Банк России

Новые нормативные требования в области информационной безопасности кредитно-финансовой сферы

перспектива на период 2019–2023 гг.

Тенденции

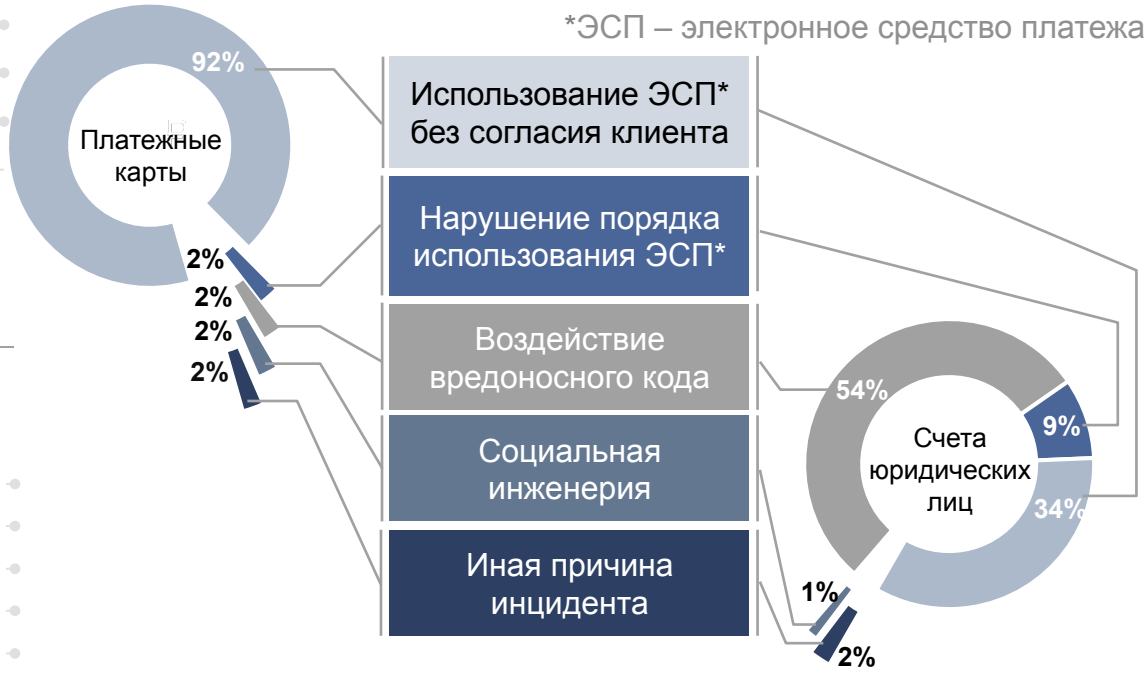
Статистика несанкционированных переводов денежных средств

Несанкционированные переводы с использованием платежных карт

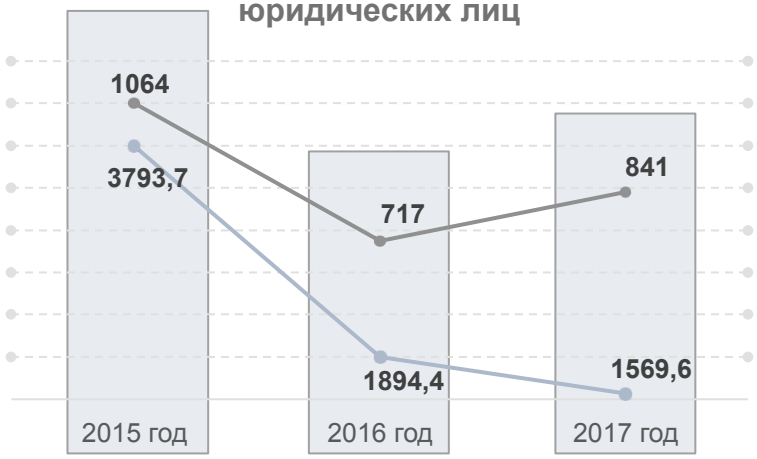
961,3 млн руб. — Объем несанкционированных операций, совершенных с использованием платежных карт **в 2017 году**

0,0016 % — Доля объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт **в 2017 году**

*ЭСП – электронное средство платежа



Несанкционированные переводы со счетов юридических лиц



1,57 млрд руб. — Объем несанкционированных операций, совершенных со счетов юридических лиц **в 2017 году**

> 50 % — Доля остановленных несанкционированных операций **в 2017 году**

Регулирование вопросов защиты информации на финансовом рынке

Предпосылки и драйверы

- Тенденции и скорость развития сферы цифровых финансовых услуг
- Активная позиция по стимулированию развития финансовых технологий в масштабах государства
- Новые полномочия Банка России по обеспечению ИБ на финансовом рынке
- Защита потребителей финансовых услуг от потерь в случае реализации информационных угроз
- Интеграция показателей киберриска в состав основных рисков финансовых организаций

Полномочия Банка России

Законодательно закреплено

- ☑ Регулирование вопросов по защите информации при осуществлении переводов денежных средств
- ☑ Регулирование вопросов по защите информации при осуществлении банковских операций
- ☑ Регулирование вопросов по защите информации при осуществлении финансовых операций
- ☑ Регулирование вопросов по информационному обмену

Целесообразно закрепить

- ☐ Право принятия Банком России решений по внесудебному блокированию:
  - фишинговых сайтов
  - сайтов, связанных с осуществлением незаконной финансовой деятельности
- ☐ Право выпуска сертификатов ключей УКЭП для поднадзорных Банку России организаций

Область регулирования и контроля

- **Субъекты национальной платежной системы** (осуществляющие переводы денежных средств)
- **Кредитные организации** (осуществляющие банковские операции)
- **Финансовые организации** (осуществляющие финансовые операции)
- **Инновационные финансовые технологии**

Основные цели

Обеспечение киберустойчивости

- контроль показателей риска реализации информационных угроз
- обеспечение непрерывности предоставления финансовых и банковских услуг
- контроль уровня операций, совершенных без согласия клиентов (фродовые операции)

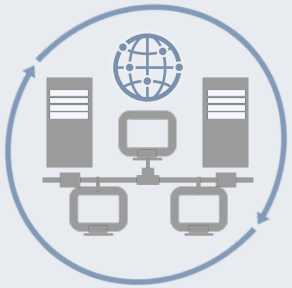
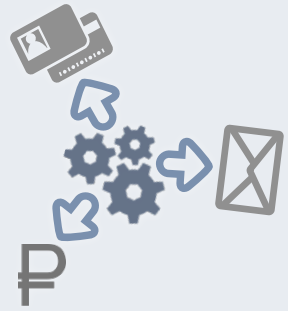
Защита потребителей финансовых услуг

- мониторинг и контроль показателей, характеризующих уровень финансовых потерь

Содействие развитию инновационных финансовых технологий

- контроль риска реализации информационных угроз
- реализация необходимого уровня информационной безопасности

Основные элементы информационной безопасности

Уровни ИБ	Методологическая составляющая	Надзорная составляющая
Инфраструктурный уровень 	**Защита инфраструктуры по комплексу ГОСТ** домен ***УР*** – «управление киберриском» домен ***ЗИ*** – «защита информации» домен ***СО*** – «мониторинг киберрисков и ситуационная осведомленность» домен ***ОНД*** – «обеспечение непрерывности выполнения бизнес- и технологических процессов финансовых организаций в случае реализации информационных угроз» домен ***УА*** – «управлением киберриском при аутсорсинге и использовании сторонних информационных услуг (сервисов)» домен ***УИ*** – «управление инцидентами ИБ»	**Надзор подразделений ИБ Банка России** **Система внешнего аудита**
Уровень приложений 	**► ГОСТ Р ИСО/МЭК 15408-3-2013 – критерии оценки безопасности информационных технологий, компоненты доверия к безопасности** **► Профиль защиты для оценки уязвимости в банковских приложениях**	**► Анализ уязвимостей приложений, критичных с точки зрения наличия уязвимостей (сертификация):** - приложения клиентов - фронт-приложения **► Сертификация ФСТЭК России**
Уровень технологии обработки данных 	**► Обеспечение целостности информации на технологических участках ее обработки** **► Протоколирование действий на технологических участках** **► Взаимодействие с клиентами финансовых организаций** - идентификация клиентов - получение подтверждения финансовых (банковских) операций - направление уведомлений о совершенных операциях **► Ведение баз данных об инцидентах ИБ, в том числе на основе претензионной работы**	**► Анализ показателей уровня риска по операциям на технологических участках** **► Анализ показателей, формируемых на основе претензионной работы**

Надзорная составляющая

Формирование системы показателей

Показатели операционной стабильности

Показатели финансовой стабильности

Показатели защищенности инфраструктуры

Показатели защищенности приложений

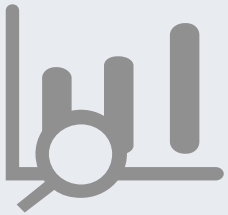
Показатели риска по операциям

Источники

- регулярная отчетность об инцидентах и информационной обмен АСОИ ФинЦЕРТ
- результаты инспекционных проверок

- результаты инспекционных проверок

- протоколирование действий на технологических участках
- информация, содержащаяся в базах данных



Состав операционных рисков финансовых организаций

показатели, характеризующие уровень несанкционированных финансовых операций

показатели , характеризующие непрерывность предоставления финансовых услуг

показатели, характеризующие финансовые потери клиентов финансовых организаций

Банк России – Центр компетенции в области обеспечения информационной безопасности

Стандартизация

Организация работы подкомитета № 1 ТК 122

Участие в работе международной организации по стандартизации

- **ISO** (Международная организация по стандартизации)
- **ITU** (Международный союз электросвязи)
- **IEC** (Международная электротехническая комиссия)

Межведомственное взаимодействие

Центр организации межведомственной работы по обеспечению ИБ на финансовом рынке

Межведомственная рабочая группа при участии представителей

- **МВД России**
- **ФСТЭК России**
- **ФСБ России**
- **Минкомсвязи России**
- **Росфинмониторинга**
- **Экспертов кредитных организаций**

Программа «Цифровая экономика»

ФинЦЕРТ Банка России - Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

Участие в создании единой системы противодействия информационным угрозам с учетом международного опыта

- **IOSCO** (Международная организация комиссии по ценным бумагам)
- **WEF** (Всемирный экономический форум)
- **FSB** (Совет по финансовой стабильности)

Подготовка кадров в сфере ИБ

Разработка учебных программ

- **переподготовка специалистов и руководителей подразделений ИБ**
- **программы бакалавриата и специалитета**
- **переподготовка на базе ведущих вузов**
- **работа по аттестации специалистов**

Международное взаимодействие

Взаимодействие с международными организациями по вопросам ИБ

- **FIRST** (Международное сообщество команд реагирования на компьютерные инциденты (Forum for Incident Response and Security Teams)
- **EAST EGAF** (Европейская команда по реагированию на инциденты, связанные с банкоматами (European ATM Security Team – Expert Group on ATM Fraud)
- **CCERTs** (Группы реагирования на компьютерные инциденты таких стран, как Израиль, Испания, страны Скандинавского региона, Болгария, Индия, Нидерланды и Япония)

Целевая архитектура ФинЦЕРТ Банка России

*АИС - автоматизированная информационная система

Оперативное «приостановление» несанкционированных переводов денежных средств

1. **Оперативное взаимодействие с участниками платежной системы Банка России по вопросам «приостановления» несанкционированных переводов денежных средств в платежной системе Банка России**
2. **Организация взаимодействия кредитных организаций с целью «приостановления» несанкционированных переводов денежных средств юридических лиц**