Банк России

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ НА ПЕРИОД 2019–2021 ГОДОВ

МОСКВА
2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 2

ПРЕДПОСЫЛКИ И ТРЕНДЫ 3

ЗАДАЧИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ БАНКА РОССИИ
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6

ОБЩИЕ ПОЛОЖЕНИЯ 8

ПРАВОВОЕ РЕГУЛИРОВАНИЕ 9

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ
ИНФРАСТРУКТУРЫ 11

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ
ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 13

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ
ТЕХНОЛОГИЙ ОБРАБОТКИ ДАННЫХ 14

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ
ФИНАНСОВЫХ ТЕХНОЛОГИЙ 15

ПОДГОТОВКА КАДРОВ И ОБЕСПЕЧЕНИЕ ДОВЕРИЯ ГРАЖДАН
К ЦИФРОВОЙ СРЕДЕ 17

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО 19

НАЦИОНАЛЬНАЯ ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА
РОССИЙСКОЙ ФЕДЕРАЦИИ» 20

ЦЕНТР КОМПЕТЕНЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И ПРОТИВОДЕЙСТВИЮ КИБЕРАТАКАМ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ 21

НАДЗОРНАЯ ДЕЯТЕЛЬНОСТЬ 23

Материал подготовлен Департаментом информационной безопасности.

Фото на обложке: Shutterstock/FOTODOM

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

ВВЕДЕНИЕ

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов (далее – Основные направления) определяют 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 06.05.2019 № 8.

Основные направления учитывают следующие документы:

- Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646;
- Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203;
- Стратегия экономической безопасности Российской Федерации на период до 2030 года, 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 Банка международных расчетов (Committee on Payments and Market Infrastructures, CPMI), Базельского комитета по банковскому надзору (Basel Committee on Banking Supervision, BIS).

ПРЕДПОСЫЛКИ И ТРЕНДЫ

Цифровая трансформация создает многочисленные преимущества для потребителей финансовых услуг, неизбежно увеличивает качество, скорость, доступность взаимодействия потребителей финансовых услуг и финансовых организаций, но вместе с тем создает дополнительные риски.

Рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, является глобальным трендом, требующим скоординированных усилий регуляторов, правоохранительных органов, организаций кредитно-финансовой сферы и потребителей финансовых услуг.

Крупномасштабные кибератаки наносят значительный экономический ущерб, приводят к изменениям в геополитических отношениях и снижению уровня доверия к информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет).

Кибератаки на цифровые финансовые системы способны спровоцировать финансовый кризис.

В Отчете Всемирного экономического форума по глобальным рискам 2018 года 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 Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка

России (далее – ФинЦЕРТ Банка России)[1], 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. – порядка 1,89 млрд руб., в 2015 г. – порядка 3,7 млрд руб.).

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. (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 копейки на 1000 рублей 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 хищения 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 прав 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;

---

[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] Здесь и далее к платежным картам относятся расчетные карты, кредитные карты, предоплаченные карты.

[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.

- увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере.

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

Основными инфраструктурными проектами, основанными на использовании цифровых технологий, в отношении которых в первую очередь Банком России 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.

ЗАДАЧИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ БАНКА РОССИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках Основных направлений Банк России ставит перед собой следующие задачи в области информационной безопасности и киберустойчивости.

1) Обеспечение киберустойчивости:
- обеспечение готовности кредитно-финансовой сферы гарантировать финансовую стабильность и операционную надежность в условиях реализации компьютерных атак, в том числе обеспечение операционной надежности и непрерывности предоставления финансовых и банковских услуг;
- контроль показателей риска реализации информационных угроз;
- контроль уровня банковских и финансовых операций, совершенных без согласия клиентов;
- мониторинг, оперативное реагирование и предотвращение компьютерных атак на организации кредитно-финансовой сферы.

2) Защита прав потребителей финансовых услуг через мониторинг показателей уровня финансовых потерь.

3) Содействие развитию инновационных финансовых технологий в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности.

Для реализации поставленных задач в Банке России создан Департамент информационной безопасности, выполняющий в том числе функции Центра компетенций в области обеспечения информационной безопасности финансовой сферы.

Центр компетенций разрабатывает методологию и обеспечивает развитие информационной безопасности в кредитно-финансовом секторе с учетом мировых трендов по следующим основным направлениям:

1) Стандартизация:
- разработка стандартов (включая разработку ГОСТ) в области информационной безопасности и киберустойчивости и организация работы подкомитета № 1 Технического комитета № 122 «Стандарты финансовых (банковских) операций» Росстандарта;
- обеспечение участия экспертов Банка России в области стандартизации в работе международных организаций.

2) Межведомственное взаимодействие по вопросам обеспечения информационной безопасности.

3) Национальная программа «Цифровая экономика Российской Федерации»:
- участие ФинЦЕРТ Банка России как лидера в реализации национальной программы «Цифровая экономика Российской Федерации» по направлению «Информационная безопасность» и по противодействию компьютерным атакам;
- участие в единой системе противодействия киберугрозам и подготовке к противодействию кибератакам в кредитно-финансовой сфере;
- формирование требований к информационной безопасности при применении инновационных технологий;
- участие в развитии программы импортозамещения, а также в анализе риска, связанного с применением компонентов инфраструктуры иностранного производства.

4) Надзор за уровнем риска информационной безопасности (киберриска) в кредитных и некредитных финансовых организациях, субъектах национальной платежной системы.

5) Противодействие распространению в кредитно-финансовой сфере информации о деятельности нелегальных участников данной сферы и об их услугах.

6) Создание условий для развития культуры информационной безопасности и кибергигиены в кредитно-финансовой сфере.

ОБЩИЕ ПОЛОЖЕНИЯ

Деятельность Банка России в сфере информационной безопасности и киберустойчивости (область регулирования) распространяется на следующие субъекты[5]:

- 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 осуществлении переводов денежных средств;

а также на следующие объекты:

- инновационные финансовые технологии.

Общим принципом информационной безопасности и киберустойчивости организаций кредитно-финансовой сферы является реализация информационной безопасности 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).

Реализация общих принципов строится с учетом следующих методологических подходов:

– на инфраструктурном уровне – применение комплекса государственных стандартов, разрабатываемых в подкомитете № 1 Технического комитета № 122 «Стандарты финансовых (банковских) операций»;
– на уровне приложений – контроль отсутствия уязвимостей в программном обеспечении, в том числе связанных с недостатками программирования;
– на уровне технологий обработки данных – обеспечение целостности и подлинности обрабатываемой информации;
– протоколирование действий и операций в объеме, достаточном в том числе для целей осуществления надзорной деятельности, обмена данными для противодействия совершению компьютерных атак, дальнейшей работы правоохранительных органов.

[5] *За исключением структурных подразделений Банка России.*

ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Обеспечение информационной безопасности на финансовом рынке требует формирования механизма правового регулирования, включающего в том числе полномочия Банка России по организации такого обеспечения и установлению регуляторных требований к участникам финансового рынка.

Правовой механизм обеспечения информационной безопасности на финансовом рынке должен гарантировать предсказуемость реализации Банком России своих полномочий, а также предсказуемость надзора за исполнением требований участниками финансового рынка.

В настоящее время в соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, Банк России определен в качестве органа, составляющего организационную основу системы обеспечения информационной безопасности Российской Федерации, а организации кредитно-финансовой сферы – в качестве участников системы.

В соответствии со статьями 57.4, 76.4-1 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (с изменениями) (далее – Закон о Банке России) Банк России по согласованию с ФСБ России и ФСТЭК России устанавливает требования к обеспечению защиты информации:

- для кредитных организаций при осуществлении банковской деятельности;
- для некредитных финансовых организаций при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью первой статьи 76.1 Закона о Банке России.

Статья 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» устанавливает обязанность операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов платежных систем, операторов услуг платежной инфраструктуры обеспечивать защиту информации при осуществлении переводов денежных средств.

Законом о Банке России установлены регуляторные полномочия Банка России по вопросам информационной безопасности и защиты информации при осуществлении:

- переводов денежных средств, банковских и финансовых операций;
- ведения базы данных о случаях и попытках несанкционированных переводов денежных средств;
- информационного обмена между организациями кредитно-финансовой сферы и ФинЦЕРТ Банка России в соответствии с частями 6 и 7 статьи 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (с изменениями).

Формирование соразмерного регуляторного воздействия в сфере информационной безопасности и киберустойчивости предполагается осуществлять по следующим направлениям:

1) Выявление в сети Интернет сайтов, используемых для совершения мошеннических действий в кредитно-финансовой сфере, и ограничение в пределах, установленных Конституцией Российской Федерации и федеральными законами, доступа потребителей финансовых услуг к таким сайтам, что требует закрепления за Банком России полномочий:

- по блокированию в сети Интернет:
  - фишинговых сайтов;
  - сайтов, связанных с предложением и (или) предоставлением финансовых услуг субъектами, не имеющими права их оказывать в соответствии с действующим законодательством;
  - сайтов, используемых для распространения информации о финансовых пирамидах, привлекающих средства и имущество физических и юридических лиц.

- по досудебному блокированию в сети Интернет сайтов, связанных с распространением вредоносного программного обеспечения.

2) Противодействие мошенничеству в финансовой сфере через выстраивание единого канала обмена данными о мобильном устройстве, абоненте номера мобильного телефона между операторами связи и банками, некредитными финансовыми организациями, в том числе микрофинансовыми организациями (важно, например, в ситуациях смены сим-карт, смены владельца номера мобильного телефона, подозрений на заражение мобильного устройства).

3) В рамках работ по совершенствованию механизмов использования усиленной квалифицированной электронной подписи и законодательства, регулирующего деятельность удостоверяющих центров, Банк России формирует комплексные предложения по выстраиванию единой системы удостоверяющих центров в кредитно-финансовой сфере, в которой удостоверяющий центр Банка России становится головным для всего финансового рынка.

4) Создание условий для безопасного оборота цифровых финансовых активов посредством установления соразмерных требований к информационной безопасности и защите информации в этой сфере. Соразмерность требований Банка России к защите информации будет зависеть от уровня рисков, объема и характера осуществляемых организацией кредитно-финансовой сферы операций, уровня и сочетания присущих ее деятельности рисков.

5) Отдельными направлениями в рамках национальной программы «Цифровая экономика Российской Федерации» являются координация деятельности участников финансового рынка в целях реализации мероприятий федеральных проектов национальной программы «Цифровая экономика Российской Федерации» по выработке подходов к регулированию требований к применению цифровых технологий на финансовом рынке с учетом требований безопасности (например, цифровые финансовые активы, искусственный интеллект, Big Data, киберфизические системы, системы распределенного реестра и другие).

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ ИНФРАСТРУКТУРЫ

Обеспечение безопасности и устойчивости вычислительной инфраструктуры является инфраструктурной задачей, решение которой предполагается реализовать путем применения комплекса государственных стандартов, разрабатываемых в рамках подкомитета №1 Технического комитета №122 «Стандарты финансовых (банковских) операций»[6].

Определение уровня защищенности вычислительной инфраструктуры (экосистемы) организаций кредитно-финансовой сферы планируется осуществлять комплексно в отношении каждой категории поднадзорных Банку России субъектов с учетом вида и масштаба (пропорциональное регулирование) их деятельности[7]. Кроме того, предполагается осуществить нормативное закрепление обязанности представления финансовыми организациями в Банк России показателей, характеризующих объем несанкционированных клиентом операций по отношению к общему объему операций. При этом при расчете данного показателя не должны будут учитываться операции, совершенные без согласия клиента в случаях, предусмотренных федеральными законами или нормативными актами Банка России, а также договором.

Формирование требований к определению уровня защищенности Банк России осуществляет в рамках разработки методологии информационной безопасности.

Методологической основой защиты информации на инфраструктурном уровне является применение комплекса государственных стандартов:

- домен УР – «Управление риском реализации информационных угроз»;
- домен ЗИ – «Защита информации финансовых организаций»;
- домен УИиСО – «Управление инцидентами защиты информации и обеспечение ситуационной осведомленности»;
- домен ОН – «Обеспечение операционной надежности»;
- домен УА – «Управление риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных услуг (сервисов)».

Цель формирования методологии – совершенствование комплекса отраслевых документов, устанавливающих требования к обеспечению информационной безопасности и управлению киберриском для построения фундаментальной основы деятельности Банка России и организаций кредитно-финансовой сферы по противодействию актуальным информационным угрозам, кибератакам и компьютерной преступности.

---

[6] *Приказ Росстандарта от 21.08.2017 №1759 «Об организации деятельности технического комитета по стандартизации «Стандарты финансовых операций».*

[7] *Положением Банка России от 17.04.2019 №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», а также Положением Банка России от 17.04.2019 №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» установлены обязательные для кредитных организаций и некредитных финансовых организаций требования к защите информации в соответствии с Национальным стандартом Российской Федерации ГОСТ Р 57 580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 №822-ст), которые вступают в силу с 1 января 2021 года.*

Основные принципы информационной безопасности и защиты информации по комплексу стандартов:

- обязательность применения документов по стандартизации, разрабатываемых Банком России;
- реализация риск-ориентированного подхода к обеспечению выполнения государственных стандартов;
- использование сервисов ФинЦЕРТ Банка России для координации деятельности организаций кредитно-финансовой сферы и повышения их готовности к противостоянию киберугрозам.

Основным документом комплекса отраслевых документов по обеспечению информационной безопасности на инфраструктурном уровне будет являться ГОСТ Р «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз. Общие положения», который определит:

- основу корпоративного управления по вопросам обеспечения информационной безопасности и киберустойчивости;
- состав и содержание процессов и ключевых направлений деятельности по обеспечению информационной безопасности для всех доменов;
- общую (единую) терминологию, используемую во всех отраслевых документах по обеспечению информационной безопасности;
- классификатор уровней обеспечения информационной безопасности (уровней защищенности) – классификатор состава и содержания требований по обеспечению информационной безопасности и мер по их реализации.

Планируется выделить три уровня защищенности – минимальный, стандартный и усиленный. Для конкретного типа финансовой организации уровень защищенности определяется с учетом:

- вида деятельности финансовой организации, состава предоставляемых финансовых услуг, реализуемых бизнес-процессов и (или) технологических процессов;
- объема финансовых операций;
- значимости финансовой организации для финансового рынка и национальной платежной системы.

Целевым индикатором завершения этапов стандартизации является формирование в 2021 г. законченного комплекса государственных стандартов.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для контроля отсутствия уязвимостей в программном обеспечении, в том числе связанных с недостатками программирования, позволяющими совершать результативные компьютерные атаки, необходимо создать организационные и технические условия проведения финансовыми организациями анализа уязвимостей прикладного программного обеспечения, используемого для осуществления перевода денежных средств (или совершения иных финансовых операций (транзакций), а также определения, какое программное обеспечение должно быть подвергнуто анализу.

В качестве методологической основы безопасности программного обеспечения следует выделить:

- разрабатываемый в настоящее время Банком России профиль защиты для оценки уязвимостей в банковских приложениях, применяемых для переводов денежных средств, включая требования по анализу уязвимостей и контролю недекларированных возможностей, в методологии Национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15 408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.11.2013 № 1340-ст «Об утверждении национального стандарта»;
- использование системы сертификации ФСТЭК России (испытательных лабораторий и органов по сертификации) для проведения работ по контролю качества программного обеспечения, распространяемого кредитной организацией, некредитной финансовой организацией среди своих клиентов для совершения действий в целях осуществления финансовых операций, и анализу его уязвимостей на основе положений профиля защиты;
- создание экосистемы для проведения работ по анализу защищенности информационной инфраструктуры, используемой для осуществления переводов денежных средств, состоящей из организаций, обладающих необходимой компетенцией, и разработчиков.

Целевыми индикаторами являются:

- нормативное закрепление системы сертификации ФСТЭК России для проведения работ по контролю качества программного обеспечения;
- разработка профиля защиты;
- формирование экосистемы для проведения работ по анализу защищенности информационной инфраструктуры.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ ТЕХНОЛОГИЙ ОБРАБОТКИ ДАННЫХ

Обеспечение безопасности обработки данных с использованием цифровых технологий является задачей, решение которой предполагается осуществлять индивидуально – применительно к каждой конкретной финансовой технологии.

Реализация требований безопасности технологий обработки данных должна обеспечивать целостность, подлинность обрабатываемой информации.

Требованиями к безопасности технологий обработки данных при осуществлении переводов денежных средств (или иных финансовых операций (транзакций) являются:

- обеспечение целостности и подлинности информации на каждом технологическом участке ее обработки;
- взаимодействие с клиентами финансовых организаций;
- протоколирование действий на технологических участках, в том числе для анализа информации об уровне риска на каждом из технологических участков;
- ведение баз данных об инцидентах информационной безопасности, в том числе на основе претензионной работы.

Ключевые технологические меры информационной безопасности и защиты информации:

- использование средств электронной подписи (криптографии);
- реализация принципа «двойного контроля» при обработке защищаемой информации;
- многофакторная аутентификация клиентов, в том числе с применением средств криптографической защиты информации;
- реализация механизмов получения дополнительного подтверждения клиентами финансовых операций.

Целевым индикатором является время разработки требований к безопасности технологий обработки данных для каждой конкретной новой финансовой технологии (не более 1 месяца) с учетом применения проактивной (упреждающей) модели.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Применение цифровых финансовых технологий, с одной стороны, способствует развитию финансового рынка, повышению финансовой доступности и развитию конкуренции, а с другой – появлению новых рисков информационной безопасности. С развитием цифровых технологий происходит рост киберугроз, требующих оперативного и своевременного обнаружения, оценки и разработки соответствующих мер по их предотвращению или минимизации возможных последствий.

Банк России с учетом лучших зарубежных практик формирует требования к информационной безопасности и операционной надежности финансовых технологий по следующим ключевым направлениям и задачам в соответствии с Основными направлениями развития финансовых технологий на период 2018–2020 годов:

1) Правовое регулирование по вопросам информационной безопасности и операционной надежности устанавливается в разрабатываемых федеральных законах.

2) Создание и развитие следующих элементов безопасной и устойчивой финансовой инфраструктуры:
- платформа для удаленной идентификации;
- Система быстрых платежей;
- платформа маркетплейс;
- платформа для регистрации финансовых сделок;
- платежная система Банка России;
- национальная система платежных карт;
- система передачи финансовых сообщений;
- платформа для облачных сервисов;
- платформа на основе технологии распределенных реестров.

3) Исследование, анализ и разработка требований к обеспечению информационной безопасности при применении следующих финансовых технологий:
- RegTech (regulatory technology), SupTech (supervision technology);
- Big Data, Smart Data;
- мобильные технологии;
- искусственный интеллект, роботизация и машинное обучение;
- биометрия;
- технология распределенных реестров;
- открытые интерфейсы (Open API).

4) Экспертиза проектов в рамках регулятивной площадки Банка России в соответствии с приказом Банка России от 03.04.2018 № ОД-846 «Об утверждении Регламента организации и проведения Банком России моделирования процессов, связанных с предоставлением (применением) инновационных продуктов, услуг и технологий в банковской сфере и иных сферах финансового рынка».

Апробация инновационных финансовых технологий, продуктов и услуг в рамках регулятивной площадки Банка России проводится с учетом комплексного анализа риска информационной безопасности (киберриска), формирования моделей угроз, возникающих при их использовании.

В качестве ключевых RegTech-проектов в области информационной безопасности и киберустойчивости финансовых организаций предполагаются следующие:

- создание системы (среды доверия) внешней оценки выполнения требований по обеспечению защиты информации при осуществлении переводов денежных средств (оценка соответствия) посредством аккредитации организаций, проводящих оценку соответствия, контроля качества их деятельности, в первую очередь со стороны Банка России. Оценка соответствия предполагает проведение независимой оценки защищенности инфраструктуры и приложений по универсальному комплексу государственных стандартов;
- реализация инициатив по массовому применению криптографии на финансовом рынке для обеспечения безопасности обработки данных с использованием цифровых технологий во взаимодействии с уполномоченным органом в области обеспечения безопасности[8];
- обмен информацией организаций кредитно-финансовой сферы, а также иных организаций о киберугрозах посредством развития информационного обмена с ФинЦЕРТ Банка России, а также обеспечения функционирования системы мониторинга платежных и финансовых транзакций;
- многофакторная аутентификация клиентов финансовых организаций, в том числе с применением средств криптографической защиты информации, при проведении и подтверждении платежных и финансовых транзакций, формируемых в недоверенной среде (среда, не контролируемая финансовой организацией).

В качестве ключевых SupTech-проектов в области информационной безопасности и киберустойчивости финансовых организаций предполагаются следующие решения:

- создание системы «Антифрод» Банка России, обеспечивающей мониторинг транзакций в платежной системе Банка России, выявление признаков совершения перевода денежных средств без согласия участников платежной системы Банка России, получение подтверждения участниками, выявление признаков «вывода» денежных средств;
- осуществление Банком России надзора за выполнением финансовыми организациями требований в сфере информационной безопасности и киберустойчивости. В рамках данного направления предполагается осуществить нормативное закрепление обязанности представления финансовыми организациями в Банк России показателей, характеризующих объем неправомерных и несанкционированных клиентом операций по отношению к общему объему операций. Сбор данных в рамках оценки соответствия соблюдения требований в сфере информационной безопасности и киберустойчивости, а также проактивное выявление показателей операционной и финансовой стабильности является базовым подходом при осуществлении дистанционного надзора и, соответственно, определении уровня риска информационной безопасности (киберриска).

[8] *В рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», а также Положения Банка России от 09.06.2012 № 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».*

ПОДГОТОВКА КАДРОВ И ОБЕСПЕЧЕНИЕ ДОВЕРИЯ ГРАЖДАН К ЦИФРОВОЙ СРЕДЕ

Установление современных требований к обеспечению информационной безопасности в условиях цифровой реальности требует наличия компетентных кадров с соответствующей квалификацией.

Вместе с тем программы подготовки специалистов, а также уровень их подготовки не отвечают потребностям организаций кредитно-финансовой сферы, а кадры не обладают новыми базовыми «цифровыми» компетенциями.

В связи с этим Банк России планирует стать связующим звеном между высшими учебными заведениями и организациями кредитно-финансовой сферы для создания условий подготовки специалистов в области информационной безопасности нового типа.

На основе предложений организаций кредитно-финансовой сферы в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» планируется сформировать направления обучения и разработать соответствующие программы обучения:

- разработать профессиональный стандарт «Специалист в области информационной безопасности организаций кредитно-финансовой сферы»;
- определить потребность в специалистах по информационной безопасности организаций кредитно-финансовой сферы;
- подготовить предложения о внесении изменений в государственные образовательные стандарты высшего образования в части подготовки специалистов по информационной безопасности организаций кредитно-финансовой сферы;
- разработать примерную программу профессиональной переподготовки «Обеспечение информационной безопасности в организациях кредитно-финансовой сферы».

Дополнительно планируется разработать методики и программы аттестации специалистов и руководителей подразделений информационной безопасности (кибербезопасности) как в очной форме на базе Университета Банка России, так и в заочной форме (с использованием технологии удаленного доступа через сеть Интернет).

В целях повышения уровня вовлеченности сотрудников подразделений безопасности Банка России и организаций кредитно-финансовой сферы в процесс подготовки кадров планируется привлекать их для участия в учебном процессе в качестве преподавателей профильных кафедр ведущих высших учебных заведений.

Обеспечение доверия граждан к цифровой среде, а также кибербезопасности человека в цифровом мире будет строиться в рамках направления по повышению уровня финансовой грамотности и базовых компетенций по кибергигиене. Банк России планирует разработать образовательные программы для представителей финансовых организаций, студентов высших учебных заведений, школ и иных учебных заведений.

Создание киберлаборатории (киберполигона) для практического обучения кадров для кредитно-финансовой сферы и Банка России. Киберполигон планируется создать как платформу для моделирования инфраструктуры организаций кредитно-финансовой сферы в целях эмуляции кибератак для выработки мер противодействия и предупреждения, а также проведения обучающих мероприятий по направлению кибербезопасности.

Системная работа по повышению финансовой грамотности населения в части информирования граждан о правилах безопасности при пользовании платежными услугами (далее – фи-

нансовая киберграмотность) является задачей Департамента информационной безопасности Банка России (п. 2.2.1.5 Положения о Департаменте информационной безопасности). Недостаточный уровень знаний и навыков населения в области безопасного пользования электронными средствами платежа, а также постоянное появление новых приемов введения в заблуждение путем обмана или злоупотребления доверием с целью хищения средств, используемых злоумышленниками для получения незаконного доступа к счетам клиентов организаций кредитно-финансовой сферы, – основная причина роста количества и объема несанкционированных операций.

Департамент информационной безопасности является информационно-координационным хабом процессов и мероприятий по повышению финансовой киберграмотности населения и привлекает для решения этой задачи другие структурные подразделения Банка России, участников рынка, а также профильные федеральные органы исполнительной власти, в ведении которых находятся вопросы просвещения, социальной защиты и правоохранительной деятельности.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Глобальные угрозы в сфере кибербезопасности требуют от стран совместных усилий, так как носят трансграничный характер, меняют устоявшиеся бизнес-модели и рождают новые вызовы для международных экономических отношений.

Банк России в рамках международного сотрудничества в сфере информационной безопасности и киберустойчивости в качестве ключевой цели определяет компетентное участие в формировании актуальной и отвечающей российским интересам повестки дня.

Основными задачами становятся обмен информацией о киберугрозах, содействие внедрению единых стандартизированных подходов в области обеспечения кибербезопасности, а также выстраивание обмена опытом по регулированию и внедрению финансовых технологий.

Несмотря на геополитические факторы, Банк России участвует в международном взаимодействии, углубляя и расширяя его по следующим направлениям.

1) Обеспечение участия экспертов Банка России в деятельности международных организаций по вопросам кибербезопасности («Многостороннее сотрудничество»). Ключевыми площадками являются Международная организация по стандартизации (International Organization for Standardization, ISO), Международная электротехническая комиссия (International Electrotechnical Commission, IEC), Международный союз электросвязи (International Telecommunication Union, ITU), Международная организация комиссий по ценным бумагам (International Organization of Securities Commissions, IOSCO), Совет по финансовой стабильности (Financial Stability Board, FSB), Всемирный экономический форум (The World Economic Forum, WEF), Комитет по платежным и рыночным инфраструктурам Банка международных расчетов (Committee on Payments and Market Infrastructures, CPMI), Международная организация страхового надзора (International Organization of Insurance Supervisors, IAIS), Базельский комитет по банковскому надзору (Basel Committee on Banking Supervision, BIS). Кроме того, перспективным направлением сотрудничества является взаимодействие с партнерами в рамках форума БРИКС.

2) Взаимодействие с центральными (национальными) банками иностранных государств по вопросам обмена информацией о киберугрозах и укрепления кибербезопасности при предоставлении финансовых услуг («Двустороннее сотрудничество»). Ключевыми партнерами Банка России являются Банк Италии, Банк Испании, Центральный банк Турецкой Республики, Гражданский кооперативный банк Индии.

3) Взаимодействие с регуляторами государств – членов Евразийского экономического союза («Интеграционное сотрудничество») в целях координации деятельности подразделений безопасности регуляторов по созданию центров реагирования на компьютерные инциденты в национальных банках стран – членов ЕАЭС, гармонизации подходов к формированию требований к обеспечению информационной безопасности и киберустойчивости, а также платежного пространства в рамках ЕАЭС, созданию среды доверия.

4) Взаимодействие с международными командами реагирования на инциденты, проведение стресс-тестирований и киберучений (Международное сообщество команд реагирования на инциденты, Европейская команда по реагированию на инциденты, связанные с банкоматами, Корпорация по управлению доменными именами и IP-адресами, Международное сообщество команд реагирования на компьютерные инциденты, группы реагирования на компьютерные инциденты Израиля, Испании, Скандинавского региона, Болгарии, Индии, Нидерландов, Японии).

НАЦИОНАЛЬНАЯ ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА РОССИЙСКОЙ ФЕДЕРАЦИИ»

Эффективное развитие финансового рынка в цифровой экономике возможно только при наличии сформированных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность).

Одним из базовых направлений национальной программы «Цифровая экономика Российской Федерации» является информационная безопасность.

Цель направления – обеспечение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз.

Банк России является связующим звеном по вопросам информационной безопасности между организациями кредитно-финансовой сферы и уполномоченными органами в сфере информационной безопасности (ФСБ России, ФСТЭК России) и участвует в реализации федерального проекта «Информационная безопасность» по следующим направлениям:

- развитие значимых платежных систем и обеспечение их информационной безопасности и киберустойчивости (за счет использования в том числе российской криптографии);
- формирование подходов к обеспечению информационной безопасности и киберустойчивости инновационных технологий (искусственный интеллект, Big Data, киберфизические системы, распределенные реестры, Интернет вещей и другие);
- подготовка компетентных кадров в сфере информационной безопасности и киберустойчивости для организаций кредитно-финансовой сферы.

Использование российской криптографии в рамках развития значимых платежных систем и обеспечения их информационной безопасности и киберустойчивости является ключевым направлением деятельности Банка России[9].

Для этого при участии ФСБ России, кредитных организаций, субъектов национальной платежной системы планируется:

- снизить правовые и административные барьеры, препятствующие массовому применению криптографии на российском финансовом рынке;
- сформировать технологические карты переводов денежных средств, описывающие криптографические алгоритмы с указанием применяемых криптографических примитивов, с учетом деятельности международных платежных систем;
- разработать криптографические алгоритмы;
- разработать в соответствии с «дорожной картой» сертифицированные программные и технические средства, реализующие средства криптографической защиты информации;
- провести работу по сертификации программных и технических средств на соответствие требованиям международных платежных систем;
- создать центр тестирования технических средств и программного обеспечения.

Совершенствование механизмов правового регулирования информационной безопасности и киберустойчивости инновационных технологий, разработанных в рамках федерального проекта «Информационная безопасность», планируется осуществлять в рамках федерального проекта «Нормативное регулирование цифровой среды» национальной программы «Цифровая экономика Российской Федерации».

---

[9] *В целях реализации Указания Банка России от 07.05.2018 № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 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».*

ЦЕНТР КОМПЕТЕНЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЮ КИБЕРАТАКАМ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ

В соответствии с решением Совета Безопасности Российской Федерации от 15 января 2015 г. № ПР-73 был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (ФинЦЕРТ Банка России).

ФинЦЕРТ Банка России 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 кибергигиены.

8) Взаимодействие с операторами по переводу цифровых финансовых активов.

Целевыми индикаторами являются:

Наименование целевого индикатора	2018 г.	2020 г.
Уровень доверия[1]	60%	80%
Уровень (удельный вес) несанкционированных финансовых операций (транзакций) [2]	0,005%	0,005%

[1] Для расчета уровня доверия клиентов ФинЦЕРТ Банка России в декабре 2018 г. провел опрос кредитных организаций и клиентов (далее – Опрос). Опрос проводился путем анкетирования кредитных организаций и их клиентов. Каждая кредитная организация заполняла анкету на основании данных не менее 100 своих клиентов следующих категорий:

– не менее 20 анкет от юридических лиц;

– не менее 20 анкет от физических лиц каждой возрастной категории (по возрастным категориям: до 25 лет, 25–40 лет, 40–60 лет, свыше 60 лет).

Анкета клиентов в том числе содержала вопрос: «Насколько Вы (как клиент кредитной организации) доверяете безопасности предоставляемых Вам финансовых услуг?». Поскольку анкетирование клиентов проводилось непосредственно кредитными организациями, при расчете показателя уровня доверия клиентов использовался корректирующий (поправочный) коэффициент. Уровень доверия в 2018 г. составил 68,53%, что свидетельствует о достаточно высокой степени осведомленности о безопасности реализуемых электронных технологий и сервисов и превышает целевое значение индикатора.

[2] Уровень (удельный вес) несанкционированных финансовых операций (транзакций) рассчитывается как отношение суммы несанкционированных операций, совершенных с использованием платежных карт, к сумме операций, совершенных с использованием платежных карт.

НАДЗОРНАЯ ДЕЯТЕЛЬНОСТЬ

Реализация контрольно-надзорных полномочий Банка России строится с учетом лучшего мирового опыта, накопленного ведущими международными организациями, в том числе Советом по финансовой стабильности (FSB)[10].

Общие принципы контроля (надзора) в сфере информационной безопасности и киберустойчивости:

1) Получение объективных данных (метрик, показателей), характеризующих уровень риска информационной безопасности (киберриска), для управления риском информационной безопасности (киберриском) в каждой организации кредитно-финансовой сферы:

- реализация системы оценки соответствия (независимая оценка поднадзорных организаций на соответствие требованиям государственных стандартов: защита информации, непрерывность деятельности, управление рисками, аутсорсинг);
- система оценки качества выполнения требований к обеспечению надлежащего уровня защиты приложений. Проводится на основе анализа уязвимостей приложений, критичных с точки зрения наличия уязвимостей (сертификация приложения клиента и фронт-приложения);
- организация сбора исходных данных, которые характеризуют уровень риска по финансовым операциям, в рамках технологии сбора данных и применения технологии Big Data для проактивного выявления «точек сосредоточения риска»;
- развитие методологии с последующим нормативным закреплением практик стресс-тестирования (киберучений) организаций кредитно-финансовой сферы.

2) Разработка методологии расчета минимального размера финансового обеспечения, требуемого для покрытия потенциального ущерба от реализации киберриска (например, дополнительные требования к капиталу кредитных организаций, независимые гарантии, страхование).

3) Получение объективных данных (показателей, метрик) по финансовым потерям потребителей финансовых услуг и формирование на их основе стратегии защиты прав потребителей финансовых услуг.

4) Определение уровня финансовой стабильности финансового рынка Российской Федерации в целом на основе данных о рисках информационной безопасности (киберрисках).

Роль Банка России заключается также в продвижении на международной арене инновационных методик и подходов к формированию методологии контроля (надзора) в сфере информационной безопасности и киберустойчивости.

Целевым индикатором является формирование к 2021 г. объективной информации в отношении:

– уровня риска отдельных организаций кредитно-финансовой сферы;
– уровня готовности отдельных организаций кредитно-финансовой сферы противостоять кибератакам (с точки зрения обработки риска информационной безопасности (киберриска) и его финансового покрытия);

---

[10] *Пункты 9, 9.1 статьи 4 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (общий банковский надзор, контроль и надзор за деятельностью некредитных финансовых организаций); часть 11 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы).*

– уровня готовности кредитно-финансовой сферы противостоять киберугрозам путем агрегирования данных по уровню риска отдельных организаций кредитно-финансовой сферы и уровню готовности каждой из них противостоять кибератакам.