Банк России

ПЛАН-ПРОСПЕКТ ОСНОВНЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ НА ПЕРИОД 2022 – 2024 ГОДОВ

ДЕПАРТАМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2022 г.

Банк России

Связь с основными стратегическими документами Банка России

- Основные направления развития финансового рынка РФ на 2022 г. и период 2023 и 2024 гг.
- Основные направления цифровизации финансового рынка на период 2022 - 2024 гг.
- Стратегия развития национальной платежной системы на 2021 - 2023 г.
- Стратегия повышения финансовой грамотности в РФ на 2017 - 2023 гг.
- Приоритетные направления повышения доступности финансовых услуг в РФ на период 2022 - 2024 гг.
- Основные направления развития системы управления данными Банка России на период 2022 - 2024 гг.

Банк России

Структура Основных направлений развития информационной безопасности кредитно-финансовой сферы

1 Текущее состояние, возможности и вызовы для развития российского финансового рынка

2 Цели и направления развития

- Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям — **Граждане**
- Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий — **Бизнес**
- Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг — **Государство**

3 Индикаторы

- Степень удовлетворенности населения уровнем безопасности финансовых услуг, оказываемых организациями кредитно-финансовой сферы
- Доля цифровых и платежных технологий, в отношении которых сформированы требования по информационной безопасности и киберустойчивости
- Отсутствие инцидентов информационной безопасности и операционной надежности в отношении системно значимых кредитных организаций и крупных финансовых организаций, которые привели к нарушению финансовой устойчивости

Банк России

Развитие информационной безопасности кредитно-финансовой сферы 2022-2024

Цели

Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям	Создание условий для безопасного внедрения цифровых и платежных технологий	Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг

Направления развития

Противодействие ОБС, социальной инженерии	Развитие регулирования	RegTech- и SupTech-проекты
Противодействие компьютерным атакам	Развитие инфраструктурных проектов	Интеграция вопросов ОН в управление операционным риском *
Финансовая киберграмотность	Развитие нац. платежной инфраструктуры и цифровой рубль	Киберучения *
	Экспериментальные правовые режимы и регуляторная песочница	Риск-профилирование
	Технологическая независимость	Аутсорсинг
	Финансовая киберграмотность	

* В части рисков информационной безопасности и операционной надежности

Форма реализации

1. Правовое регулирование
2. Методология и стандартизация информационной безопасности и киберустойчивости
3. Надзорная деятельность
4. Развитие ФинЦЕРТ — Развитие ФинЦЕРТ
5. Реализация технологических процессов / цифровизация

Базовые блоки

6. Международное сотрудничество и изучение международного опыта
7. Подготовка кадров
8. Работа с данными

Банк России

1. Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям

Противодействие совершению операций без согласия клиента, социальной инженерии

1. Совершенствование механизмов:
   - 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;
   -мониторинга операций с целью выявления аномалий, указывающих на возможные мошеннические действия

2. Информационный обмен с МВД России сведениями из базы данных по операциям по переводу денежных средств без согласия клиента (проект федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»)

3. Включение показателей качества антифрод-процедур в механизмы оценки операционных рисков кредитных организаций

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Цифровизация

Методология

ФинЦЕРТ

Работа с данными

Банк России

1. Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям

4 Развитие каналов обращения в правоохранительные органы (ЕПГУ, ДБО)

5 Изменение процедуры рассмотрения обращений потребителей

6 Повышение безопасности при предоставлении кредита (займа) онлайн:

- введение механизма самозапрета на выдачу кредита или только онлайн-кредита через БКИ (credit lock);
- повышение качества идентификации и аутентификации получателей кредита (займа) онлайн;
- определение показателей и лимитов по управлению операционным риском при выдаче кредитов;
- защита от закредитованности в результате действий мошенников

7 Обеспечение принципа пропорциональности в регулировании рынка микрофинансовых институтов

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Методология

Работа с данными

1. Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям

Противодействие компьютерным атакам

1. Формирование и совершенствование информационного обмена между Банком России и финансовыми организациями по тактике, технике совершения компьютерных атак, в том числе для целей формирования сценариев проведения киберучений, сокращения времени реагирования на компьютерные атаки

2. Развитие информационного обмена ФинЦЕРТ с организациями кредитно-финансовой сферы в части противодействия компьютерным атакам как отраслевого центра безопасности критической информационной инфраструктуры

3. Реализация мер противодействия целевым компьютерным атакам в зависимости от уровня опасности некредитными финансовыми организациями, являющимися крупными инфраструктурными организациями финансового рынка и субъектами критической информационной инфраструктуры

ДИБ - соисполнитель

ДИБ - отв. исполнитель


Правовое регулирование


Надзор


Цифровизация


Работа с данными


Методология


ФинЦЕРТ


Кадры

Банк России

1. Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям

Финансовая киберграмотность

1. Реализация программ по повышению финансовой киберграмотности и пропаганде кибергигиены для различных категорий населения, в том числе лиц с низким уровнем дохода, социально незащищенных категорий населения
2. Реализация Единой рамки компетенций в области финансовой грамотности
3. Размещение социальной рекламы и просветительского контента по теме противодействия социальной инженерии и повышения финансовой киберграмотности населения, в том числе в СМИ федерального, регионального и местного уровня, а также на объектах транспортной и социальной инфраструктуры с учетом особенностей соответствующих целевых групп населения
4. Усиление информационной работы кредитных организаций, направленной на повышение осмотрительности клиентов в отношении сохранности личных и финансовых данных
5. Организация на федеральных и региональных ТВ каналах информационно-просветительского программ по финансовой киберграмотности

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

Кадры

Надзор

Работа с данными

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Развитие регулирования*

Обеспечение ИБ и киберустойчивости через регулирование и последующий надзор за следующими финтех-проектами:

1. Цифровой профиль
2. Маркетплейс
3. Открытые интерфейсы на финансовом рынке (Open API), открытые банковские интерфейсы в национальной платежной системе, а также интерфейсы небанковских поставщиков платежных услуг
4. Электронное хранение документов
5. Экосистемы:
   - обеспечение безопасности информационной инфраструктуры участников финансовой экосистемы;
   - обеспечение безопасности технологий, реализуемых в рамках финансовых экосистем;
   - обеспечение безопасности обработки «больших данных»;
   - регистрация, классификация и обмен информацией об инцидентах защиты информации и операционной надежности между участниками финансовой экосистемы;
   - управление риском информационной безопасности в рамках финансовых экосистем;
   - противодействие социальной инженерии в отношении пользователей финансовых экосистем;
   - регулирование платежных сервисов в экосистемах с точки зрения информационной безопасности

* В части оценки системных рисков, связанных с применением финансовых технологий, и достаточности регуляторного периметра с учетом тенденций в развитии финансовых технологий.

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Кадры

Методология

Международное сотрудничество

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

6 Единая информационная система проверки сведений об абоненте (ЕИС ПСА)

7 Обеспечение информационной безопасности для новых способов инициирования платежей и переводов (смарт-устройства и другие)

8 Коммерческие биометрические системы

9 Новые субъекты НПС (небанковские поставщики платежных услуг и другие)

10 Внедрение механизмов оборота данных организаций кредитно-финансовой сферы в части их информационной безопасности, включая целостность

11 Формирование «среды доверия» при удаленном предоставлении финансовых услуг и сервисов для реализации протоколов информационной безопасности в сервисах, предоставляемых банками и НФО клиентам дистанционно

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Кадры

Методология

Международное сотрудничество

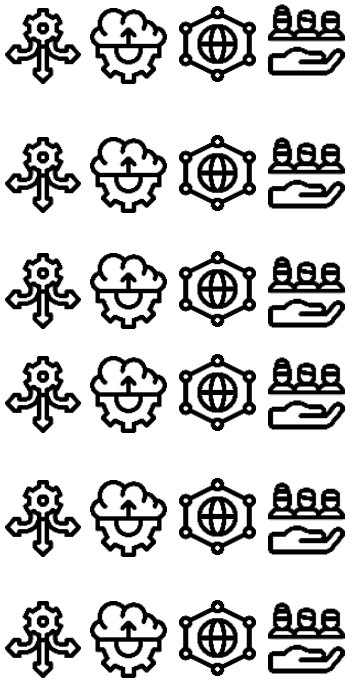
Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Развитие инфраструктурных проектов

Обеспечение информационной безопасности для следующих финтех-проектов:

1. Развитие новых способов идентификации и аутентификации, использования биометрических технологий
2. Развитие удаленной идентификации, в том числе для нерезидентов
3. Цифровые финансовые активы и краудфандинг
4. Повышение доступности применения электронной подписи для массового сегмента
5. Оценка рисков, связанных с применением финансовых технологий, и достаточности регуляторного периметра с учетом тенденций в развитии финансовых технологий
6. Цифровизация ипотеки



ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

Международное сотрудничество

Цифровизация

Кадры

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Обеспечение информационной безопасности для следующих финтех-проектов:

7 Создание оператора автоматизированной информационной системы страхования (АИС страхования), поддержка бюро страховых историй

8 Развитие факторинга

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

Международное сотрудничество

Цифровизация

Кадры

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Развитие национальной платежной инфраструктуры и цифровой рубль

1. Расширение доступа к платежной системе Банка России, в том числе нерезидентов

2. Система быстрых платежей:
   - расширение доступа к СБП, в том числе нерезидентов;
   - развитие сервисов СБП, включая вопросы управления рисками ИБ;
   - мобильное приложение СБПэй;
   - интероперабельность СБП, в том числе интеграция национальных СБП государств – членов ЕАЭС с СБП

3. Система передачи финансовых сообщений:
   - расширение участия нерезидентов;
   - внедрение новых сервисов в СПФС;
   - развитие института сервис-бюро;
   - реализация интернет-доступа к СПФС;
   - поддержка ISO 20022 в СПФС

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Цифровизация

Методология

Международное сотрудничество

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

4 Цифровой рубль:

- развитие безопасности технологии обработки информации на стадиях жизненного цикла Цифрового рубля, включая создание среды «доверия», обеспечивающей надлежащую криптографическую аутентификацию участников операций с Цифровым рублем;
- развитие антифрод-механизмов (мониторинг операций с целью выявления аномалий, указывающих на возможные мошеннические действия, и компрометацию участников платформы) с учетом специфики операций в Цифровых рублях;
- 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

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Цифровизация

Методология

Международное сотрудничество

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Экспериментальные правовые режимы и регуляторная песочница

1. Обеспечение информационной безопасности и киберустойчивости

2. Моделирование процессов, связанных с предоставлением (применением) инновационных продуктов, услуг и технологий в банковской сфере и иных сферах финансового рынка, с учетом требований информационной безопасности

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

Кадры

Цифровизация

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Технологическая независимость

1. Координация деятельности значимых объектов критической информационной инфраструктуры в целях снижения риска технологической зависимости финансовых организаций и инфраструктуры от внешних поставщиков

2. Обеспечение информационной безопасности, в том числе с использованием российских криптографических средств, в значимых платежных системах

3. Организация функционирования отраслевого центра компетенций в целях импортозамещения программного обеспечения в интересах финансового сектора экономики

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Надзор

Кадры

Методология

Цифровизация

Банк России

2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий

Финансовая киберграмотность

1. Развитие школьников и студентов на площадке ОЦ «Сириус»

2. Реализация образовательных программ по информационной безопасности на базе ведущих ВУЗов, в том числе в рамках Базовой кафедры НИУ ВШЭ

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

Кадры

Работа с данными

Банк России

3. Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг

RegTech- и SupTech-проекты

1. Совершенствование системы внешнего аудита информационной безопасности (Внешний аудит):
   - аудит по вопросам защиты информации и операционной надежности;
   - аудит поставщиков облачных сервисов;
   - аудит безопасности приложений

2. Внедрение системы мониторинга и анализа операционных рисков кредитных организаций

3. Совершенствование анализа новостного фона для оценки рисков поднадзорных организаций

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Работа с данными

Методология

Международное сотрудничество

Банк России

3. Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг

Киберучения

1. Проведение стресс-тестирования («киберучений») деятельности организаций кредитно-финансовой сферы

2. Оценка финансовой устойчивости поднадзорных организаций в рамках оценки возможности поднадзорных организаций выявлять, реагировать и восстанавливаться в случае реализации инцидентов информационной безопасности (операционной надежности)

3. Оценка реализации системы управления рисками информационной безопасности и операционной надежности (киберустойчивости)

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

ФинЦЕРТ

Надзор

Работа с данными

3. Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг

Риск-профилирование

1. Разработка метрик оценки рисков финансовой устойчивости и стабильности, включая метрики оценки рисков аутсорсинга услуг финансовыми организациями, в части рисков ИБ и операционной надежности

2. Развитие механизма риск-профилирования финансовых организаций по киберриску

3. Мониторинг и выявление киберрисков, влияющих на финансовую устойчивость и операционную надежность крупных финансовых организаций, финансовых объединений, финансовых экосистем

ДИБ - соисполнитель

ДИБ - отв. исполнитель

Методология

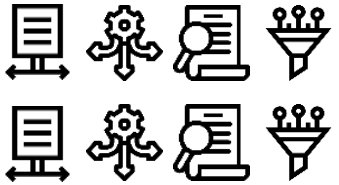
Работа с данными

Надзор

3. Обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг

Аутсорсинг информационных технологий и использование облачных сервисов

1. Совершенствование института аутсорсинга для финансовых организаций с учетом киберрисков
2. Развитие механизмов применения облачных сервисов в кредитно-финансовой сфере



ДИБ - соисполнитель

ДИБ - отв. исполнитель

Правовое регулирование

Надзор

Методология

Работа с данными

Базовый блок. Международное сотрудничество

1. Участие в деятельности международных организаций по вопросам ИБ («Многостороннее сотрудничество»)
2. Взаимодействие с регуляторами иностранных государств - ЕАЭС, БРИКС («Интеграционное сотрудничество»)
3. Взаимодействие с национальными (центральными) банками иностранных государств («Двустороннее сотрудничество»)
4. Сотрудничество в области обеспечения информационной безопасности и киберустойчивости в сфере финансовых рынков стран ЕАЭС:
   - Концепция формирования общего финансового рынка ЕАЭС;
   - Доверенная третья сторона для государств - членов ЕАЭС

Базовый блок. Подготовка кадров в сфере ИБ

1. Утверждение и внедрение профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере»
2. Развитие государственных образовательных стандартов высшего образования в части подготовки специалистов по информационной безопасности в кредитно-финансовой сфере
3. Развитие практических навыков специалистов по информационной безопасности в кредитно-финансовой сфере
4. Практико-ориентированное обучение по информационной безопасности «КиберКурс»
5. 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
6. Реализация инфраструктуры киберполигона для целей деятельности Банка России по подготовке кадров в сфере ИБ

Базовый блок. Работа с данными

1. Обеспечение качества и доверия к данными, в том числе автоматизация управления качеством данных:
   - риск-профиля;
   - о компьютерных атаках;
   - об операциях без согласия клиента

2. Предоставление данных и сервисов внешним пользователям для целей страхования киберрисков

3. Внедрение практик управления данными для целей:
   - обеспечения информационной безопасности данных в поднадзорных организациях и в Банке России;
   - обеспечение качества данных, используемых для формирования риск-профиля, аналитики компьютерных атак и информации об операциях без согласия клиента

4. Развитие правил работы с данными в структурных подразделениях Банка России в части информационной безопасности

Предложения к проекту Основных направлений просим направлять до 15 августа 2022 года:

Digital@cbr.ru

Банк России

СПАСИБО ЗА ВНИМАНИЕ!