординированной работы Банка России и наших поднадзорных организаций.

При этом в результате проведенных в отчетном периоде 122 проверок кредитных и некредитных финансовых организаций ФинЦЕРТ выявил 694 нарушения федеральных законов Российской Федерации, нормативных и иных актов Банка России. Нарушения приводят к снижению эффективно-

---

[1] *Операторы платежных систем, операторы услуг платежной инфраструктуры и операторы по переводу денежных средств.*

[2] *Положение Банка России № 382-П.*

[3] *Стандарт Банка России СТО БР БФБО-1.5-2018.*

сти организации информационной безопасности и к потенциальной возможности реализации ряда угроз информационной безопасности.

Задача Банка России – не формально проверять выполнение требований по использованию средств защиты, а стремиться к обеспечению качественного контроля за рисками наших поднадзорных (как отдельных организаций, так и элементов экономических и финансовых экосистем), их готовности противостоять компьютерным атакам не только технически, но и финансово. Работа в этом направлении будет развиваться в соответствии с недавно одобренным Советом директоров Банка России основополагающим документом – Основными направлениями развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов.

Заместитель Председателя
Банка России **Д.Г. Скобелкин**

ОБЩАЯ ИНФОРМАЦИЯ

ОСНОВНЫЕ СОБЫТИЯ 2018–2019 ГОДОВ

Июль 2018	Банки начали подключаться к АСОИ ФинЦЕРТ
Сентябрь 2018	На базе АСОИ ФинЦЕРТ развернут функционал прототипа АС «Фид-АнтиФрод»
Октябрь 2018	АСОИ ФинЦЕРТ протестирована кредитными организациями, успешно прошла приемочные испытания и введена в постоянную эксплуатацию
Ноябрь 2018	Выпущен стандарт Банка России СТО БР БФБО-1.5-2018, определяющий формы и сроки взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации
Декабрь 2018	Опубликовано Указание Банка России от 8 октября 2018 г. № 4926-У, устанавливающее форму и порядок обмена информацией о случаях и (или) попытках осуществления переводов денежных средств без согласия клиента
Январь 2019	Начато подключение к АСОИ ФинЦЕРТ некредитных финансовых организаций
Март 2019	Опубликовано Положение Банка России от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России»
Май 2019	Опубликовано Положение Банка России от 17 апреля 2019 г. №683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». Опубликовано Положение Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

МЕЖДУНАРОДНАЯ И РОССИЙСКАЯ ОБСТАНОВКА

В Отчете Всемирного экономического форума по глобальным рискам 2018 г. кибератаки определены как разновидность базового глобального технологического риска.

В качестве мирового тренда отмечается увеличение финансовых потерь от кибератак, нарушение целостности и непрерывности функционирования в том числе финансового рынка (17% всего объема кибератак приходится на финансовый сектор). Изощренность методов, способов и средств совершения кибератак требует от регуляторов гибкости, оперативности, использования инновационных цифровых технологий и методов работы.

Соединенные Штаты Америки, Канада, Сингапур, Австралия, Малайзия, Новая Зеландия, Япония, Великобритания, Австрия – эти страны, в большей степени подготовленные к кибератакам, становятся наиболее привлекательными для потребителей финансовых услуг, что является фактором ускорения их экономического развития.

К ключевым рискам в кредитно-финансовой сфере относятся:

- финансовые потери клиентов (потребителей финансовых услуг), подрывающие доверие к современным финансовым технологиям;
- финансовые потери отдельных финансовых организаций, способные оказать существенное негативное (критическое) воздействие на их финансовое положение;
- нарушение операционной надежности и непрерывности предоставления финансовых услуг, приводящее к репутационному ущербу и нарастанию социальной напряженности в обществе;
- развитие системного кризиса в случае возникновения инцидентов информационной безопасности вследствие кибератак в значимых для финансового рынка организациях.

Международной организацией комиссий по ценным бумагам (IOSCO) установлены следующие критерии надлежащего функционирования значимой инфраструктуры финансового рынка:

- способность возобновить операции в течение двух часов после нарушения;
- обеспечение расчетов при наступлении срока погашения обязательств и завершенности транзакций.

В Российской Федерации, по данным ФинЦЕРТ, объем несанкционированных операций со счетов юридических лиц по итогам 2018 г. составил 1,469 млрд руб. (в 2017 г. – порядка 1,57 млрд руб., в 2016 г. – 1,89 млрд руб., в 2015 г. – 3,7 млрд руб.)[1].

На территории России и за ее пределами объем несанкционированных операций с использованием платежных карт[2], эмитированных российскими кредитными организациями, в 2018 г. составил 1,384 млрд руб.

---

[1] *По данным, полученным из форм обязательной отчетности об инцидентах информационной безопасности, официально представляемых кредитными организациями в Банк России, и данным, полученным в рамках информационного обмена, организованного ФинЦЕРТ Банка России.*

[2] *К платежным картам относятся расчетные, кредитные и предоплаченные карты.*

(в 2017 г. – 0,961 млрд руб., в 2016 г. – 1,08 млрд руб., в 2015 г. – 1,14 млрд руб.)[3].

Удельный вес таких операций в общем объеме операций с использованием платежных карт, эмитированных российскими кредитными организациями[4], в 2018 г. составил 0,0018% (1,8 коп. на 1000 руб. переводов).

При этом лимиты допустимого удельного веса несанкционированных переводов денежных средств, установленные Европейской службой банковского надзора (EBA), составляют 0,005% (5 евроцентов на 1000 евро переводов).

В Российской Федерации не зарегистрированы инциденты, которые приводили бы к критичному ущербу в системно значимых организациях кредитно-финансовой сферы. Вместе с тем ряд инцидентов вызывал нарушение непрерывности предоставления финансовых услуг и, как следствие, рост социальной напряженности в обществе. В малых и средних финансовых организациях инциденты информационной безопасности могут являться причиной прекращения их деятельности.

Результаты анализа покушений на хищение денежных средств кредитных организаций показывают, что риску хищения подвержены денежные средства в объеме, сопоставимом со средним дневным остатком по корреспондентскому счету кредитной организации, открытому в Банке России, суммированным со средним дневным приходом по соответствующему корреспондентскому счету.

Указанный объем денежных средств для малых и средних кредитных организаций нередко сопоставим с величиной их собственных средств (капитала).

К трендам, формирующим предпосылки для повышения значимости развития информационной безопасности финансового рынка Российской Федерации, относятся:

- скорость развития сферы цифровых финансовых услуг для повышения удобства и качества их предоставления в целях улучшения конкурентоспособности;
- активная позиция руководства страны по созданию цифровой экосистемы, стимулирующей развитие финансовых технологий;
- усиление роли защиты потребителей финансовых услуг от финансовых потерь и, как следствие, повышение доверия к финансовой системе Российской Федерации;
- интеграция показателей риска информационной безопасности (киберриска) в состав основных рисков финансовых организаций;
- увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере.

---

[3] *По данным формы отчетности о несанкционированных операциях с использованием платежных карт, представляемой кредитными организациями в Банк России. Увеличение показателя ущерба, связанного с несанкционированными операциями, обусловлено повышением уровня достоверности данных, представляемых в формах отчетности, формированием организационно-правовой основы для оперативного обмена данными.*

[4] *По данным формы отчетности о платежных картах и электронных денежных средствах, представляемой кредитными организациями в Банк России.*

Развитие цифровой среды неразрывно связано с применением постоянно возникающих прорывных и перспективных цифровых технологий.

Главными инфраструктурными проектами, основанными на использовании цифровых технологий, в отношении которых Банком России в первую очередь устанавливаются требования информационной безопасности, являются:

- платформа удаленной идентификации (Единая биометрическая система);
- Система быстрых платежей;
- платформа маркетплейс;
- цифровой профиль клиента.

В дальнейшем цифровая трансформация качественно изменит технологии предоставления финансовых услуг, поэтому, руководствуясь глобальными трендами развития, Банк России должен сформулировать новые подходы к информационной безопасности и киберустойчивости финансовой экосистемы в условиях:

- изменения архитектуры систем (использование технологии распределенных реестров);
- удаленного доступа к финансовым услугам и повсеместного использования мобильных технологий;
- применения новых перспективных технологий для целей информационной безопасности и киберустойчивости (Big Data, искусственный интеллект);
- Интернета вещей как элемента платежного пространства.

СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В сентябре 2019 г. Совет директоров Банка России одобрил Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов (далее – Основные направления). Документ определяет ключевые цели и задачи развития информационной безопасности и киберустойчивости, среди которых:

- обеспечение информационной безопасности и киберустойчивости в целях финансовой стабильности каждой организации финансового рынка;
- обеспечение операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы;
- противодействие компьютерным атакам, в том числе при использовании инновационных финансовых технологий;
- защита прав потребителей финансовых услуг.

Основные направления включают описание предпосылок и трендов в развитии информационной безопасности кредитно-финансовой сферы Российской Федерации, задачи и ключевые направления деятельности Банка России в области информационной безопасности и киберустойчивости, а также описание мероприятий в указанной области.

Мероприятия, предусмотренные Основными направлениями, разработаны в том числе в целях реализации комплекса отдельных задач в рамках федеральных проектов национальной программы «Цифровая экономика

Российской Федерации», утвержденных протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 6.05.2019 № 8.

Основные направления учитывают следующие документы:

- Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5.12.2016 № 646;
- Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденная Указом Президента Российской Федерации от 9.05.2017 № 203;
- Стратегия экономической безопасности Российской Федерации на период до 2030 г., утвержденная Указом Президента Российской Федерации от 13.05.2017 № 208;
- Основные направления развития финансового рынка Российской Федерации на период 2019–2021 годов;
- Основные направления развития финансовых технологий на период 2018–2020 годов;
- Приоритетные направления международной деятельности Банка России на период 2019–2021 годов.

Основные направления соответствуют мировому опыту и лучшим практикам в области обеспечения информационной безопасности финансовой сферы и управления риском информационной безопасности (киберриском): при разработке Основных направлений использовался опыт Национального института стандартов и технологий США (National Institute of Standards and Technology, NIST), Денежно-кредитного управления Сингапура (Monetary Authority of Singapore, MAS), Европейской службы банковского надзора (European Banking Authority, EBA), Международной организации комиссий по ценным бумагам (International Organization of Securities Commissions, IOSCO), Комитета по платежным и рыночным инфраструктурам при Банке международных расчетов (Committee on Payments and Market Infrastructures, CPMI), Базельского комитета по банковскому надзору (Basel Committee on Banking Supervision, BCBS).

Деятельность Банка России в сфере информационной безопасности и киберустойчивости (область регулирования) распространяется на следующие субъекты:

- кредитные организации, осуществляющие банковские операции;
- финансовые организации, осуществляющие финансовые операции в соответствии со статьей 76.1 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»;
- субъекты национальной платежной системы при проведении переводов денежных средств;
- инновационные финансовые технологии.

Общим принципом информационной безопасности и киберустойчивости организаций кредитно-финансовой сферы является реализация информационной безопасности на следующих уровнях:

- безопасность инфраструктуры – инфраструктурный уровень;
- безопасность прикладного программного обеспечения – уровень приложений;
- безопасность технологий обработки данных – уровень технологий обработки данных;
- протоколирование действий и операций (транзакций).

Реализация общих принципов строится с учетом следующих методологических подходов:

1. На инфраструктурном уровне – применение комплекса государственных стандартов, разрабатываемых в подкомитете № 1 Технического комитета № 122 «Стандарты финансовых (банковских) операций».

2. На уровне приложений – контроль отсутствия уязвимостей в программном обеспечении, в том числе связанных с недостатками программирования.

3. На уровне технологий обработки данных – обеспечение целостности и подлинности обрабатываемой информации.

4. Протоколирование действий и операций в объеме, достаточном в том числе для осуществления надзорной деятельности, обмена данными (с целью противодействия совершению компьютерных атак), дальнейшей работы правоохранительных органов.

ЦЕЛИ И ЗАДАЧИ ФИНЦЕРТ

ФинЦЕРТ Банка России является центром компетенций по обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере и осуществляет развитие информационной безопасности и киберустойчивости по следующим направлениям.

1. Выполнение функций отраслевого сегмента Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

2. Организация и координация деятельности организаций кредитно-финансовой сферы в качестве центра компетенций по противодействию кибератакам:

- автоматизированный сбор информации обо всех инцидентах поднадзорных субъектов;
- проведение эффективного технического анализа и экспертной оценки, в том числе компьютерные исследования и разбор вредоносных программ;
- оперативное распространение информации об инцидентах и правилах реагирования на них.

3. Выполнение функций центра координации деятельности по блокировке несанкционированных переводов денежных средств в платежной системе Банка России и иных платежных системах.

4. Прекращение функционирования фишинговых ресурсов и ресурсов, распространяющих вредоносное программное обеспечение, телефонных номеров и СМС-рассылок, используемых в мошеннических целях.

5. Взаимодействие с центральными (национальными) банками иностранных государств (в том числе государств – членов ЕАЭС) по вопросам мониторинга и реагирования на компьютерные атаки.

6. Взаимодействие с международными центрами реагирования на компьютерные атаки.

7. Повышение финансовой грамотности и пропаганда «компьютерной гигиены».

8. Взаимодействие с операторами по переводу цифровых финансовых активов.

Ключевые показатели эффективности ФинЦЕРТ (%)

Наименование целевого показателя	Целевое значение на 2017 год	Фактическое значение за 2017 год	Целевое значение на 2018 год	Фактическое значение за 2018 год	Целевое значение на 2020 год
Уровень доверия клиентов и контрагентов финансовых организаций к безопасности реализуемых электронных платежных сервисов	30	40	60	70	80
Доля объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт	0,005	0,0016	0,005	0,0018	0,005

ОБМЕН ИНФОРМАЦИЕЙ ОБ УГРОЗАХ. УЧАСТНИКИ, ЗАДАЧИ, ИНСТРУМЕНТЫ

В эпоху развития технологий и инноваций ФинЦЕРТ является лидером в реализации национальной программы «Цифровая экономика Российской Федерации» по направлению «Информационная безопасность» и по противодействию компьютерным атакам. ФинЦЕРТ осуществляет сбор и обработку поступающей от кредитных и некредитных финансовых организаций информации о произошедших и предотвращенных компьютерных атаках, пострадавших организациях и их клиентах, а также о лицах и организациях, причастных к совершению компьютерных атак, средствах и методах их совершения. На основе анализа получаемых данных ФинЦЕРТ уведомляет участников обмена об угрозах в области информационной безопасности в целях противодействия атакам на информационные ресурсы других участников обмена.

УЧАСТНИКИ ИНФОРМАЦИОННОГО ОБМЕНА

Информацию об угрозах информационной безопасности ФинЦЕРТ 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, курирующих информационную безопасность отрасли.

Для упрощения процесса информационного обмена, а также повышения оперативности и уровня его защищенности используется АСОИ ФинЦЕРТ, к которой в настоящий момент подключены все банки Российской Федерации, также ведется подключение страховых организаций и прочих

участников обмена. Всего к АСОИ ФинЦЕРТ подключено 826 организаций[5].

Число участников информационного обмена ФинЦЕРТ из категории «Некредитные финансовые организации» (НФО) по сравнению с предыдущим годом увеличилось более чем на 100 организаций. Это связано с повышением доверия к ФинЦЕРТ со стороны поднадзорных Банку России организаций и последующим введением в действие Положения Банка России № 684-П.

Число участников информационного обмена ФинЦЕРТ – НФО увеличилось более чем на 100 организаций

Также в отчетном периоде участниками информационного обмена стали более 20 вендоров защитных решений, разработчиков БПО, опера-

Рисунок 1
Структура участников информационного обмена ФинЦЕРТ

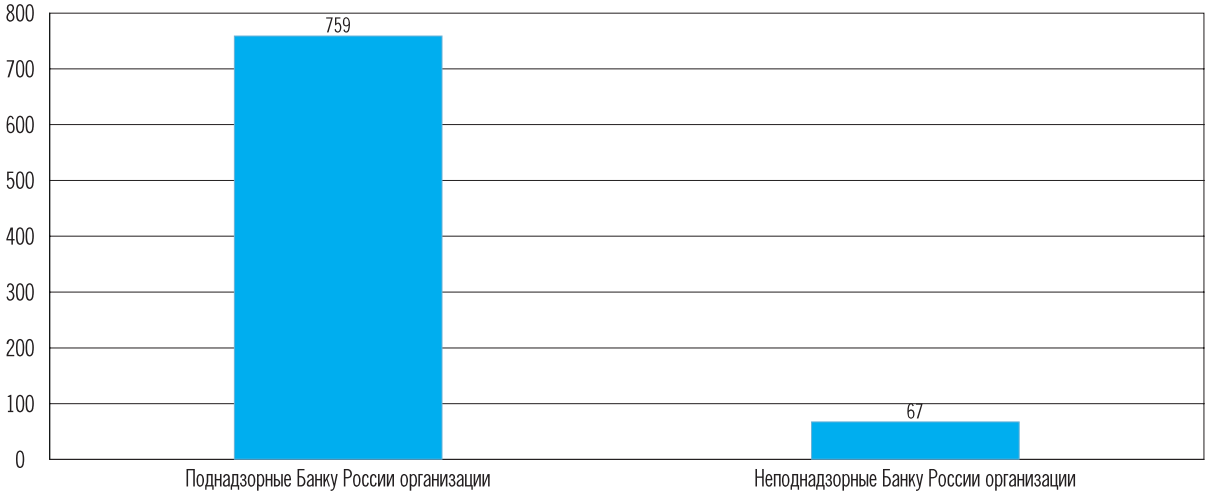
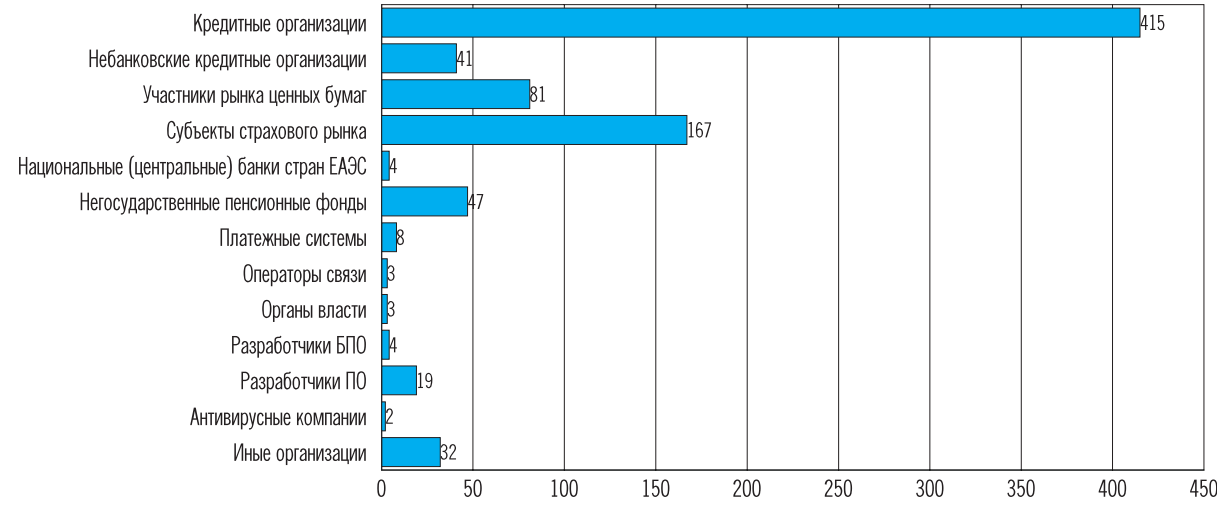


Рисунок 2
Структура участников информационного обмена ФинЦЕРТ по виду деятельности



[5] *ФинЦЕРТ изменил подход к классификации участников обмена по сравнению с 2018 г. ввиду принятия ряда нормативных актов, а также присоединения к АСОИ ФинЦЕРТ новых участников. Рисунок 2 основан на наиболее полной классификации и показывает данные по количеству участников разных категорий.*

Рисунок 3
Новые участники обмена – неподнадзорные Банку России организации

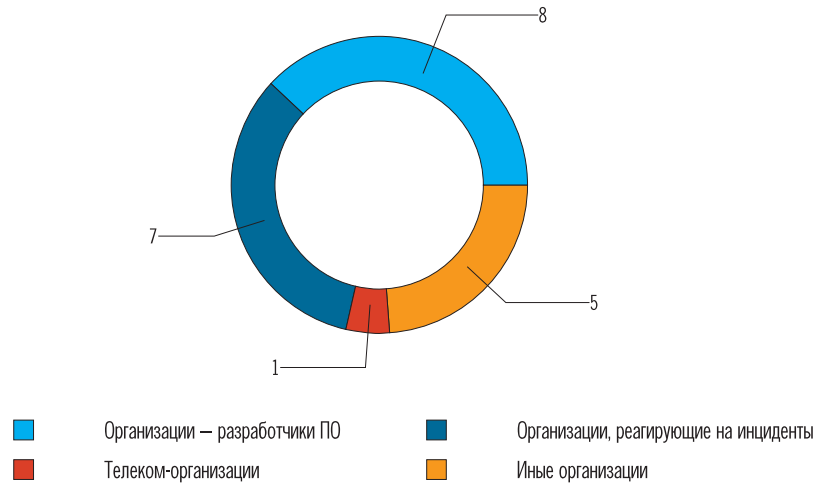
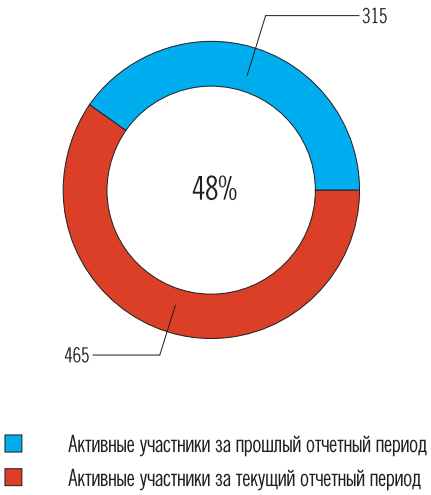


Рисунок 4
Активные участники информационного обмена



торов 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. За прошедший год было заключено 21 такое соглашение.

Необходимо отметить, что за рассматриваемый период количество активных участников информационного обмена ФинЦЕРТ, регулярно передающих информацию о выявленных угрозах и уязвимостях, увеличилось на 48% (с 315 до 465). Данное обстоятельство связано с активной реализацией поднадзорными организациями стандарта Банка России СТО БР БФБО-1.5-2018.

Количество активных участников информационного обмена ФинЦЕРТ увеличилось в 1,5 раза

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Взаимодействие ФинЦЕРТ с иностранными партнерами продолжает развиваться в направлении создания единого киберпространства и доверенной финансовой среды в рамках Евразийского экономического союза (ЕАЭС) и информационного обмена с национальными и международными организациями по обеспечению кибербезопасности[6].

В 2018 г. Банк России подписал со всеми участниками ЕАЭС соглашения о взаимодействии в области обеспечения информационной безопасности и в настоящее время оказывает консультационную и методологическую помощь национальным (центральным) банкам стран – участниц ЕАЭС по созданию собственных групп реагирования на компьютерные инциденты. В 2019 г. ФинЦЕРТ подготовил и заключил со всеми национальными (центральными) банками стран – участниц ЕАЭС пятистороннее соглашение о создании Рабочей группы по вопросам обеспечения информационной безопасности финансового рынка и противодействия компьютерным атакам в кредитно-финансовой сфере. Целью рабочей группы является подготовка рекомендаций по повышению уровня информационной безопасности финансовых рынков сторон путем сближения механизмов обеспечения информационной безопасности, в том числе механизмов, направленных на предупреждение и выявление компьютерных атак, создание условий для их пресечения.

Рисунок 5
Международная работа ФинЦЕРТ

[6] *Данные функции ФинЦЕРТ выполняет в рамках реализации задачи Банка России по обеспечению устойчивости финансовых организаций и доступности финансовых услуг в соответствии с Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».*

Также в рамках информационного обмена ФинЦЕРТ сотрудничает с зарубежными организациями, в том числе с группами реагирования ряда государств постсоветского пространства, а также Франции, Испании, Болгарии и иных стран. ФинЦЕРТ уведомлял партнеров о выявленных уязвимостях в информационных ресурсах, находящихся в зоне их ответственности, а также о готовящихся кибератаках и преступлениях в зоне их юрисдикции.

В конце 2018 г. было заключено лицензионное соглашение с Carnegie Mellon University, владельцем акронима CERT, который используется в англоязычном наименовании ФинЦЕРТ (Financial CERT). С декабря 2018 г. ФинЦЕРТ от лица Банка России получил статус авторизованного пользователя акронима CERT, что конкретизирует и укрепляет статус ФинЦЕРТ на международном уровне и способствует повышению эффективности взаимодействия с зарубежными организациями в области информационной безопасности финансовой сферы.

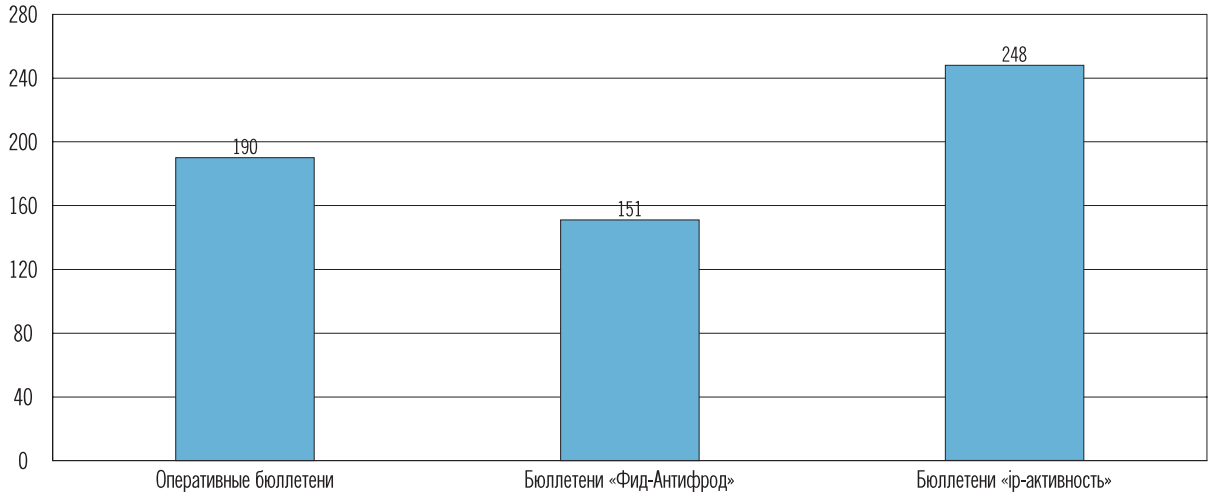
Опыт Банка России по созданию центров реагирования на кибератаки в кредитно-финансовой сфере учтен в проекте перечня рекомендаций по итогам Конференции АТЭС, направленных на развитие информационной безопасности в Азиатско-Тихоокеанском регионе.

ИНФОРМИРОВАНИЕ УЧАСТНИКОВ ОБМЕНА

ФинЦЕРТ стал в 2,7 раза чаще информировать участников обмена о киберугрозах

Как и предполагалось, расширение международного сотрудничества, увеличение числа участников обмена, а также их возросшая активность позволили ФинЦЕРТ аккумулировать значительные объемы информации о киберугрозах и кибератаках, подробно и детально изучать особенности каждого из показателей и своевременно оповещать своих партнеров об угрозах с предоставлением средств противодействия им. За рабочий год сформированы и разосланы 589 бюллетеней, что на 180% больше, чем годом ранее (211 бюллетеней).

Рисунок 6
Виды рассылаемых ФинЦЕРТ бюллетеней



АВТОМАТИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА

Система АСОИ ФинЦЕРТ

В 2018 г. для упрощения процесса информационного обмена, а также повышения его оперативности и защищенности Банком России была создана автоматизированная система обработки инцидентов (АСОИ ФинЦЕРТ). Первая очередь системы начала работу 1 июля 2018 г., когда к ней стали подключаться участники информационного обмена ФинЦЕРТ. Применение АСОИ ФинЦЕРТ для информирования об инцидентах информационной безопасности предусмотрено стандартом Банка России СТО БР БФБО-1.5-2018. Использование участником информационного обмена АСОИ ФинЦЕРТ позволяет существенно облегчить выполнение требований федеральных законов № 187-ФЗ и № 167-ФЗ, положений Банка России № 382-П и № 672-П, указаний Банка России № 4926-У и № 5039-У.

АСОИ ФинЦЕРТ была протестирована кредитными организациями, в 2018 г. успешно прошла приемочные испытания и приказом Банка России была введена в постоянную эксплуатацию. В течение второго полугодия 2018 г. проводилась работа по подключению к АСОИ ФинЦЕРТ всех кредитных организаций, с начала 2019 г. осуществляется подключение некредитных финансовых организаций. В настоящий момент к АСОИ ФинЦЕРТ подключено 826 участников информационного обмена (в том числе практически все организации, являющиеся операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем), число пользователей системы постоянно увеличивается.

Первая очередь АСОИ ФинЦЕРТ построена на базе отказоустойчивой и защищенной инфраструктуры и состоит из информационного портала, сервиса личных кабинетов участников, специализированных технологических подсистем и подсистемы информационной безопасности. Сегодня функционал системы позволяет автоматизировать следующие процессы между участниками информационного обмена и ФинЦЕРТ:

- 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 ФинЦЕРТ бюллетеней);
- оперативное взаимодействие между участником и ФинЦЕРТ по инцидентам и запросам;
- мониторинг информационных атак на организации кредитно-финансовой сферы и поддержка взаимодействия ФинЦЕРТ с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов.

АСОИ ФинЦЕРТ поддерживает получение и прием данных от участников информационного обмена, передаваемых посредством:

- заполнения в личном кабинете интерактивных форм об инцидентах, уязвимостях, угрозах;

- передачи информации, предусмотренной стандартом Банка России СТО БР БФБО-1.5-2018, в виде json-файлов, оформленных в соответствии с форматами системы и загружаемых в личный кабинет;
- взаимодействия систем на стороне участников обмена с АСОИ ФинЦЕРТ по API (прикладному протоколу программного взаимодействия).

На информационно-технологической базе АСОИ ФинЦЕРТ 26.09.2018 развернут функционал прототипа АС «Фид-АнтиФрод», обеспечивающего возможность выполнения требований Федерального закона № 167-ФЗ в части создания, формирования и ведения базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения кредитными организациями данных из этой базы.

Текущая средняя нагрузка на АСОИ ФинЦЕРТ – 1100 пользователей, одновременно работающих с системой, более 1000 запросов в сутки, до 120 бюллетеней (в рамках уникальных и групповых рассылок) в месяц.

С момента запуска АСОИ ФинЦЕРТ от участников получено и зарегистрировано более 300 тыс. сообщений об инцидентах, из них более 60% – с использованием API (в том числе по инцидентам, содержащим операции, осуществленные без согласия клиента).

Участники информационного обмена прислали в ФинЦЕРТ более 300 тыс. сообщений об инцидентах

В настоящее время проводятся работы по дальнейшему развитию АСОИ ФинЦЕРТ, в том числе планируется увеличение технической инфраструктуры для обеспечения бесперебойной работы системы, снижения времени технологических перерывов, реализации полнофункционального тестового контура, а также следующих возможностей:

- расширение функций информационно-сервисного портала и сервисов личных кабинетов АСОИ ФинЦЕРТ;
- оптимизация интерфейсной части для повышения оперативности взаимодействия;
- реализация возможности получения данных от участника в автоматическом режиме (по API) для всех видов инцидентов;
- предоставление сервиса в личном кабинете участника по проверке ВПО (включая специализированную «песочницу»);
- дополнительные функции по проверке авторства и целостности сообщений/запросов при взаимодействии с участниками с применением криптографических средств (сервис обмена электронными сообщениями между участниками и ФинЦЕРТ с использованием электронной подписи);
- реализация возможности пошагового заполнения электронных форм при информировании об операциях, осуществленных без согласия клиента («визарды» для упрощения заполнения информации);
- реализация функционала распространения индикаторов компрометации (IOC, «фидов») в машиночитаемых форматах для последующего их использования (в том числе в SIEM-системах участников);
- реализация функционала для участников по API-доступу к бюллетеням;
- предоставление участникам возможности передачи через личный кабинет «дампов» сетевого трафика и лог-файлов веб-серверов для последующего анализа в ФинЦЕРТ;

Банк России запустит «песочницу» для участников обмена ФинЦЕРТ

- сервис уведомлений о критических инцидентах по СМС;
- сервис автоматического и автоматизированного взаимодействия участников с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Система «Фид-АнтиФрод»

В соответствии с требованиями Федерального закона № 167-ФЗ в Банке России создана база данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и с 26.09.2018 обеспечена возможность получения данных из этой базы для всех организаций, являющихся операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем.

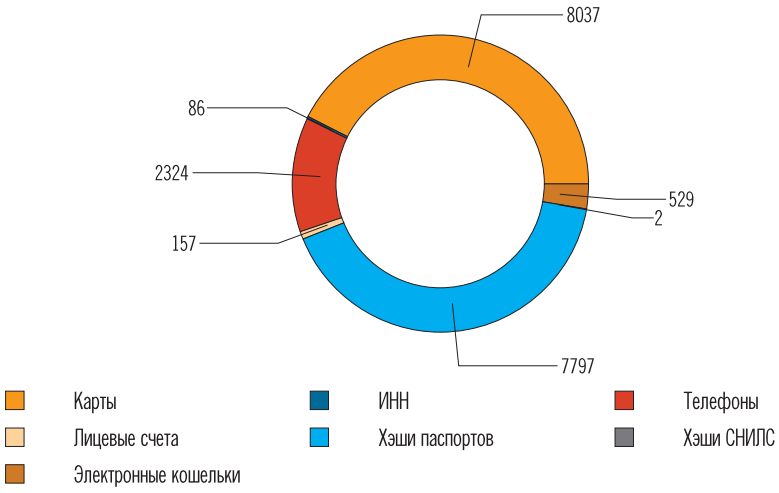
В настоящее время данный функционал реализуется прототипом АС «Фид-АнтиФрод», завершается создание полнофункциональной системы. АС «Фид-АнтиФрод» будет работать как самостоятельная система на основе АСОИ ФинЦЕРТ, используемой в качестве базовой инфраструктурно-технологической платформы.

АС «Фид-АнтиФрод» предназначена для аккумулирования и быстрого обмена информацией об операциях без согласия клиента. Основными участниками такого обмена являются операторы по переводу электронных денежных средств, операторы услуг платежной инфраструктуры и Банк России. Информация об операциях без согласия клиента от участников информационного обмена передается в ФинЦЕРТ. Далее с использованием АС «Фид-АнтиФрод» и АСОИ ФинЦЕРТ осуществляется оперативное информирование кредитных организаций, являющих получателями денежных средств по операциям, совершенным без согласия клиента. Затем в результате анализа информации по таким операциям формируются специальные сообщения для всех кредитных организаций (так называемые «фиды», содержащие признаки операций, совершенных без согласия клиента), которые позволяют применять кредитным организациям как меры предупредительного характера, так и меры реагирования.

В результате функционирования АС «Фид-АнтиФрод» (прототипа АС «Фид-АнтиФрод») участники информационного обмена получают информацию:

- о хэшированных данных номеров паспортов получателей денежных средств по операциям, осуществленным без согласия клиента;
- о хэшированных данных СНИЛС получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни ИНН организаций – получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни счетов получателей денежных средств и БИК банков по операциям, осуществленным без согласия клиента;
- перечни номеров карточек получателей денежных средств по операциям, осуществленным без согласия клиента;
- перечни номеров телефонов получателей денежных средств, задействованных в операциях, осуществленных без согласия клиента;

Рисунок 7
Сообщения о признаках несанкционированных операций, переданные в ФинЦЕРТ, по состоянию на 31.08.2019



- перечни номеров электронных кошельков получателей денежных средств, задействованных в операциях, осуществленных без согласия клиента.

К настоящему моменту накоплено почти 19 тыс. сообщений об уникальных признаках операций, совершенных без согласия клиента.

Данные из АС «Фид-АнтиФрод» (прототипа АС «Фид-АнтиФрод») позволяют кредитным организациям дополнять свои антифрод-системы информацией, получаемой от других банков, уже столкнувшихся с мошенниками. Это существенно повышает эффективность работы по предотвращению хищений денежных средств со счетов клиентов.

На 2019–2020 гг. запланировано развитие АС «Фид-АнтиФрод», которая позволит увеличить скорость и оперативность функционирования системы, повысить качество «фидов», создать возможность для информирования о всех видах мошеннических операций, совершаемых без согласия клиента.

ВЫВОДЫ И ПРОГНОЗЫ

После вступления в силу Федерального закона № 167-ФЗ и начала работы АСОИ ФинЦЕРТ прозрачность предоставляемых в Банк России данных о хищениях существенно повысилась, при этом по итогам 2018 г. центр получил высокие оценки своей работы со стороны банковского сообщества[7]. Наряду с этим в условиях снижения преступности и смещения фокуса внимания злоумышленников с организаций кредитно-финансового сектора на их клиентов первостепенное значение в области информа-

[7] *По результатам опроса 116 кредитных организаций показатель оценки участниками обмена работы ФинЦЕРТ по итогам 2018 г. составляет более 8 из 10 баллов в случае, когда происходит хищение денежных средств или компьютерная атака, а также когда необходима блокировка ресурсов в сети Интернет или номеров телефонов, используемых в мошеннических целях. Рассылки ФинЦЕРТ более 89% респондентов отметили как информативные.*

ционного обмена об угрозах и рисках приобретает обмен информацией о признаках несанкционированных операций.

На фоне развития финансового рынка и его нормативно-правового регулирования это приведет к дальнейшему росту количества участников информационного обмена и увеличению объема получаемых ФинЦЕРТ данных. Дальнейшая автоматизация информационного обмена позволит взаимодействовать с ними наиболее оперативно, получая актуальную информацию об угрозах в сфере информационной безопасности и своевременно направляя ее участникам обмена.

БОРЬБА С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ: БЛОКИРОВКА ВРЕДОНОСНЫХ САЙТОВ, СМС-РАССЫЛОК И КОЛЛ-ЦЕНТРОВ КРИМИНАЛЬНЫХ СТРУКТУР

В 2018 г. более 97% хищений со счетов физических лиц и 39% хищений со счетов юридических лиц было совершено с использованием приемов социальной инженерии (злонамеренное введение в заблуждение путем обмана или злоупотребления доверием). Отличительная черта этого вида мошенничества – таргетированность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на их счета, при этом средства ее достижения варьируются.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Анализ средств и методов социальной инженерии позволяет сделать вывод, что основными объективными факторами, способствующими распространению социальной инженерии, являются неправомерный доступ и обработка персональных данных физических лиц.

Так, для хищения денежных средств методом социальной инженерии мошенникам достаточно владеть информацией о фамилии, имени и отчестве (далее – ФИО), а также о номере телефона физического лица. При этом данные, относящиеся к банковской тайне, необязательны для совершения противоправных действий, они лишь уточняют и дополняют необходимую информацию.

По результатам мониторинга информационного поля вокруг темы утечек баз данных за период 1.01.2019 – 30.06.2019 было выявлено 18 ключевых событий, из них только три события касались утечек баз данных

организаций финансового сектора. Определенное количество утечек баз данных, обсуждаемых в публичном пространстве, связано с государственными структурами. Также за период 1.01.2019 – 30.06.2019 произошли еще три утечки баз данных организаций кредитно-финансовой сферы, информация о которых не получила широкого распространения в социальных медиа и СМИ. За данный период обнаружено 12 903 публикации с предложениями о покупке/продаже различных баз данных, при этом только 12% относились к базам данных кредитно-финансовых организаций. В связи с этим следует отметить важность принятия Федерального закона № 167-ФЗ, принятия Банком России в рамках имеющихся полномочий необходимых нормативных актов[8], вводящих в том числе требования национальных стандартов, а также методических рекомендаций и стандартов Банка России[9], направленных на противодействие хищению денежных средств.

Наряду с этим часть утечек баз данных Роскомнадзор не классифицирует как утечку именно персональных данных. Согласно Стратегии повышения финансовой доступности в Российской Федерации на период 2018–2020 годов, уровень владения счетами высокий и доля взрослого населения (в возрасте от 18 лет и старше), имеющего банковские счета, составляет 79,5%. На основании этого можно сделать вывод о том, что утечки из организаций кредитно-финансовой сферы затрагивают лишь небольшое количество взрослого населения Российской Федерации. Таким образом, источниками утечки персональных данных являются не столько уполномоченные сотрудники организаций кредитно-финансовой сферы, имеющие доступ к указанным данным, сколько иные многочисленные операторы обработки персональных данных.

Результаты мониторинга и анализа информации об утечках данных клиентов кредитно-финансовых организаций показывают, что каналами утечек являются также следующие.

1. Получение данных в результате несанкционированного доступа к многочисленным ресурсам в сети Интернет, продающим какие-либо товары или оказывающим какие-либо услуги с дистанционной оплатой с использованием карт. При оформлении заказов клиенты таких ресурсов часто сообщают о себе данные в объеме, достаточном для их дальнейшей идентификации (ФИО, адрес, номера телефонов). А номера банковских карт, использованных для оплаты, иногда получают в результате скрытого встраивания в код ресурсов вредоносного кода, считывающего, сохраняющего и передающего их взломщикам. В некоторых случаях данные клиентов могут быть проданы самими владельцами или сотрудниками указанных ресурсов.

---

[8] *Приказ Банка России от 27 сентября 2018 г. № ОД-2525 «Об установлении признаков осуществления перевода денежных средств без согласия клиента»; Указание Банка России № 4926-У; Положение Банка России № 683-П; Положение Банка России № 684-П.*

[9] http://cbr.ru/credit/Gubzi_docs/stnd/.

2. Получение данных в результате наблюдения за массовыми торговыми площадками, ведение разведки в отношении конкретных участников таких ресурсов. Может использоваться парсинг (автоматическое сканирование) страниц ресурсов с последующей чисткой и обработкой результатов. Данные платежных карт часто сообщают в переписке или в телефонных разговорах сами участники. В дальнейшем они могут сопоставляться и компилироваться с информацией, ранее полученной из других источников, в том числе из прошлых утечек баз данных иного назначения, доступных на рынке (базы данных налогоплательщиков, владельцев автомобилей, недвижимости и иной собственности), социальных сетей. В некоторых случаях в результате таких разведывательных и аналитических мероприятий полный набор данных о конкретном клиенте кредитно-финансовой организации может так и не быть получен, однако недостающие сведения либо выясняются у самого клиента в процессе разговора с ним оператора («звонаря»), либо вообще игнорируются, и разговор строится только на имеющихся неполных данных.
3. Персональные данные также легко доступны широкому кругу лиц в телеграм-ботах за определенную плату.

Следует допустить возможность существования любых иных каналов получения преступниками информации о клиентах кредитно-финансовых организаций. Также допускается повторение попыток мошенничества в отношении уже пострадавших от мошенничества граждан в случаях, когда преступники сохраняют полученные ранее данные. Повторное обращение к таким клиентам может осуществляться под предлогом проведения расследования первого случая.

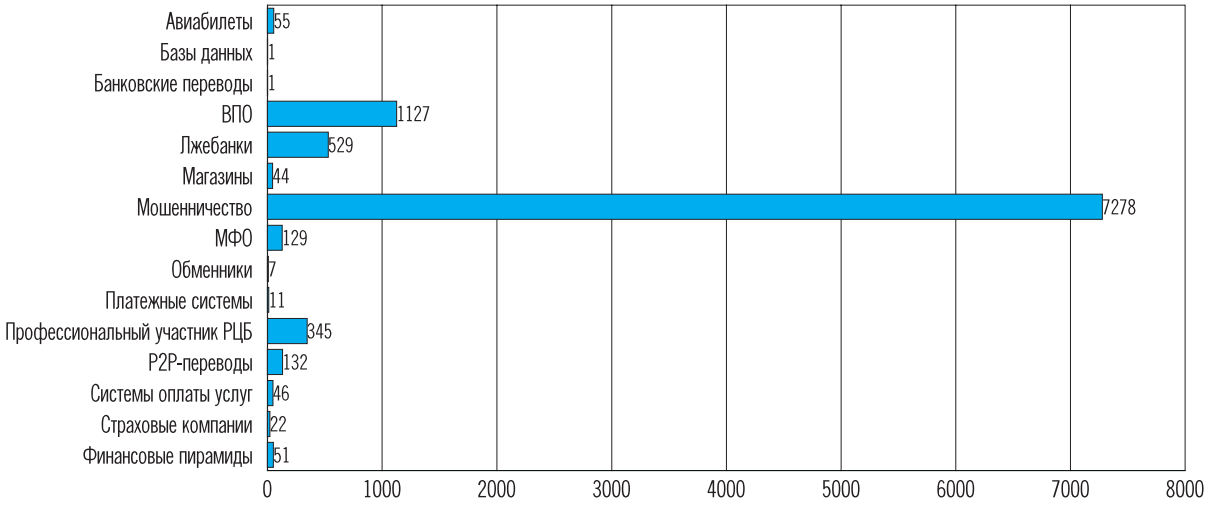
Противодействие подобным преступлениям – одно из целевых направлений работы ФинЦЕРТ. Прекращение работы мошеннических колл-центров и блокировка СМС-рассылок происходят при участии операторов связи и телеком-провайдеров. При обнаружении сайтов с вредоносным программным обеспечением ФинЦЕРТ направляет информацию о них в ГосСОПКА. Разделегирование фишинговых сайтов производится при участии регистраторов доменных имен – как российских, так и зарубежных.

СНЯТИЕ С ДЕЛЕГИРОВАНИЯ ФИШИНГОВЫХ САЙТОВ

Минимальное время разделегирования домена снизилось с 24 до 3 часов

Для борьбы с фишингом у Банка России в лице ФинЦЕРТ есть полномочия по инициированию снятия с делегирования мошеннических интернет-ресурсов: он уведомляет регистраторов доменных имен о доменах, с которых рассылается вредоносный код и осуществляются мошеннические действия, связанные с использованием платежных карт. В рамках указанной деятельности ФинЦЕРТ взаимодействует с Координационным центром доменов .ru/.рф, Фондом Развития Интернет и Центром взаимодействия компьютерных сетей «MSK-IX». Разделегирование доменов занимает от 3 часов до 3 дней.

Рисунок 8
Разделегированные домены



В отчетном периоде зафиксирован значительный (почти в 7 раз) рост количества сайтов в категории мошеннических (лжеопросы, лжекомпенсации, лжевыигрыши и так далее). ФинЦЕРТ инициировал снятие с делегирования 9778 фишинговых доменов – на 486% больше их числа годом ранее (1668 доменов). Рост количества запросов на разделегирование обусловлен развитием данного направления деятельности ФинЦЕРТ (в частности, появлением дежурной службы, благодаря чему снятие с делегирования доменов осуществляется в режиме 24/7/365), а также активным взаимодействием с международными организациями и иностранными группами реагирования.

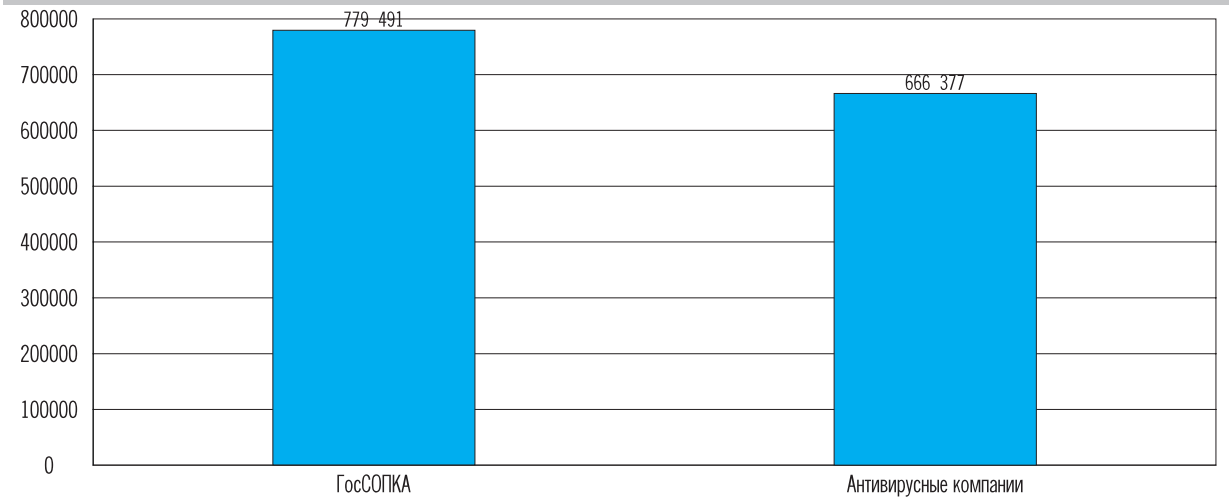
Начиная с сентября 2018 г. ФинЦЕРТ направил информацию о 9778 фишинговых доменах для снятия с делегирования

Положительное решение о разделегировании предложенных ФинЦЕРТ доменов за отчетный период было принято по 85% ресурсов (в предыдущем отчетном периоде – 76%). Рост доли (при значительном повышения общего количества) разделегированных сайтов обусловлен высоким качеством экспертизы ФинЦЕРТ при оценке мошеннических ресурсов, а также расширением сотрудничества ФинЦЕРТ с регистраторами и хостерами, в том числе зарубежными. Так, за истекший год в доменных зонах .ru, .рф, .su инициировано снятие с делегирования 3303 доменов, в остальных зонах – 6475. Это полностью подтвердило сделанный в предыдущем отчете прогноз о постепенном переходе мошеннических ресурсов в юрисдикцию иностранных доменных зон.

2/3 разделегируемых доменов приходится на зарубежные ресурсы

В настоящее время запросы на разделегирование фишинговых ресурсов, находящихся за пределами доменных зон .ru, .рф, .su, в отношении которых у ФинЦЕРТ нет соответствующих компетенций, направляются в адрес компетентных организаций для оказания содействия по снятию с делегирования. Также информация направляется в Генеральную прокуратуру Российской Федерации, которая в свою очередь выносит постановление о возбуждении административного производства о признании информации запрещенной к распространению на территории Российской Федерации и направляет его в суд.

Рисунок 9
Выявленные домены с ВПО



После принятия проекта федерального закона № 605945-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» процедура блокирования сайтов, находящихся в иностранных доменных зонах, будет существенно упрощена. У Банка России появятся полномочия по внесудебной блокировке фишинговых сайтов путем прямого взаимодействия с Роскомнадзором по вопросам включения сайтов в реестр запрещенной к распространению на территории Российской Федерации информации.

Указанный законопроект предполагает также введение досудебного механизма блокировки сайтов, распространяющих вредоносное программное обеспечение. Банк России получит право обращаться в суд с заявлением в защиту прав, свобод и законных интересов неопределенного круга лиц в связи с размещением указанной информации в информационно-телекоммуникационных сетях, в том числе в сети Интернет. После принятия решения судом Банк России будет вправе обратиться в Роскомнадзор для принятия соответствующих мер[10].

САЙТЫ С ВПО

Вредоносное программное обеспечение по-прежнему остается одним из основных инструментов компьютерных преступников. Рассылки писем с зараженными вирусами файлами или ссылками на сайты с ВПО активно используются для атак на финансовые организации и их клиентов. В целях

[10] *Роскомнадзор осуществляет в дальнейшем взаимодействие с провайдером для устранения нарушений. Провайдер же в свою очередь уведомляет администратора сайта о выявленных нарушениях и предоставляет ему возможность устранить выявленные нарушения. В случае непринятия мер провайдером или оператором Роскомнадзор уведомляет операторов связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети Интернет, или к размещенной на нем информации.*

противодействия мошенническим ресурсам ФинЦЕРТ взаимодействует с антивирусными лабораториями и с ГосСОПКА.

В период с 1.09.2018 по 31.08.2019 ФинЦЕРТ выявил и направил информацию в ГосСОПКА и антивирусные лаборатории для включения в базы этих организаций 779 491 и 666 377 доменных имен ресурсов с ВПО соответственно.

С 1.09.2018 по 31.08.2019 ФинЦЕРТ выявил около 780 тыс. сайтов с ВПО

БОРЬБА С СМС-РАССЫЛКАМИ И КОЛЛ-ЦЕНТРАМИ МОШЕННИЧЕСКИХ СТРУКТУР

В 2019 г. в арсенале злоумышленников появился новый способ обмана жертв. Технология подмены исходящего телефонного номера на номера, идентичные номерам колл-центров кредитных организаций, позволила им успешно выдавать себя за сотрудников служб безопасности банков

Рисунок 10
Количество заблокированных телефонных номеров

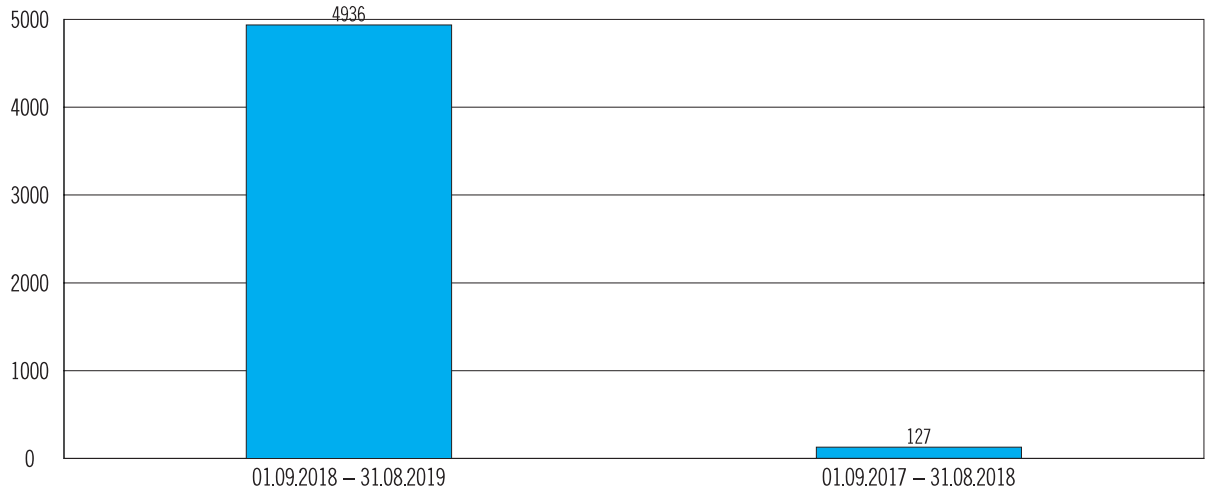
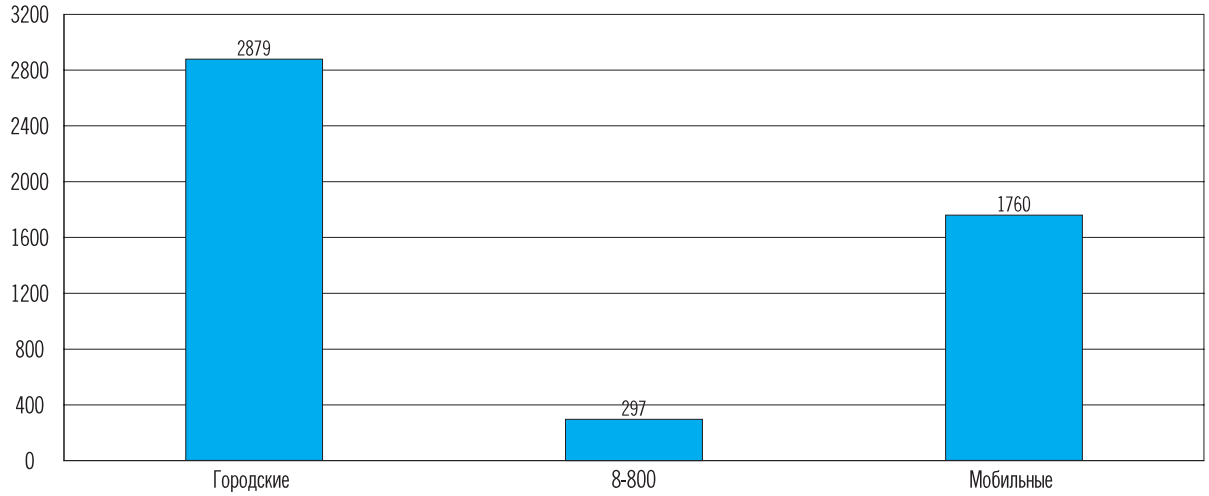


Рисунок 11
Чаще всего мошенники звонят с городских номеров (в том числе подмененных)



и под видом блокировки подозрительных транзакций совершать хищения средств жертв.

Количество заблокированных телефонных номеров выросло в 38 раз

Как следствие, количество поступающих в ФинЦЕРТ сообщений о номерах телефонов злоумышленников существенно увеличилось. В результате ФинЦЕРТ отправил на блокировку в сигнальной сети информацию о 4936 номерах мобильных операторов и номерах в коде 8-800, задействованных в мошеннических СМС-рассылках, получении рассылок, атаках, заражениях ВПО и так далее.

РИСКИ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Обладая персональными данными, злоумышленники с легкостью имитируют диалог с сотрудником банка, страховой компании, государственной структуры или иной организации. Исходя из предположения, что указанные данные могут быть известны только им, жертва поддается на обман, сообщая в конечном итоге контрольные слова, коды подтверждений и другую информацию, предоставляющую мошенникам возможность вывести с подконтрольных клиенту счетов денежные средства.

Первым субъективным фактором, обусловливающим успешность хищения, является низкий уровень «компьютерной гигиены» жертвы. Переход по ссылкам из непроверенных источников на зараженные сайты, скачивание «кастомизированных» приложений и бесплатных «авторских» аналогов известных программ на мобильные телефоны, игнорирование установки антивируса и его предупреждений – все это делает возможным получение злоумышленниками логина и пароля от личного кабинета или первичных данных по банковской карте. Однако чтобы завершить платеж, им нужно получить CVC- и CVV-коды (если речь идет о платеже на стороннем сайте) и одноразовый пароль для подтверждения операции.

Для того чтобы убедить человека выдать эту информацию (либо принудить жертву совершить платеж самостоятельно – например, через банкомат), преступнику необходим личный контакт с жертвой – звонок по телефону. И здесь решающим является второй фактор – уровень критичности мышления в стрессовой ситуации. Стресс не обязательно должен иметь негативный характер: это сильное эмоциональное потрясение, которое может быть положительным и радостным.

Повышение киберграмотности населения

В связи с активным внедрением систем дистанционного банковского обслуживания и появлением новых видов угроз в кредитно-финансовой сфере необходимо повышение информированности населения о правилах безопасного использования платежных инструментов и банковских услуг (киберграмотности).

Сотрудники ФинЦЕРТ провели 24 публичных мероприятия для разных целевых аудиторий. Примерная численность прошедших обучение, а также слушателей по всем мероприятиям составила более 2000 человек.

Для младшей начальной школы (1–4 класс) были проведены два открытых урока по «компьютерной гигиене»; для средней и старшей школы

(5–11 класс) – пять мероприятий по киберграмотности с охватом более 1000 человек; для старшей школы в целях профориентации (9–11 класс) – четыре мероприятия.

В части профориентации в рамках смены ОЦ «Сириус» образовательного фонда «Талант и успех» проведена работа с талантливыми школьниками – авторами проекта «Средство автоматизации выявления индикаторов компрометации, полученных участниками информационного обмена. Разработка утилиты, позволяющей проводить экспресс-диагностику информационных систем банка на предмет вмешательства вредоносных программ». Подобного рода деятельность осуществляется для профориентации школьников и студентов с целью их последующего привлечения к работе в организациях кредитно-финансового сектора, включая Банк России.

Для людей старшего возраста был проведен цикл из пяти лекций по финансовой безопасности и противодействию кибермошенничеству с пробным охватом более 100 человек на площадке Центральной библиотеки им. Некрасова в рамках программы мэра Москвы «Московское долголетие».

Помимо этого, эксперты ФинЦЕРТ выступили на пяти публичных площадках с общим числом участников более 1500 слушателей.

Информационная кампания

Если первый субъективный фактор риска практически не зависит от когнитивных параметров личности, то второй может быть использован мошенниками, а следовательно, Банку России нужно работать в направлении противодействия ему. Чтобы эта работа была максимально эффективной, она должна быть адресной. Адресность, в свою очередь, достигается максимально точным описанием психологического портрета и ключевых точек уязвимости жертв. Совместно с представителями служб информационной безопасности банков, психологами и представителями структурных подразделений Банка России были проанализированы данные кредитных организаций и выделены пять основных типов жертв:

- индивидуалисты (благополучные в финансовом плане, легко тратят деньги на себя и удовольствия, излишне доверяют новым технологиям);
- школьники, студенты, лица с особенностями социальной адаптации (доверчивые, расточительные, импульсивные, склонные к риску; противоречивая самоидентификация);
- бюджетораспорядители семей с невысоким уровнем дохода и высокой финансовой нагрузкой (целеустремленные, высоко ценят семейные и дружеские связи, ответственные);
- домохозяйки (уступчивые, доверчивые; внешний локус контроля);
- пенсионеры.

На основе этих и иных данных Банк России проводит информационную кампанию при содействии федеральных и региональных СМИ, а также социальных медиа. Ее цель заключается в том, чтобы предупредить жите-

лей России об актуальных угрозах в сфере телефонного мошенничества, а также дать гражданам рекомендации по противодействию им.

ВЫВОДЫ И ПРОГНОЗЫ

В условиях снижения преступности и числа целевых атак на организации кредитно-финансового сектора первостепенное значение приобретают бесперебойность их функционирования и защита (обеспечение целостности и конфиденциальности) персональных и платежных данных их клиентов. С хищением конфиденциальной информации связана значительная часть инцидентов, когда кража данных является этапом для подготовки хищения средств. Утечки персональных и учетных данных значительно упрощают процесс получения доступа к данным платежных карт, при этом сама по себе продажа тех и других в Даркнете также является способом получения незаконного дохода.

Повышение степени защищенности информационных систем кредитных организаций привело к тому, что фокус внимания преступников сместился на атаки на клиентов банков. Как следствие, спрос на данные продолжит расти, и в связи с этим тенденция роста числа покушений на хищение платежных и персональных данных клиентов банков сохранится. Результативность и масштаб последствий этих преступлений будут зависеть от того, насколько добросовестно организации кредитно-финансового сектора будут соблюдать законодательство и нормативные требования Банка России, в том числе регулирующие порядок доступа, использования и передачи данных, а также правила их размещения в облачных хранилищах.

При этом необходимо помнить, что соучастниками хищения данных становятся как профессиональные преступники, так и недобросовестные сотрудники коммерческих, государственных, медицинских и иных учреждений. Поэтому базовым элементом атак останется социальная инженерия, которая в условиях разнообразия типов скомпрометированных данных обеспечит рост видов «заходов» и схем обмана граждан. В связи с этим одновременно с борьбой с утечками необходимо вести профилактическую работу с клиентами банков.

КОНТРОЛЬНО-НАДЗОРНАЯ ДЕЯТЕЛЬНОСТЬ ФИНЦЕРТ

ФинЦЕРТ установил, что все случаи хищения денежных средств произошли в связи с многочисленными нарушениями требований федеральных законов Российской Федерации и нормативных и иных актов Банка России в части обеспечения защиты информации, отсутствием должного внимания и внутреннего контроля поднадзорных организаций к вопросам информационной безопасности и недостаточной осведомленностью работников поднадзорных организаций об актуальных угрозах информационной безопасности (в том числе о методах социальной инженерии).

РЕЗУЛЬТАТЫ ПРОВЕРОК

Одним из приоритетных направлений деятельности Департамента информационной безопасности является участие в плановых и внеплановых проверках субъектов кредитно-финансовой сферы по вопросам выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств и применения информационных технологий.

За период с сентября 2018 г. по август 2019 г. включительно по тематике информационной безопасности и информационных технологий были организованы 122 проверки субъектов кредитно-финансовой сферы (кредитных организаций, некредитных финансовых организаций).

1. По результатам указанных проверок выявлено 694 нарушения федеральных законов Российской Федерации, нормативных и иных актов Банка России:

- **8 нарушений требований федеральных законов, таких как федеральные законы № 161-ФЗ, № 395-1, № 325-ФЗ;**

- **447 нарушений требований Положения Банка России № 382-П,** в том числе:
  - 53 нарушения в части необеспечения регистрации действий при осуществлении доступа работников к защищаемой информации и действий, связанных с назначением и распределением прав доступа к защищаемой информации, отсутствия необходимых внутренних документов (пп. 2.6.3);
  - 52 нарушения в части отсутствия технических средств защиты информации от воздействия вредоносного кода на средствах вычислительной техники (пп. 2.7.1);
  - 34 нарушения в части необеспечения использования технических средств защиты информации от воздействия вредоносного кода различных производителей на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств (пп. 2.7.3);
  - 31 нарушение в части несанкционированного расширения прав доступа работников к защищаемой информации (назначение излишних прав доступа) (пп. 2.6.4);
  - 14 нарушений в части отсутствия учета и контроля состава программного обеспечения, установленного на средствах вычислительной техники (пп. 2.10.1).
- **5 нарушений требований Положения Банка России № 672-П,** в том числе 4 нарушения, связанных с необеспечением надлежащей защиты электронных сообщений при их передаче в Банк России (п. 14.3).
- **6 нарушений требований Положения Банка России № 684-П**, в том числе:
  - 3 нарушения в части недоведения до клиентов рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (п. 2);
  - 3 нарушения, связанных с невыполнением требований технической документации при использовании СКЗИ (п. 3).
- **96 нарушений требований Положения Банка России № 552-П,** в том числе:
  - 14 нарушений в части невыполнения требований эксплуатационной документации на СКЗИ и АРМ КБР (п. 2.4);
  - 12 нарушений, связанных с невыполнением процедур идентификации, аутентификации и авторизации при логическом доступе работников к участку платежной системы Банка России с использованием персонифицированных уникальных учетных записей (п. 4.1);
  - 8 нарушений в части необеспечения срока хранения информации систем видеонаблюдения и контроля доступа в течение не менее трех лет (п. 3.4).

- **61 нарушение требований иных документов Банка России (положений Банка России № 242-П, № 471-П, Указания Банка России № 2831-У).**
- **71 нарушение положений стандарта Банка России СТО БР ИББС-1.0-2014,** в том числе:
  – 6 нарушений в части несоблюдения принципа предоставления работникам минимально необходимых для выполнения их служебных обязанностей прав и полномочий (пп. 7.2.1);
  – 10 нарушений, связанных с конфликтом интересов при совмещении функций разработки и сопровождения, разработки и эксплуатации, сопровождения и эксплуатации АБС/ПО, функций администратора системы и администратора информационной безопасности, выполнения операций в АБС и контроля их выполнения (пп. 7.2.3);
  – 5 нарушений в части невыполнения правил и процедур управления предоставлением/отзывом и блокированием доступа к информационным активам Банка, блокирования сеанса доступа после установленного времени бездействия (пп. 7.4.3);
  – 10 нарушений в части отсутствия средств антивирусной защиты на автоматизированных рабочих местах (АРМ) или серверах АБС, а также в части невыполнения регулярного обновления средств антивирусной защиты (пп. 7.5.1);
  – 9 нарушений в части использования одного и того же средства антивирусной защиты на серверном оборудовании и рабочих станциях (пп. 7.5.6).

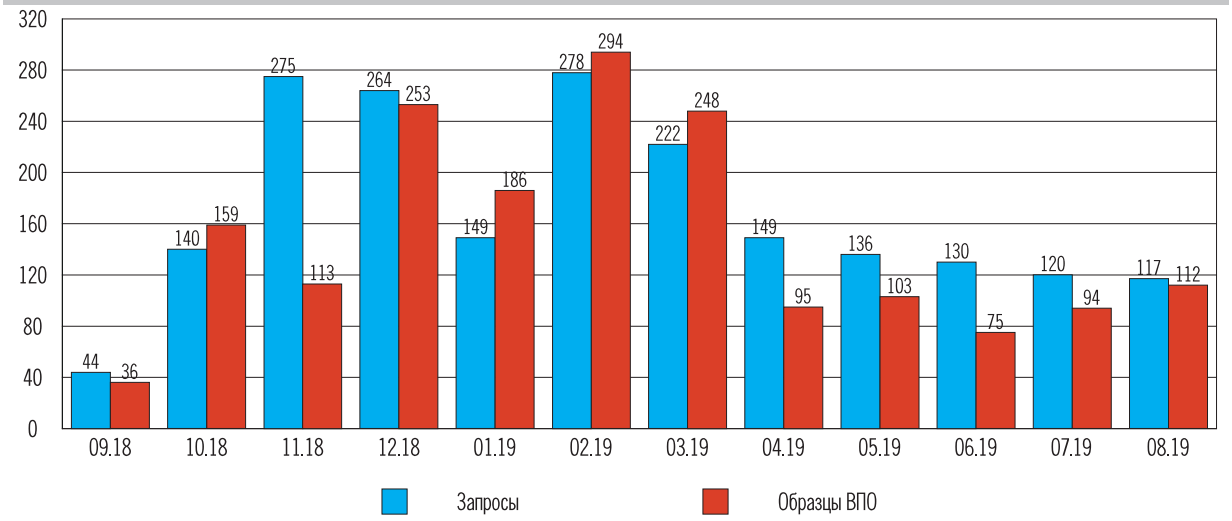
2. Результаты проведенных проверок показывают, что все выявленные нарушения связаны с человеческим фактором, а именно:

– недостаточное знание и понимание нормативной базы по вопросам информационной безопасности;
– недостаточная ответственность работников поднадзорных организаций в отношении выполнения требований к обеспечению информационной безопасности;
– недостаточная организация в поднадзорных организациях внутреннего аудита и внутреннего контроля по вопросам информационной безопасности;
– формальное отношение собственников и руководителей поднадзорных организаций к выполнению требований по обеспечению информационной безопасности как к неприоритетному направлению работы.

Выявленные нарушения приводят к снижению эффективности организации информационной безопасности и к потенциальной возможности реализации ряда угроз информационной безопасности, в том числе:

– необоснованному расширению полномочий и прав доступа отдельных работников организации, позволяющему осуществлять бесконтрольные действия с защищаемой информацией, в том числе с электронными платежными документами, персональными данными и остатками на счетах клиентов (нарушения, связанные

Рисунок 12
Поступление запросов по месяцам



с наличием факторов, провоцирующих конфликт интересов и излишнюю концентрацию полномочий; необеспечением регистрации действий лиц, обладающих правами доступа к защищаемой информации; необеспечением учета объектов информационной инфраструктуры и используемого программного обеспечения);

– возможности успешного воздействия вредоносного кода на объекты информационной инфраструктуры, открывающего доступ злоумышленникам к несанкционированному управлению данными счетов клиентов, позволяющего имитировать действия клиента по совершению электронных платежей, приостановке возможности осуществления поднадзорной организацией и ее клиентами необходимых операций (нарушения, связанные с отсутствием должной защиты от воздействия вредоносного кода, своевременного и эффективного реагирования на воздействие вредоносного кода). Так, в период с 1.09.2018 по 31.08.2019 через АСОИ ФинЦЕРТ от участников информационного обмена поступило 2024 запроса по теме компьютерных атак, содержавших 1768 образцов вредоносного программного обеспечения.
– осуществлению злоумышленниками воздействия на объекты информационной инфраструктуры вследствие неэффективного контроля доступа к объектам участка платежной системы Банка России;
– возможности создания подложных электронных платежных поручений при осуществлении переводов денежных средств в результате невыполнения требований к организации работы с криптографическими ключами;
– низкой эффективности организации системы внутреннего контроля в части обеспечения информационной безопасности вследствие необеспечения своевременного реагирования на инциденты информационной безопасности и анализа их причин.

АНАЛИЗ ПРИЧИН И ПОСЛЕДСТВИЙ НАРУШЕНИЙ

Отмеченные изъяны в обеспечении информационной безопасности финансовых организаций приводят к реальным потерям денежных средств и утечкам защищаемой информации.

Несмотря на то, что Департамент информационной безопасности проводит профилактику возможных кибератак путем выпуска соответствующих бюллетеней, за период с сентября 2018 г. по настоящее время в поднадзорных организациях им был зафиксирован ряд инцидентов информационной безопасности (в том числе хищений денежных средств у поднадзорных организаций). Так, например:

1. В конце 2018 г. в результате хакерской атаки на кредитную организацию был осуществлен ряд несанкционированных переводов денежных средств на общую сумму более 5,5 млн руб. и 15 тыс. евро. Причиной стало нарушение нормативных актов Банка России, в частности:

– невыполнение требований Положения Банка России № 382-П об использовании средств защиты информации от воздействия вредоносного кода и обеспечении выявления фальсифицированных электронных сообщений (пп. 2.7.1 и 2.10.4);
– в нарушение требований СТО БР ИББС-1.0-2014 не были разделены сегменты вычислительных сетей и не обеспечена эшелонированная централизованная антивирусная защита (пп. 7.4.5 и 7.5.6).

2. В начале 2019 г. в связи с отсутствием надлежащей защиты от воздействия вредоносного кода произошло заражение вредоносным ПО информационной инфраструктуры кредитной организации, в результате чего был осуществлен ряд несанкционированных переводов с ее корреспондентского счета с использованием платежной системы Банка России на общую сумму свыше 22 млн рублей.

3. В начале 2019 г. в результате использования злоумышленниками уязвимости программного обеспечения интернет-ресурса кредитной организации произошла утечка персональных данных клиентов – физических лиц данной кредитной организации, что увеличивает риск осуществления результативных атак на клиентов. Причиной стало нарушение нормативных актов Банка России, в частности Положения Банка России № 382-П:

– отсутствие контроля со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий (пп. 2.5.3);
– невыполнение требований по информационной безопасности на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры, в том числе нереализация запрета несанкционированного копирования защищаемой информации (пп. 2.5.6);
– невыполнение требований к защите информации при осуществлении переводов денежных средств в разработанном кредитной организацией ПО (пп. 2.5.7).

4. В середине 2019 г. в результате действий злоумышленников осуществлены несанкционированные переводы денежных средств кредитной организации на общую сумму 755 тыс. руб., а также несанкционированные переводы денежных средств некредитной финансовой организации на общую сумму более 16 млн долл. США. Причиной в обоих случаях стала недостаточная осведомленность работников организаций в области обеспечения защиты информации (п. 2.12 Положения Банка России № 382-П, п. 8.9 СТО БР ИББС-1.0-2014), в частности работники не смогли распознать действия социальной инженерии, направленные на них.

Анализ инцидентов, в расследовании которых принимал участие Департамент информационной безопасности, позволил выявить **основные факторы, способствовавшие успешному совершению атаки на организации кредитно-финансовой сферы**.

1. Некорректная настройка почтовых серверов и недостаточная проверка входящих писем, в результате чего их возможно использовать как «отражатели» (а равно и получение фишинговых писем целевой организацией): формируется письмо с заведомо несуществующим адресом в организации, где установлен почтовый сервер, который будет использован в роли «отражателя», в исходном письме модифицируются («спуфятся») заголовки, относящиеся к отправителю. При получении такого письма сервер организации, который собираются использовать в роли «отражателя», обнаруживает, что такого получателя нет, – и возвращает письмо отправителю (по полю, указанному в Reply, где содержится адрес целевой организации). В целевую организацию приходит стандартный ответ вида «ваше письмо не удалось доставить получателю», во вложении – «плохое» письмо. Как показывает практика, это позволяет обойти большинство спам-фильтров и повышает процент открываемости писем на стороне целевой организации, так как срабатывает человеческий фактор («не помню, что я там отправлял, надо посмотреть»). Особенно хорошо это работает в отношении людей, которые вынуждены отправлять большое количество писем в адреса совершенно разных организаций: секретари, работники тендерных отделов и так далее. Основной метод защиты – предотвращение использования своего почтового сервера в качестве «рассыльщика». Этого можно достичь при помощи хотя бы проверки SPF-записи отправителя, а также проверок DKIM/DMARC. Рекомендация для потенциальных «получателей»: настройка проверки SPF-записи отправителя и настройка DKIM/DMARC. Чем больше организаций это сделает, тем меньше вероятности, что такое письмо «пройдет» на стороне «сервера-отражателя», поскольку в технических заголовках всегда виден реальный адрес отправителя, в 99% случаев не совпадающий с ip-адресами того домена, от имени которого делают рассылку.
2. Отсутствие актуальных патчей для программного обеспечения, прежде всего операционной системы Windows и офисного программного обеспечения Microsoft Office. Основной список используемых уязвимостей не изменился по сравнению с 2018 – началом 2019 г.:

№	Уязвимость	Описание	Устранение	Комментарий
1	CVE-2015-1641	Некорректно сформированный RTF-документ Microsoft Office	Установка пакетов обновления MS Office	Используется в начальной фазе атаки в фишинговом письме, позволяет атакующему загрузить программное обеспечение и установить связь с командным сервером для проведения дальнейшей атаки. Использовалась группой Carbanak (Cobalt Strike)
2	CVE-2014-1812 CVE-2014-4113 CVE-2015-1701 CVE-2015-2363 CVE-2015-2426 CVE-2016-7255	Повышение привилегий в ОС семейства Windows	Установка кумулятивных обновлений Windows через Центр обновления Microsoft	Используется в фазе закрепления, перемещения по сети, разведки для получения доступа к интересующим объектам сети. Используется различным специализированным ПО, таким как Cobalt Strike, Metasploit, Empire
3	CVE-2017-11882 CVE-2018-0802	Нарушение данных в области памяти Microsoft Office и его компонентов, позволяющее выполнить произвольный код	Установка пакетов обновления MS Office	Используется в начальной фазе атаки в фишинговом письме, позволяет атакующему загрузить программное обеспечение и установить связь с командным сервером для проведения дальнейшей атаки. Использовалась группой Carbanak (Cobalt Strike)
4	CVE-2017-0199 CVE-2017-8570	Уязвимости, связанные с некорректной обработкой встраиваемых в документ Microsoft Office Word различных объектов (подгружаемых данных из других документов и так далее)		

3. Отсутствие контроля активности внутри локальной сети и отсутствие сегментации сети, что дает возможность атакующим запускать инструменты разведки (например, сканеры уязвимостей, средства для перехвата паролей администраторов, запуск процессов с повышенными привилегиями и так далее).
4. Отсутствие периодических тренировок по кибербезопасности, проводимых с пользователями, особенно работающими на критичных АРМ.

РЕКОМЕНДАЦИИ

Основные рекомендации, которые позволят минимизировать риски успешной кибератаки на организацию кредитно-финансовой сферы и выполнить нормативные требования, предъявляемые Банком России:

- использование и своевременное обновление современного антивирусного программного обеспечения;
- своевременная установка исправлений (patch-management) безопасности операционных систем и прикладного программного обеспечения;
- использование учетных записей с минимально необходимыми для работы пользователя привилегиями, ограничение количества учетных записей локальных администраторов;
- проведение регулярных тренингов с пользователями внутри организации и с представителями организаций-клиентов по линии осведомленности в области информационной безопасности (security awareness);

- проведение «киберучений», проверяющих готовность персонала противостоять атакам на информационную инфраструктуру организации, а также устойчивость к атакам с использованием социальной инженерии;
- качественные парольные политики (необходимо исключить использование сотрудниками паролей, не соответствующих требованиям безопасности);
- исключение применения уязвимых конфигураций домена Active Directory, например назначение локальных администраторов политиками домена; целесообразно использовать «лучшие практики» (Best Practices) от производителя при конфигурировании домена;
- отсутствие в организации неконтролируемых каналов доступа в сеть Интернет (в обход межсетевых экранов и иных программно-аппаратных средств контроля и ограничения).

Для улучшения процессов обнаружения и реагирования на атаки необходимо:

- вести протоколы (журналы, логи) сетевых соединений пограничных устройств, установить разумный и достаточный период их хранения, но не менее трех месяцев (90 дней);
- вести протоколы (журналы, логи) критичных для осуществления банковских операций систем не менее пяти лет, остальных систем, критичных для организации, – не менее трех лет (согласно Положению Банка России № 382-П);
- проводить периодические проверки инфраструктуры по известным индикаторам компрометации систем и сетей (IOC), разработать и применять соответствующие процедуры реагирования в случаях выявления срабатываний по индикаторам;
- ввести в эксплуатацию средства обнаружения вторжений (IDS), содержащие сигнатуры обнаружения следов работы часто использующегося атакующими программного обеспечения (Mimikatz, Meterpreter и так далее);
- исключить установку и массовое использование администраторами сетей средств удаленного администрирования наподобие TeamViewer, RAdmin; в случае необходимости установки таких средств обеспечить протоколирование и хранение журналов, ограничить диапазон ip-адресов подключения;
- составить единый список разрешенного к использованию программного обеспечения, своевременно актуализировать данный список, осуществлять контроль за соблюдением списка;
- исключить хранение в открытом виде паролей доступа к критичным информационным системам, по возможности организовать централизованное хранение паролей;
- в случаях выявления атак и неспособности самостоятельно справиться с ними и их последствиями рекомендуется привлекать специализированные экспертные организации для оказания помощи.

ТРЕНДЫ

В течение 2019 г. наблюдается снижение количества попыток атак на организации кредитно-финансовой сферы. Интерес преступных групп, ранее активно атаковавших банки и другие организации кредитно-финансовой сферы России, сместился в сторону стран СНГ и дальнего зарубежья.

С меньшей интенсивностью продолжаются и атаки на устройства самообслуживания, осуществляемые, как правило, неустойчивыми малыми группами либо одиночками. При этом скиммеры и шиммеры почти не встречаются, позиции сохраняют только blackbox-атаки с использованием специализированных устройств (без учета некомпьютерных атак – взломов, взрывов, хищений устройств и прочего).

На стабильном уровне сохраняется количество атак на клиентов банков – юридических лиц и индивидуальных предпринимателей. Основной инструмент таких атак – вредоносное программное обеспечение RTM.

Сохраняется высокая интенсивность кампаний по распространению вредоносного программного обеспечения класса ransomware, хотя они и не являются целевыми по отношению к организациям кредитно-финансовой сферы.