# Нормативное регулирование и обеспечение кибербезопасности в организациях кредитно-финансовой сферы

**В.О. Лебедев**

**главный инженер отдела методологии и стандартизации киберустойчивости и информационной безопасности финансовых организаций Управления методологии и стандартизации информационной безопасности Главного управления безопасности и защиты информации**

# Нормативное регулирование вопросов обеспечения кибербезопасности в КФС

В рамках своей компетенции Банк России осуществляет регулирование и контроль вопросов информационной безопасности при осуществлении переводов денежных средств (часть 3 статьи 27 Федерального закона 27 июня 2011 года № 161-ФЗ «О национальной платежной системе»).

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».

# Основные цели нормативного регулирования вопросов обеспечения кибербезопасности в КФС

**- минимизация объема несанкционированных переводов денежных средств;**

**- минимизация риска нарушения финансовой стабильности в деятельности организаций кредитно-финансовой сферы в результате реализации компьютерных атак на их информационные ресурсы, а также в случаях хищений денежных средств.;**

**- минимизация риска возникновения непосредственного финансового ущерба клиентов и контрагентов организаций кредитно-финансовой сферы, связанного с несанкционированными финансовыми транзакциями, в том числе несанкционированными переводами денежных средств;**

**- обеспечение доверия клиентов и контрагентов организаций кредитно-финансовой сферы к безопасности реализуемых электронных технологий и сервисов.**

# Актуальность вопросов кибербезопасности в КФС

**Актуальность вопросов кибербезопасности в КФС определена максимальным интересом и вниманием криминалитета к возможности быстрого личного обогащения путем использования уязвимостей информационных технологий, используемых и реализуемых организациями кредитно-финансовой сферы.**

**Анализ результатов реагирования на инциденты информационной безопасности, проводимый Банком России, показывает, что злоумышленниками в основном изучены уязвимости информационных технологий, в первую очередь программного обеспечения, используемого кредитными организациями для осуществления переводов денежных средств, и отработаны схемы осуществления несанкционированных переводов денежных средств в национальной платежной системе с последующим их выведением и обналичиваем.**

## Основные направления реализации компьютерных атак

**- атака на информационную инфраструктуру организаций кредитно-финансовой сферы путем внедрения вредоносного кода в автоматизированные банковские системы, платежное программное обеспечение;**

**- атака на клиентов организаций кредитно-финансовой сферы путем внедрения вредоносного кода в программное обеспечение ПЭВМ, смартфонов, АРМ клиента Банка России.**

# Основные виды ущерба от деятельности злоумышленников при реализации успешных компьютерных атак на организации кредитно-финансовой сферы

**- непосредственный финансовый ущерб, связанный с несанкционированными переводами денежных средств;**

**- выведение денежных средств из легального финансового оборота;**

**- нарушение финансовой стабильности в деятельности организаций кредитно-финансовой сферы;**

**- нанесение репутационного ущерба организациям кредитно-финансовой сферы и, как следствие, формирование условий недоверия к их деятельности со стороны граждан Российской Федерации.**

# Основные причины реализации успешных компьютерных атак на организации кредитно-финансовой сферы

**- наличие уязвимостей ИБ в применяемых организациями информационных системах и платежных приложениях;**

**- недостатки в обеспечении ИБ в кредитных организациях, отсутствие должного соблюдения организациями требований, установленных нормативными актами и отраслевыми стандартами Банка России;**

**- отсутствие должного внимания менеджмента организаций к реализации безопасных технологий, в том числе при осуществлении переводов денежных средств;**

**- отсутствие должной координации деятельности организаций по противодействию массовым (веерным) и типовым компьютерным атакам;**

**- общая криминализация применения компьютерных технологий.**

# Направления действий

## Объединение усилий финансовых организаций и государства


Создание на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России единой системы противодействия хищениям денежных средств

## Организационно-правовые направления

Законодательное закрепление права Банка России по нормативному регулированию вопросов, связанных с обеспечением информационной безопасности всей информационной инфраструктуры финансовых организаций и всей информации, обрабатываемой в финансовых организациях (по согласованию с ФСБ России и ФСТЭК России)

Ввод в действие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в финансовых организациях

Нормативное закрепление обязанности финансовых организаций по применению национальных стандартов по защите информации

Реализация системы подтверждения соответствия обеспечения информационной безопасности финансовых организациях требованиям национальных стандартов

# ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ БАНКА РОССИИ

На сегодняшний день в информационном обмене, организованном Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России, участвуют 629 организаций, из них:

- 430 кредитных организаций, 18 небанковских кредитных организаций и 105 некредитных финансовых организаций
- 74 иных организаций (ФОИВ, разработчики программного обеспечения, организации, оказывающие услуги в области информационных технологий)
- правоохранительные органы (МВД России, ФСБ России)

Основные функции Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России:

- организация обмена информации, значимой для предотвращения компьютерных атак, между Банком России, правоохранительными органами, финансовыми организациями
- подготовка аналитических материалов для финансовых организаций
- разработка рекомендаций по обеспечению защиты информации для финансовых организаций, в том числе при осуществлении переводов денежных средств

# СТАНДАРТЫ БАНКА РОССИИ (СТО БР ИББС)

**по состоянию на 01.05.2018**

**Общие положения**
**СТО БР ИББС – 1.0 - 2014**

**Аудит информационной безопасности**
**СТО БР ИББС – 1.1 - 2007**

**Методика оценки соответствия**
**СТО БР ИББС – 1.2 - 2014**

**Сбор и анализ технических данных при реагировании на инциденты ИБ при осуществлении переводов денежных средств**
**СТО БР ИББС – 1.3 - 2016**

**Управление риском нарушения информационной безопасности при аутсорсинге**
**СТО БР ИББС – 1.4 - 2018**

---

**Технология подготовки, направления и форматы электронных сообщений для информационного обмена с Банком России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средстве СТО БР ИББС – 1.5 (проект)**

# Рекомендации в области стандартизации (РС БР ИББС)

## по состоянию на 01.05.2018

**Документы по обеспечению информационной безопасности**
**РС БР ИББС – 2.0 - 2007**

**Руководство по самооценке**
**РС БР ИББС – 2.1 - 2007**

**Методика оценки рисков**
**РС БР ИББС – 2.2 - 2009**

**Требования по обеспечению безопасности ПДн в ИСПДн**
**РС БР ИББС – 2.3 – 2010**
**(отменены, см. СТО 1.0)**

**Отраслевая частная модель безопасности ПДн**
**РС БР ИББС – 2.4 – 2010**
**(отменены, введено Указание 3889-У)**

**Менеджмент инцидентов информационной безопасности**
**РС БР ИББС – 2.5 - 2014**

**Обеспечение ИБ на стадиях жизненного цикла АБС**
**РС БР ИББС – 2.6 - 2014**

**Ресурсное обеспечение ИБ**
**РС БР ИББС – 2.7 - 2015**

**Обеспечение ИБ при использовании технологии виртуализации**
**РС БР ИББС – 2.8 - 2015**

**Предотвращение утечек информации**
**РС БР ИББС – 2.9 – 2016**

# НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ГОСТ Р

**по состоянию на 01.05.2018**

**Безопасность финансовых (банковских) операций.
Защита информации финансовых организаций.
Базовый состав организационных и технических мер
ГОСТ Р 57580.1-2017**

**Безопасность финансовых (банковских) операций.
Защита информации финансовых организаций.
Методика оценки соответствия
ГОСТ Р 57580.2-2018**