Банк России

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ НА ПЕРИОД 2023–2025 ГОДОВ

Москва
2023

ОГЛАВЛЕНИЕ

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов одобрены Советом директоров Банка России 22.05.2023.

Материал подготовлен Департаментом информационной безопасности.

Фото на обложке: Shutterstock/FOTODOM
107016, Москва, ул. Неглинная, 12
Официальный сайт Банка России: www.cbr.ru

ВВЕДЕНИЕ

Развитие информационной безопасности и киберустойчивости в организациях кредитно-финансовой сферы в 2019–2021 годах осуществлялось в рамках реализации четырех ключевых задач, предусмотренных Основными направлениями развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов (далее – Основные направления 2019–2021). Основные направления 2019–2021 утверждены протоколом заседания Совета директоров Банка России от 6 сентября 2019 года № 23.

В ходе реализации Основных направлений 2019–2021 достигнуты следующие результаты:

1. Задача «Обеспечение информационной безопасности и киберустойчивости в целях финансовой стабильности каждой организации финансового рынка»:

- сформированы пропорциональные регуляторные требования по защите информации при предоставлении банковских услуг, осуществлении деятельности в сфере финансовых рынков, осуществлении переводов денежных средств в платежной системе Банка России;
- организован надзорный процесс по вопросам защиты информации:
  - обеспечен регулярный расчет риск-профиля в отношении всех кредитных организаций, крупных некредитных финансовых организаций. Показатели риск-профиля включены в композитный риск-профиль финансовых объединений;
  - реализован на системной основе дистанционный и контактный надзор;
  - разработана методология, в соответствии с которой на регулярной основе проводятся киберучения;
- отсутствуют факты нарушения финансовой стабильности в результате реализации успешных компьютерных атак.

2. Задача «Обеспечение операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы»:

- сформированы пропорциональные регуляторные требования для всех поднадзорных организаций кредитно-финансовой сферы, в том числе закреплены полномочия Банка России по установлению требований к операционной надежности, определены требования к операционной надежности для кредитных и некредитных финансовых организаций;
- обеспечен регулярный расчет риск-профиля в отношении всех кредитных организаций, крупных некредитных финансовых организаций по вопросам операционной надежности;
- вопросы операционной надежности интегрированы в вопросы управления операционным риском.

В рамках реализации Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов (далее – Основные направления 2023–2025) будет продолжена работа по реализации надзорных мероприятий по вопросам операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы.

3. Задача «Противодействие компьютерным атакам, в том числе при использовании инновационных финансовых технологий»:

- сформированы пропорциональные регуляторные требования по вопросам защиты информации и операционной надежности в отношении новых участников финансового рынка

(оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов, оператор финансовой платформы, оператор инвестиционной платформы);

- реализованы требования по защите информации для ключевых инфраструктурных проектов финансового рынка: Единая биометрическая система, Система быстрых платежей, платежная система Банка России, Система передачи финансовых сообщений;
- реализован информационный обмен Центра взаимодействия и реагирования Департамента информационной безопасности Банка России (ФинЦЕРТ) со всеми поднадзорными Банку России организациями кредитно-финансовой сферы по вопросам противодействия компьютерным атакам. Количество организаций – участников информационного обмена превысило 800. ФинЦЕРТ выполняет функции отраслевого центра по взаимодействию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- отсутствуют системные сбои на финансовом рынке в результате реализации успешных компьютерных атак.

4. Задача «Защита прав потребителей финансовых услуг»:

- реализованы правовые, организационные и технологические условия противодействия совершению операций по переводу денежных средств без согласия клиентов;
- созданы правовые основы по внесудебному ограничению доступа на территории Российской Федерации к ресурсам в сети Интернет, используемым для совершения мошеннических действий. Разработан механизм блокировки сайтов в рамках взаимодействия Банка России и Генеральной прокуратуры Российской Федерации. Время блокировки сайтов сокращено с нескольких недель до нескольких суток;
- реализованы мероприятия по повышению уровня киберграмотности различных категорий населения: разработаны и размещены на объектах транспортной и социальной инфраструктуры информационно-просветительские материалы, проведены обучающие мероприятия для талантливых детей и молодежи на базе образовательного центра «Сириус», а также кибердиктант и финансовый онлайн-зачет;
- сформированы требования к подготовке кадров в сфере информационной безопасности: определена потребность в кадрах, реализована программа практико-ориентированного обучения по информационной безопасности «КиберКурс» для 7 тыс. специалистов, заключены соглашения с высшими учебными заведениями и проведена экспертиза образовательных программ по подготовке бакалавров, специалистов и магистров по информационной безопасности в кредитно-финансовой сфере.

В рамках реализации Основных направлений 2023–2025 будет продолжено выполнение мероприятий, связанных с противодействием социальной инженерии на банковском рынке.

За время реализации Основных направлений 2019–2021 заключено 11 соглашений (меморандумов) по вопросам обмена опытом и укрепления безопасности при предоставлении финансовых услуг; создана рабочая группа по информационной безопасности БРИКС; организован обмен информацией с государствами – членами ЕАЭС и БРИКС, а также командами реагирования на инциденты; обеспечено участие экспертов Банка России в работе международных организаций по вопросам кибербезопасности.

Кроме того, обеспечено достижение целевых индикаторов, определенных Основными направлениями 2019–2021:

УРОВЕНЬ ДОВЕРИЯ *Табл. 1*
(%)

	План	**Факт**
2018 год	60	70,9
2021 год	60	58,5*

** Методика расчета показателя скорректирована. Значение показателя по результатам 2021 года составило 73,32%.*

УРОВЕНЬ НЕСАНКЦИОНИРОВАННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ *Табл. 2*
(%)

	План	**Факт**
2018 год	0,005	0,0023
2021 год	0,005	0,0013

ВОЗМОЖНОСТИ И ВЫЗОВЫ ДЛЯ РАЗВИТИЯ РОССИЙСКОГО ФИНАНСОВОГО РЫНКА

В контексте текущих тенденций выделяется несколько вызовов, которые меняют традиционные подходы к построению информационной безопасности в кредитно-финансовой сфере:

- операционная надежность и защита информации в условиях снижения риска технологической зависимости организаций кредитно-финансовой сферы и инфраструктуры от внешних контрагентов;
- защита прав потребителей финансовых услуг в рамках снижения доли операций, совершаемых без согласия клиентов;
- повышение уровня доверия к финансовым услугам в условиях быстрого развития технологий.

Потенциал технологий, в том числе платежных и финансовых, является одним из факторов развития и преодоления возникающих вызовов.

Цели и основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов сохраняют преемственность с Основными направлениями 2019–2021.

При разработке Основных направлений 2023–2025 учтены следующие документы стратегического планирования:

- 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;
- Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400;
- Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденные Указом Президента Российской Федерации от 12.04.2021 № 213;
- Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 годы, утвержденная распоряжением Правительства Российской Федерации от 25.09.2017 № 2039-р;
- Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов;
- Стратегия развития национальной платежной системы на 2021–2023 годы;
- Основные направления развития системы управления данными Банка России на 2022–2024 годы;
- Приоритетные направления повышения доступности финансовых услуг в Российской Федерации на период 2022–2024 годов;
- проект Основных направлений цифровизации финансового рынка на период 2023–2025 годов;
- План мероприятий («дорожная карта») в сфере SupTech и RegTech в Банке России до 2023 года.

Основные направления 2023–2025 определяют следующие ключевые цели развития информационной безопасности кредитно-финансовой сферы:

- защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям;

- создание условий для безопасного внедрения цифровых и платежных технологий и обеспечения технологического суверенитета;
- обеспечение контроля рисков информационной безопасности, операционной надежности для непрерывности оказания банковских и финансовых услуг.

Достижение указанных целей неразрывно связано с соблюдением баланса интересов граждан, бизнеса и государства при реализации Основных направлений 2023–2025.

Чтобы вести мониторинг осуществления целей развития информационной безопасности, сформирован набор комплексных индикаторов:

Наименование индикатора	2021 год	2022 год	2025 год
Степень удовлетворенности населения уровнем безопасности финансовых услуг, оказываемых организациями кредитно-финансовой сферы	58,5%	62,6%	Не ниже 70%
Доля необходимых для внедрения цифровых и платежных технологий мероприятий по информационной безопасности, которые выполняются в срок	–	–	Не менее 90%
Доля системно значимых кредитных организаций и крупных финансовых организаций, у которых в течение календарного года отсутствовали инциденты информационной безопасности и операционной надежности, влияющие на достижение показателей операционной надежности в части непрерывности оказания финансовых услуг	–	–	Не менее 95%

Реализация Основных направлений 2023–2025 будет осуществляться при взаимодействии с федеральными органами исполнительной власти, организациями кредитно-финансовой сферы, экспертным и научным сообществами.

1. ЗАЩИТА ПРАВ ПОТРЕБИТЕЛЕЙ ФИНАНСОВЫХ УСЛУГ И ПОВЫШЕНИЕ УРОВНЯ ДОВЕРИЯ К ЦИФРОВЫМ ТЕХНОЛОГИЯМ

В 2022 году объем операций без согласия клиентов увеличился по сравнению с 2021 годом (+4,29%) и составил 14 165,44 млн рублей. Рост происходил на фоне активного развития новых дистанционных платежных и финансовых сервисов, а также увеличения (+39%, до 1458,6 трлн руб.) объема денежных переводов с использованием электронных средств платежа. Благодаря расширению комплекса мер, которые банки принимают для противодействия мошенничеству, количество операций без согласия клиентов в 2022 году снизилось по сравнению с 2021 годом (-15,31%) и составило 876,59 тыс. единиц.

В 2022 году доля объема операций без согласия клиентов в общем объеме операций по переводу денежных средств составила 0,00097% (в 2021 году – 0,00130%). Эти значения не превышают как установленный Банком России целевой показатель доли таких операций в общем объеме операций (0,005%), совершенных с использованием платежных карт, так и аналогичный показатель Европейской службы банковского надзора (EBA)[1].

Как показывают результаты анализа, существенная доля хищений совершается в результате использования мошенниками приемов и методов социальной инженерии, то есть манипулирования людьми с целью получения личных и финансовых данных. Вместе с тем доля таких хищений увеличилась на 1% по сравнению с 2021 годом и составляет 50,4%.

1.1. Противодействие совершению операций без согласия клиентов, социальной инженерии

В рамках противодействия совершению операций без согласия клиентов, социальной инженерии планируется реализовать следующие мероприятия:

- **Совершенствование механизмов сохранения и возврата денежных средств в части:**
  - возврата денежных средств с учетом фактических значений показателей и критериев эффективности антифрод-процедур в кредитных организациях;
  - ограничения удаленного доступа к электронным средствам платежа;
  - повышения качества антифрод-процедур в кредитных организациях;
  - снижения рисков манипулирования процедурой возврата денежных средств со стороны клиентов;
  - противодействия дропперам (создание условий, при которых экономически нецелесообразно и невыгодно совершать хищения денежных средств);
  - повышения качества заполняемости сведений о реквизитах получателей денежных средств по операциям без согласия клиентов.
- **Информационный обмен с МВД России сведениями из базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиентов.** Предусматривается совершенствование оперативного взаимодействия и обмена информацией, имеющейся в распоряжении Банка России и МВД России, координация работ по выявлению цепочек вывода денежных средств, а также реализация механизма ограничения банками доступа к счетам, если информация об операциях содержится в базах данных Банка России и МВД России о совершенных противоправных действиях.

Дополнительно планируется проработать вопрос повышения качества информации из базы данных Банка России (фидов) с учетом следующих подходов:

- автоматизация и онлайн-обработка запросов на исключение из базы данных Банка России (фидов);

[1] 0,005% (5 евроцентов на 1000 евро переводов).

- учет результатов, связанных с оценкой кредитными организациями информации из базы данных Банка России (фидов) при рассмотрении обращений по операциям без согласия клиентов;
- развитие централизованных сервисов дистрибуции данных по атрибуции, вовлеченных в осуществление операций без согласия клиентов (фидов), до уровня сервисов репутации по хозяйствующим субъектам с учетом данных, содержащихся в инфраструктуре операционных центров операторов платежных систем;
- интеграция цифровых отпечатков устройств в состав данных об операциях без согласия клиентов (фидов).

• **Дополнение механизмов оценки операционных рисков кредитных организаций показателями качества антифрод-процедур.** Планируется установить в составе требований к управлению операционным риском контрольные показатели уровня риска информационной безопасности, включая следующие показатели, характеризующие долю (по количеству и сумме денежных средств):

- операции без согласия клиентов (фродовые операции) в общем объеме операций по переводу денежных средств;
- операции, в отношении которых кредитной организацией ошибочно приостановлено исполнение распоряжения об операции, в общем объеме операций без согласия клиентов (фродовых операций);
- операции, в отношении которых кредитной организацией ошибочно не приостановлено исполнение распоряжения об операции, в общем объеме операций без согласия клиентов (фродовых операций).

• **Развитие каналов юридически значимых обращений в правоохранительные органы (Единый портал государственных и муниципальных услуг, системы дистанционного банковского обслуживания).** Это послужит сокращению временны́х издержек, негативно влияющих на ход расследования мошеннических действий, поскольку совершенствование процедур возбуждения уголовного дела является ключевым элементом обеспечения необходимого уровня защиты интересов клиентов кредитных организаций в условиях масштабного распространения социальной инженерии.

• **Обеспечение возможности применения персональных мер ответственности в отношении должностных лиц за нарушение законодательства в сфере защиты персональных данных.** Мера направлена на предотвращение утечек сведений, содержащих персональные данные и (или) банковскую тайну. Планируется нормативно закрепить квалификационные требования, а также требования к деловой репутации должностных лиц организаций кредитно-финансовой сферы, отвечающих за вопросы информационной безопасности и защиты информации.

• **Повышение безопасности при предоставлении кредита (займа) онлайн.** Рост доступности финансовых услуг и переход на дистанционные каналы их получения создают существенные риски развития практик мошенничества при получении потребительских займов (кредитов) третьими лицами с использованием методов социальной инженерии. Для снижения указанных рисков планируется реализовать механизм, предусматривающий право гражданина установить (снять) в своей кредитной истории запрет на заключение с ним договора потребительского займа (кредита) путем подачи в любую кредитную организацию или квалифицированное бюро кредитных историй соответствующего заявления.

• **Развитие процедур идентификации и антифрод-процедур в микрофинансовых организациях** для обеспечения защиты информации и борьбы с противоправными действиями при получении услуг микрофинансовых организаций.

• **Развитие взаимодействия финансовых организаций с операторами связи и телематических услуг по противодействию социальной инженерии по вопросам обмена информацией о клиентах (абонентах)** для снижения рисков совершения операций без согласия клиентов с использованием приемов и методов социальной инженерии, в том числе с использованием

услуг операторов связи. Также планируется проработка вариантов использования клиентских сервисов безопасного пользования услугами операторов связи, включая:

- сервисы определителя номера телефона и голосового помощника;
- сервисы категорирования коммуникаций абонентов услуг связи;
- сервисы, информирующие клиента (до осуществления перевода денежных средств) о наличии признаков операции без согласия клиента, фишинговом и мошенническом ресурсе.

- **Совершенствование анализа новостного фона для оценки рисков поднадзорных организаций.** Банк России планирует выработать подходы к оценке информационного фона, или сентимент (англ. sentiment – настроение), по вопросам информационной безопасности, операционной надежности, противодействия совершению операций без согласия клиентов с использованием методов социальной инженерии и степени его влияния на деятельность организаций кредитно-финансовой сферы и поведение потребителей финансовых услуг. Наличие такой информации позволит оперативнее выявлять тенденции в финансовой сфере, а также прогнозировать модели поведения потребителей финансовых услуг. Для этого планируется разработать и внедрить процессы сбора, обработки и анализа информации, получаемой из разных источников, включая средства массовой информации, социальные сети, публикации, в том числе в мессенджерах.

1.2. Противодействие компьютерным атакам

В рамках направления по противодействию компьютерным атакам планируется реализовать следующее:

- **Формирование и совершенствование информационного обмена между Банком России и финансовыми организациями по тактике, технике совершения компьютерных атак.** Это необходимо в том числе для целей формирования сценариев проведения киберучений, сокращения времени реагирования на компьютерные атаки. Чтобы повысить эффективность реагирования на компьютерные атаки, цепочки компьютерных атак и качество расследования киберинцидентов, планируется дальнейшее развитие информационного взаимодействия ФинЦЕРТ с организациями кредитно-финансовой сферы. Для этого будет проведена доработка форм и порядка обмена информацией о случаях и попытках осуществления переводов денежных средств без согласия клиентов.

Планируется продолжить дорабатывать техническую инфраструктуру ФинЦЕРТ, используемую для информирования участников кредитно-финансовой сферы, в целях реализации новых подходов к форме предоставления данных. Это позволит повысить скорость взаимодействия и своевременно (в том числе превентивно) реагировать на компьютерные атаки.

Кроме того, предусмотрена разработка алгоритмов формирования информационных бюллетеней ФинЦЕРТ и сценариев атак для киберучений.

- **Развитие информационного обмена ФинЦЕРТ с организациями кредитно-финансовой сферы для противодействия компьютерным атакам.** Банк России продолжит дорабатывать техническую инфраструктуру ФинЦЕРТ, выполняющего функции «отраслевого» центра ГосСОПКА, используемую для информирования участников кредитно-финансовой сферы в целях реализации новых подходов к форме предоставления данных. Это позволит повысить скорость взаимодействия и реагирования на компьютерные атаки.
- **Реализация некредитными финансовыми организациями, являющимися крупными инфраструктурными организациями финансового рынка и субъектами критической информационной инфраструктуры, мер по противодействию целевым компьютерным атакам в зависимости от уровня опасности.** В целях обеспечения непрерывности оказания финансовых услуг Банк России продолжит формирование и актуализацию требований (в рамках операционной надежности) для некредитных финансовых организаций, являющихся субъектами критической информационной инфраструктуры, по противодействию целевым компьютерным

атакам в зависимости от уровня опасности, установленного федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

1.3. Финансовая киберграмотность

В рамках мероприятий по развитию финансовой киберграмотности планируется реализовать:

- **Программы по повышению финансовой киберграмотности и пропаганде кибергигиены для различных категорий населения, в том числе для лиц с низким уровнем дохода и социально незащищенных категорий населения.** В рамках обеспечения возможности безопасного получения финансовых услуг Банк России планирует уделять особое внимание формированию и продвижению базовых навыков и установок по финансовой киберграмотности и кибергигиене среди социально уязвимых категорий населения. Для этого будут реализованы как информационно-просветительские, так и образовательные мероприятия с применением современных педагогических технологий и форматов продуктивного, дифференцированного обучения, а также с реализацией компетентностного подхода и развивающего обучения.

Развитие кадрового потенциала, в частности включение подрастающего и старшего поколений в информационно-просветительскую и образовательную работу, потребует разработки образовательного контента и привлечения добровольцев финансовой киберграмотности и кибергигиены. Это позволит сформировать сеть социальных контактов для продвижения базовых навыков и установок по финансовой киберграмотности и кибергигиене среди целевых категорий населения.

Разработку информационно-просветительского контента по информированию граждан о мошеннических схемах и лицах, их применяющих, Банк России планирует строить на основе анализа данных. Для этого будет осуществлен переход к системному использованию методов продвинутой аналитики данных об инцидентах защиты информации и результатах их расследования.

- **Применение Единой рамки компетенций по финансовой грамотности (далее – Единая рамка) в вопросах повышения финансовой киберграмотности и кибергигиены.** Единая рамка содержит базовые компетенции по финансовой грамотности для учащихся школьного возраста (от 15 лет), взрослого населения и является основой для развития различных инструментов повышения финансовой грамотности (включая вопросы финансовой киберграмотности и кибергигиены): образовательные программы, программы дополнительного образования, олимпиады и так далее. Единая рамка описывает общие разделы и образовательные результаты по темам на двух уровнях: базовом и продвинутом.

Целью является формирование необходимых компетенций и навыков у граждан Российской Федерации в области финансовой киберграмотности и кибергигиены, способствующих безопасному использованию финансовых продуктов и услуг.

На основании Единой рамки будут разрабатываться информационно-просветительские материалы, программы и курсы по финансовой киберграмотности и кибергигиене.

Приоритетной задачей является закрепление и реализация во всех информационно-просветительских и образовательных инициативах базовых и продвинутых компетенций в области финансовой киберграмотности и кибергигиены по трем категориям:

- осведомленность, знание и понимание;
- уверенность, мотивация и позиция;
- навыки и поведение.

Для педагогических работников, включающих в образовательные программы вопросы финансовой киберграмотности и кибергигиены, планируется проведение методических мероприятий, практико-ориентированного обучения с изучением приемов и методов противодействия социальной инженерии на финансовом рынке.

- **Размещение социальной рекламы, просветительского контента и программ о противодействии социальной инженерии и повышении финансовой киберграмотности населения.** Банк России совместно с Правительством Российской Федерации, субъектами Российской Федерации планирует продолжить разработку информационно-просветительских материалов (визуальный, аудио-, видеоконтент) для распространения на объектах транспортной и социальной инфраструктуры, а также освещение тематики финансовой киберграмотности и кибергигиены в средствах массовой информации федерального, регионального и местного уровней. При формировании контента будут приняты во внимание социально-психологические особенности различных категорий населения, связанные с восприятием такой информации.

Разработка и регулярная актуализация информационно-просветительского контента будут строиться на основе глубокой аналитики данных о мошеннических схемах и лицах, их применяющих. Кроме того, будет сформировано экспертное сообщество, создающее синергетический эффект от обмена знаниями, практиками в области разработки и адаптации контента с учетом когнитивных способностей и особенностей поведения и восприятия информации различными категориями граждан Российской Федерации.

- **Усиление финансовыми организациями информационной работы, направленной на повышение осмотрительности клиентов в отношении сохранности личных и финансовых данных.** Планируется расширить использование кредитными организациями инструментов информационной работы, направленных на повышение осмотрительности их клиентов при совершении финансовых операций, в том числе переводов денежных средств.

С учетом анализа поведенческого опыта получателей финансовых услуг будут актуализированы и при необходимости нормативно закреплены новые подходы к доведению до клиентов – получателей финансовых услуг информации о возможных рисках несанкционированного доступа к личной и финансовой информации, а также совершения операций без согласия клиентов с использованием методов социальной инженерии.

2. СОЗДАНИЕ УСЛОВИЙ ДЛЯ БЕЗОПАСНОГО ВНЕДРЕНИЯ ЦИФРОВЫХ И ПЛАТЕЖНЫХ ТЕХНОЛОГИЙ И ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА

Активное развитие цифровых технологий значительно изменило потребности и ожидания получателей финансовых услуг. Клиенты становятся более требовательными, и большое значение приобретает потребительский опыт, который напрямую связан с цифровизацией и использованием технологий. Клиентов интересует возможность дистанционного получения широкого спектра услуг, охватывающих все сферы жизнедеятельности; они отдают предпочтение удобным, простым и быстрым сервисам, для получения которых не нужно повторно проходить авторизацию и вводить свои личные данные.

Однако ускоренное развитие технологий создает и существенные риски кибератак на клиентов и финансовые организации, а также мошенничества на финансовом рынке.

2.1. Развитие регулирования

Банк России планирует сформировать условия для обеспечения информационной безопасности и киберустойчивости цифровых и платежных технологий через регулирование и последующий надзор по следующим приоритетным направлениям:

- цифровой профиль;
- маркетплейс;
- открытые интерфейсы на финансовом рынке (Open API), открытые банковские интерфейсы в национальной платежной системе, а также интерфейсы небанковских поставщиков платежных услуг;
- электронное хранение документов;
- экосистемы;
- Единая информационная система проверки сведений об абоненте (ЕИС ПСА);
- обеспечение информационной безопасности для новых способов инициирования платежей и переводов (смарт-устройства и другие);
- Единая биометрическая система и коммерческие биометрические системы;
- новые субъекты национальной платежной системы (небанковские поставщики платежных услуг и другие);
- оборот данных организаций кредитно-финансовой сферы в части их информационной безопасности, включая целостность;
- среда доверия при удаленном предоставлении финансовых услуг и программ для реализации протоколов информационной безопасности.

В рамках дальнейшего совершенствования регулирования будут реализованы инициативы, связанные с формированием правовых механизмов обеспечения информационной безопасности и киберустойчивости в области цифровых и платежных технологий. В целях проведения единой государственной политики в сфере информационной безопасности и киберустойчивости указанные подходы будут согласованы с ФСБ России и ФСТЭК России.

Банк России планирует расширить набор надзорных инструментов и практик, учитывающих принцип соразмерности и разумности для надлежащего выполнения поднадзорными организациями кредитно-финансовой сферы требований по защите информации и операционной надежности.

Банк России продолжит мониторинг международной повестки по вопросам обеспечения информационной безопасности и киберустойчивости цифровых и платежных технологий, используя данный процесс в том числе для защиты национальных интересов при формировании международных подходов к техническим и технологическим процессам обеспечения инфор-

мационной безопасности и киберустойчивости, а также продвижения лучших российских подходов и практик.

Важной задачей остается развитие практических навыков сотрудников подразделений информационной безопасности по реагированию на компьютерные атаки и расследованию киберинцидентов в отношении цифровых и платежных технологий. Развитие практических навыков планируется осуществлять в рамках программы практико-ориентированного обучения.

2.2. Развитие национальной платежной инфраструктуры и цифровой рубль

Банк России продолжит формировать условия для внедрения инновационных продуктов и сервисов с учетом поддержания среды доверия между участниками платежной отрасли за счет определения стандартов информационной безопасности, обеспечивающих непрерывность осуществления переводов денежных средств, доступность платежных сервисов, а также снижение потерь участников финансового рынка от действий мошенников, включая социальную инженерию.

Приоритетными направлениями являются:

- развитие стандартов информационной безопасности, обеспечивающих расширение доступа к платежной системе Банка России, в том числе нерезидентов;
- развитие Системы быстрых платежей (СБП) в части:
  - внедрения механизмов информационной безопасности для интероперабельности СБП, в том числе интеграция национальных СБП государств – членов ЕАЭС с российской СБП;
  - расширения доступа к СБП, в том числе нерезидентов;
  - развития системы управления рисками информационной безопасности;
  - обеспечения информационной безопасности и надежности мобильного приложения СБПэй;
- развитие Системы передачи финансовых сообщений (СПФС) по следующим направлениям:
  - совершенствование стандартов информационной безопасности, обеспечивающих расширение участия нерезидентов;
  - обеспечение информационной безопасности при внедрении новых сервисов в СПФС;
  - развитие института сервис-бюро в части механизмов информационной безопасности;
  - реализация интернет-доступа к СПФС;
  - поддержка стандартов ИБ ISO 20022 в СПФС.

В целях развития трансграничных платежей в национальной валюте, повышения роли российского рубля и его продвижения за пределами Российской Федерации, а также поддержки экспорта платежных услуг в другие страны Банк России планирует развивать вопросы информационной безопасности и киберустойчивости для доступа к сервисам платежной системы Банка России, СБП, СПФС банкам стран ЕАЭС и иным организациям – нерезидентам Российской Федерации.

- Цифровой рубль:
  - определение требований к защите информации, предъявляемых к участникам платформы цифрового рубля, и сопровождение участников платформы цифрового рубля по вопросам обеспечения информационной безопасности;
  - создание правовой и организационной основы для выстраивания механизмов оценки соответствия, контроля устойчивости к актуальным угрозам и тестирования применяемых технологий, алгоритмов, технических и программных средств в части вопросов информационной безопасности;

– развитие антифрод-механизмов (мониторинг операций с целью выявления аномалий, указывающих на возможные мошеннические действия, а также компрометацию участников платформы цифрового рубля) с учетом специфики операций в цифровых рублях.

Для использования цифровой финансовой инфраструктуры участниками финансового рынка Банк России продолжит формировать условия для безопасного внедрения финансовыми организациями цифровых и платежных технологий в рамках следующих проектов:

- развитие новых способов идентификации и аутентификации;
- развитие удаленной идентификации для резидентов и нерезидентов;
- развитие цифровых финансовых активов, утилитарных цифровых прав, краудфандинга;
- повышение доступности применения электронной подписи для массового сегмента;
- создание оператора автоматизированной информационной системы страхования (АИС страхования), поддержка бюро страховых историй;
- развитие взаимодействия организаций кредитно-финансовой сферы с федеральными органами исполнительной власти, включая доступ к государственным информационным системам (в том числе Единая биометрическая система (ЕБС), единая система идентификации и аутентификации (ЕСИА), «Госключ»).

Банк России планирует продолжить формирование требований к информационной безопасности и киберустойчивости цифровых и платежных технологий с учетом актуальных киберугроз и рисков, а также мониторинг фактического уровня защищенности и киберустойчивости реализуемых проектов. Требования, методология и практические инструменты информационной безопасности и киберустойчивости цифровых и платежных технологий будут разрабатываться во взаимодействии с федеральными органами исполнительной власти, организациями кредитно-финансовой сферы с учетом принципов разумной централизации и максимальной автоматизации процессов обмена информацией.

2.3. Экспериментальные правовые режимы и регулятивная «песочница»

Банк России продолжит проводить исследование инновационных финансовых продуктов, предложенных участниками рынка, на предмет информационной безопасности и киберустойчивости в рамках регулятивной «песочницы», а также формировать подходы к обеспечению информационной безопасности и киберустойчивости при пилотировании новых инновационных продуктов, услуг и технологий в банковской сфере и иных сферах финансового рынка.

Апробацию инновационных финансовых технологий, продуктов и услуг в рамках регулятивной площадки Банка России планируется проводить с учетом комплексного анализа риска информационной безопасности (киберриска). Аналогичный подход будет применяться к новым бизнес-моделям и решениям в рамках экспериментальных правовых режимов. Кроме того, планируется развитие инструментов мониторинга инцидентов информационной безопасности в рамках указанных режимов.

По результатам рассмотрения финансовых продуктов в регулятивной «песочнице» или их пилотирования в экспериментальных правовых режимах Банк России продолжит работу по совершенствованию правового регулирования в области информационной безопасности и киберустойчивости.

2.4. Технологический суверенитет

В целях снижения риска технологической зависимости финансовых организаций и инфраструктуры от внешних поставщиков Банк России будет осуществлять координацию деятельности организаций кредитно-финансовой сферы. Для этого в Банке России создан от-

раслевой центр компетенций (тестирования) для финансового сектора экономики, который обеспечит контроль рисков применения иностранных информационных технологий и их импортозамещение с учетом следующих подходов:

- определение приоритетов импортозамещения по номенклатуре программного и аппаратного обеспечения;
- реализация механизма оценки зрелости решений российских производителей и поставщиков информационных технологий;
- определение вариантов обработки рисков использования иностранных информационных технологий;
- распределение задач по техническому тестированию среди организаций кредитно-финансовой сферы, а также обобщение и раскрытие полученных результатов тестирования;
- осуществление взаимодействия с ответственными федеральными органами исполнительной власти, российскими производителями и поставщиками информационных технологий;
- обмен опытом по данной тематике, в том числе с организациями из иных отраслей экономики;
- формирование консолидированного запроса кредитно-финансовой сферы ответственным федеральным органам исполнительной власти на приобретение или разработку отечественных информационных технологий в интересах организаций кредитно-финансовой сферы, в частности для формирования целевого финансирования лидеров рынка по отдельным направлениям технологического суверенитета, максимально полно соответствующих потребностям кредитно-финансовой сферы;
- распределение и реализация выполнения технических функций тестирования ИТ-решений с использованием ресурсов организаций кредитно-финансовой сферы;
- осуществление контроля за реализацией вопросов импортозамещения в рамках действующих полномочий Банка России по обеспечению операционной надежности.

Важной задачей в вопросах технологического суверенитета станет обеспечение информационной безопасности, в том числе с использованием российских криптографических средств в значимых платежных системах. Для этого планируется:

- организовать тестирование кредитными организациями российских аппаратных модулей безопасности, предназначенных для использования в карточных платежных системах;
- внести изменения в правила платежных систем в целях реализации требований, установленных Положением Банка России от 04.06.2020 № 719-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».

Банк России планирует участвовать в разработке федеральными органами исполнительной власти требований информационной безопасности, предъявляемых к субъектам критической информационной инфраструктуры, которые являются организациями кредитно-финансовой сферы.

3. ОБЕСПЕЧЕНИЕ КОНТРОЛЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОПЕРАЦИОННОЙ НАДЕЖНОСТИ ДЛЯ НЕПРЕРЫВНОСТИ ОКАЗАНИЯ БАНКОВСКИХ И ФИНАНСОВЫХ УСЛУГ

Создавая условия для безопасного оказания финансовых услуг, в том числе с использованием инновационных цифровых и платежных технологий, Банк России учитывает общие надзорные тенденции как для финансового сектора, так и для сферы информационных технологий и информационной безопасности. Задачи Банка России – обеспечение непрерывности предоставления банковских и финансовых услуг (обеспечение операционной надежности) и контроль рисков информационной безопасности для выявления на ранних стадиях рисков, которые могут повлиять на финансовую устойчивость организаций кредитно-финансовой сферы.

3.1. RegTech- и SupTech-проекты

В ходе мероприятий по развитию RegTech- и SupTech-проектов планируется реализовать следующее:

- **Совершенствование системы внешнего аудита информационной безопасности.** Обеспечение качества оценки соответствия защиты информации в организациях кредитно-финансовой сферы определено в составе инициативы в рамках Основных направлений развития технологий SupTech и RegTech на период 2021–2023 годов.

При разработке концепции совершенствования системы внешнего аудита информационной безопасности планируется проработать вопрос создания дополнительных правовых механизмов повышения качества оценки соответствия защиты информации в организациях кредитно-финансовой сферы и роста качества услуг проверяющих организаций. Данные механизмы будут использованы при формировании требований к обеспечению достоверности результатов внешнего аудита посредством привлечения к нему проверяющих организаций, имеющих подтверждение соответствия их деятельности национальным стандартам, идентичным международным.

Систему внешнего аудита планируется реализовать в отношении:

- аудита по вопросам защиты информации и операционной надежности;
- аудита поставщиков облачных сервисов;
- аудита безопасности приложений.

- **Внедрение системы мониторинга и анализа операционных рисков кредитных организаций.** Планируется реализовать комплекс мероприятий по мониторингу и анализу рисков информационной безопасности в составе операционных рисков в соответствии с Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

Важным направлением станет качественный переход к системному использованию методов продвинутой аналитики для анализа операционных рисков кредитных организаций с учетом данных, формируемых в рамках мероприятий:

- по результатам анализа инцидентов информационной безопасности и операционной надежности;

- по расчету риск-профиля организаций кредитно-финансовой сферы и финансовых объединений;
- по надзору, в том числе в форме киберучений;
- по анализу данных, получаемых в рамках форм отчетности по тематике управления операционным риском и обеспечения операционной надежности.

Банк России планирует интегрировать результаты мониторинга и анализа операционных рисков кредитных организаций в оценку экономического положения, планов восстановления финансовой устойчивости, а также качества внутренних процедур оценки достаточности капитала (ВПОДК) кредитных организаций в части:

- риска информационной безопасности;
- риска информационной безопасности, связанного с возможным совершением операций без согласия клиентов;
- риска информационной безопасности, связанного с возможным нарушением операционной надежности.

Дополнительно будут проработаны вопросы разработки, тестирования и последующей корректировки методики оценки возможностей поднадзорных организаций кредитно-финансовой сферы выявлять инциденты информационной безопасности и операционной надежности, реагировать на них и восстанавливаться в случае их реализации, а также методики оценки организации системы управления рисками информационной безопасности и операционной надежности.

- **Создание правовых условий для аутсорсинга информационных технологий и использования облачных услуг финансовыми организациями** (подробнее – см. подраздел 3.4).

3.2. Киберучения

Банк России планирует продолжить развитие надзорного стресс-тестирования организаций кредитно-финансовой сферы с целью обеспечения информационной безопасности и операционной надежности в рамках расширения перечня сценариев, вопросов и задач, рассматриваемых при проведении киберучений.

Реализация данного направления позволит обеспечить контроль операционных рисков организаций кредитно-финансовой сферы по указанным направлениям в условиях перехода к технологическому суверенитету, а также контроль за уровнем качества предоставляемых клиентам и контрагентам ИТ-сервисов.

В рамках киберучений планируется осуществить следующие мероприятия:

- проведение киберучений (стресс-тестирований) деятельности организаций кредитно-финансовой сферы;
- оценка киберриска для целей интеграции в надзорную оценку операционного риска в части:
  - риска информационной безопасности;
  - риска информационной безопасности, связанного с возможным совершением операций без согласия клиентов;
  - риска информационной безопасности, связанного с возможным нарушением операционной надежности.

Планируется развитие сценарного подхода в рамках надзорного стресс-тестирования с целью оценки устойчивости поднадзорных организаций кредитно-финансовой сферы в результате реализации инцидентов информационной безопасности и операционной надежности.

Результаты киберучений будут использоваться в системе мониторинга и анализа операционных рисков организаций кредитно-финансовой сферы.

3.3. Риск-профилирование

Банк России продолжит практику формирования риск-профиля поднадзорных организаций для оценки фактических рисков информационной безопасности и операционной надежности. Показатели риск-профиля используются в рамках реализации общего процесса по организации и проведению киберучений в ходе надзорных мероприятий, а также учитываются при определении режима надзора в отношении организаций кредитно-финансовой сферы. Для этого планируется провести следующие мероприятия:

- разработка метрик оценки киберриска, включая метрики оценки рисков поставщиков услуг аутсорсинга, в части рисков информационной безопасности и операционной надежности, а именно:
  - риска информационной безопасности;
  - риска информационной безопасности, связанного с возможным совершением операций без согласия клиентов;
  - риска информационной безопасности, связанного с возможным нарушением операционной надежности;
- развитие механизма риск-профилирования финансовых организаций по киберриску;
- мониторинг и выявление киберрисков, влияющих на финансовую устойчивость и операционную надежность крупных финансовых организаций, финансовых объединений, финансовых экосистем.

Результаты риск-профилирования будут использоваться в системе мониторинга и анализа операционных рисков организаций кредитно-финансовой сферы.

3.4. Аутсорсинг информационных технологий и использование облачных сервисов

Использование услуг поставщиков аутсорсинга информационных технологий и облачных сервисов требует от организаций кредитно-финансовой сферы отдельного внимания к передаваемым бизнес-процессам и функциям, подпадающим под регулирование в области защиты информации и операционной надежности со стороны Банка России. При этом поставщики услуг аутсорсинга информационных технологий и облачных сервисов должны в полной мере соблюдать требования законодательства в отношении выполнения бизнес-процессов и функций, переданных на аутсорсинг. Такой подход соответствует международной практике.

В рамках данной задачи планируется реализовать следующие мероприятия:

- совершенствование института аутсорсинга информационных технологий и облачных сервисов для финансовых организаций с учетом киберрисков;
- мониторинг рисков аутсорсинга информационных технологий и облачных сервисов;
- развитие механизмов применения облачных сервисов в кредитно-финансовой сфере. Для совершенствования института аутсорсинга информационных технологий и облачных услуг информационных систем и их компонентов, в частности облачных и файловых хранилищ, серверов, иных устройств и систем сбора, хранения и обработки информации, Банк России совместно с уполномоченными федеральными органами исполнительной власти планирует создать правовые условия для размещения, хранения и иной обработки сведений, получаемых в рамках деятельности организаций кредитно-финансовой сферы. При этом предусмотрено использование принадлежащих поставщикам услуг аутсорсинга информационных систем и их компонентов, а также определение правового статуса поставщика услуг аутсорсинга информационных технологий и облачных услуг с распространением на него требований по обеспечению защиты банковской тайны и иных охраняемых законом видов тайн.

В развитие норм, формирующих условия использования услуг аутсорсинга, Банк России планирует определить порядок взаимодействия при аутсорсинге информационных технологий и облачных услуг, а также разработать требования к управлению риском при аутсорсинге.

Для обеспечения надлежащего выполнения требований к защите информации и операционной надежности Банк России продолжит совершенствовать набор надзорных инструментов и практик по анализу рисков, связанных с использованием услуг аутсорсинга, в том числе развивать инструменты определения порогового значения уровня концентрации поставщиков услуг аутсорсинга, свидетельствующего о наличии системных рисков.

Базовый блок. Международное сотрудничество

Банк России продолжит линию развития международного сотрудничества по вопросам информационной безопасности, сформулированную в Основных направлениях 2019–2021. Это обеспечит преемственность подходов к развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации в сфере информационной безопасности и киберустойчивости, а также компетентного участия в формировании актуальной и отвечающей российским интересам повестки дня.

Основными задачами в текущих условиях продолжат оставаться выстраивание обмена опытом по регулированию и внедрение финансовых технологий совместно с центральными (национальными) банками.

При этом, учитывая результаты международного взаимодействия, достигнутые в 2019–2021 годах, Банк России планирует, с одной стороны, продолжить расширение повестки взаимодействия и числа его участников, а с другой – укрепление и дополнение уже существующих связей за счет тесного и углубленного сотрудничества.

- **Многостороннее сотрудничество.** Банк России будет участвовать в деятельности международных организаций по вопросам информационной безопасности и киберустойчивости через изучение подходов и лучших практик регулирования и надзора по вопросам киберустойчивости. В этой работе будут задействованы главным образом площадки Международной организации по стандартизации (International Organization for Standardization, ISO), Международной электротехнической комиссии (International Electrotechnical Commission, IEC), Международного союза электросвязи (International Telecommunication Union, ITU).

В том числе будет проводиться мониторинг деятельности Международной организации комиссий по ценным бумагам (International Organization of Securities Commissions, IOSCO), Совета по финансовой стабильности (Financial Stability Board, FSB), Комитета по платежным и рыночным инфраструктурам Банка международных расчетов (Committee on Payments and Market Infrastructures, CPMI), Международной организации страхового надзора (International Organization of Insurance Supervisors, IAIS), Базельского комитета по банковскому надзору (Basel Committee on Banking Supervision, BIS).

- **Интеграционное сотрудничество.** Взаимодействие с национальными (центральными) банками государств – членов ЕАЭС и БРИКС по вопросам обмена информацией и лучшими практиками в сфере защиты прав потребителей финансовых услуг и повышения уровня доверия к цифровым технологиям, информационной безопасности и киберустойчивости цифровых и платежных технологий, включая вопросы стандартизации в области информационной безопасности.
- **Двустороннее сотрудничество.** Взаимодействие с регуляторами и надзорными органами иностранных государств по вопросам обмена информацией и лучшими практиками в сфере информационной безопасности и киберустойчивости.

Базовый блок. Подготовка кадров в сфере информационной безопасности

В сфере информационной безопасности, как и в сфере информационных технологий, зачастую наблюдаются дефицит кадров и недостаточно высокий уровень их подготовки. Информационная безопасность в силу своей специфики находится на переднем плане при внедрении инноваций, новых цифровых и платежных технологий, поэтому развитие кадрового потенциала – одна из приоритетных задач.

- **Внедрение профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере».** Профессиональный стандарт как инструмент национальной системы квалификации разработан совместно с экспертным, научным и бизнес-сообществами в интересах отрасли кредитно-финансовой сферы для создания необходимых компетенций.

В профессиональном стандарте сформированы требования к трудовым действиям, знаниям и умениям специалистов по информационной безопасности различных уровней, предусматривающие поступательное развитие и совершенствование профессиональных навыков.

Для совершенствования организационных мер обеспечения информационной безопасности, операционной надежности организаций кредитно-финансовой сферы, а также с учетом современных вызовов и угроз Банк России планирует проводить регулярную актуализацию положений профессионального стандарта.

- **Развитие государственных образовательных стандартов высшего образования для подготовки специалистов по информационной безопасности в кредитно-финансовой сфере.** Профессиональные стандарты создают базис для разработки образовательных стандартов, поэтому Банк России проработает вопросы формирования требований к образованию и направлениям подготовки специалистов по информационной безопасности в кредитно-финансовой сфере. С этой целью будут сформированы подходы к доработке федеральных государственных стандартов по направлениям подготовки специалистов по информационной безопасности и разработке методических рекомендаций по подготовке специалистов по информационной безопасности в кредитно-финансовой сфере различных уровней образования. На их основе предполагается разработать обучающие программы для образовательных учреждений Российской Федерации.
- **Реализация образовательных программ, в том числе дополнительного профессионального образования, по информационной безопасности на базе ведущих вузов.** В целях применения единых стандартов качества подготовки специалистов по информационной безопасности с фундаментальными знаниями особенностей функционирования финансового рынка планируется создание инновационной образовательной экосистемы по подготовке практико-ориентированных специалистов в области информационной безопасности в кредитно-финансовой сфере, в том числе на основе симбиоза фундаментальной научной базы и высокого уровня экспертизы специалистов реального сектора экономики.

Банк России продолжит создание условий для подготовки специалистов в области информационной безопасности нового типа. Так, планируется создать территориально распределенную сеть вузов, реализующих образовательные программы по информационной безопасности в кредитно-финансовой сфере.

Кроме того, предполагается разработка и создание уникальных образовательных продуктов по информационной безопасности для талантливой молодежи на базе ведущих научных и образовательных центров, консорциумов, объединений вузов Российской Федерации, а также базовой кафедры НИУ ВШЭ.

- **Анализ и планирование потребности в специалистах по информационной безопасности в кредитно-финансовой сфере.** В целях планирования общей потребности отрасли в кадровом обеспечении специалистами по информационной безопасности Банк России продолжит

практику мониторинга перспективной потребности организаций кредитно-финансовой сферы в кадрах. Анализ результатов исследования позволит сформировать прогнозную модель необходимого количества выпускников в области информационной безопасности, а также станет основой проектируемых образовательных программ и продуктов.

- **Развитие практических навыков специалистов по информационной безопасности в кредитно-финансовой сфере.** Реализация практико-ориентированного подхода в обучении для всех уровней образовательной системы Российской Федерации по направлениям информационной безопасности в кредитно-финансовой сфере позволит сформировать пул практических навыков у будущих специалистов.

Планируется создать условия для их формирования в научной и исследовательской деятельности образовательных учреждений с фокусом внимания, ориентированным на рассмотрение практических аспектов и актуальных вопросов информационной безопасности в кредитно-финансовой сфере.

Образовательные инициативы Банка России в целях наращивания актуальной технической экспертизы специалистов по информационной безопасности в кредитно-финансовой сфере будут реализовываться в рамках организации и проведения практической и проектной деятельности.

- **Практико-ориентированное обучение по информационной безопасности «КиберКурс».** Для формирования практических навыков работников, занимающихся информационной безопасностью, Банк России продолжит реализацию программы практико-ориентированного обучения по информационной безопасности «КиберКурс». Программа позволит актуализировать уже имеющиеся знания, поддерживать профессиональные компетенции в сфере информационной безопасности, развивать межведомственное взаимодействие, а также снижать уровень киберпреступности и кибермошенничества в кредитно-финансовой сфере в целом.
- **Регулярное повышение квалификации профессорско-преподавательского состава в сфере современных цифровых финансовых инструментов и технологий.** Для формирования у обучающихся актуальных знаний и компетенций в сфере финансового рынка Банк России планирует применять комплексный подход к системе повышения квалификации профессорско-преподавательского состава в сфере современных цифровых финансовых инструментов и технологий. Оно будет проходить на базе лучшего опыта организаций кредитно-финансовой сферы. Предполагается создание педагогического сообщества профессионалов, ориентированного на разработку педагогических практик и методик преподавания актуальных знаний по финансовой киберграмотности и кибергигиене.

Базовый блок. Работа с данными

- **Обеспечение качества и доверия к данным.** Реализуя Основные направления развития системы управления данными Банка России на 2022–2024 годы, Банк России планирует сформировать системный подход к обеспечению качества и доверия как к данным, используемым в Банке России для принятия управленческих решений, так и к данным, предоставляемым и получаемым от поднадзорных организаций и участников информационного взаимодействия с ФинЦЕРТ.

В рамках данного направления планируется повысить эффективность использования видов данных, необходимых:

- для расчета риск-профиля поднадзорных организаций;
- для глубокой аналитики компьютерных атак;
- для обеспечения качества и оперативности представления информации об операциях без согласия клиентов.

Автоматизация управления качеством данных позволит реализовать возможность оперативного мониторинга состояния данных и их аналитики для осуществления стратегических задач Банка России по развитию информационной безопасности кредитно-финансовой сферы.

- **Предоставление данных и сервисов внешним пользователям для целей страхования киберрисков.** По данным международных экспертов, по состоянию на 2022 год глобальный рынок страхования киберрисков достигнет 14 млрд долл. США, а к 2025 году он будет составлять уже 20 млрд долл. США. Задача страхования киберрисков состоит в покрытии убытков, возникших в результате успешно реализованных кибератак. Банк России планирует сформировать условия создания института страхования киберрисков и предоставить расширенный перечень данных внешним пользователям для формирования моделей страхования.
- **Внедрение практик управления данными.** Банк России будет развивать практики управления данными в целях обеспечения информационной безопасности данных в поднадзорных организациях и в Банке России, а также качества данных, используемых для формирования риск-профиля, аналитики компьютерных атак и информации об операциях без согласия клиентов.
- **Развитие правил работы с данными в структурных подразделениях Банка России в части информационной безопасности.** Для обеспечения реализации практик управления безопасностью данных планируется сформировать правила работы с данными в структурных подразделениях Банка России, в том числе определить объекты доступа, единые правила управления доступом к данным, ролевую модель ответственности и механизмы предоставления доступа к наборам данных.