Банк России

ВЗАИМОДЕЙСТВИЕ БАНКА РОССИИ И ПОДНАДЗОРНЫХ ОРГАНИЗАЦИЙ В ОБЛАСТИ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КИБЕРУСТОЙЧИВОСТИ И ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Андрей Выборнов
заместитель директора – начальник Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России

2019 г.

Регулирование вопросов защиты информации на финансовом рынке

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

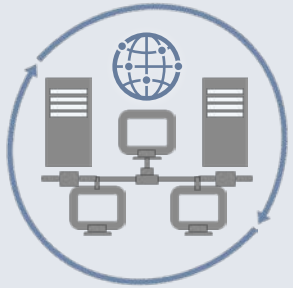
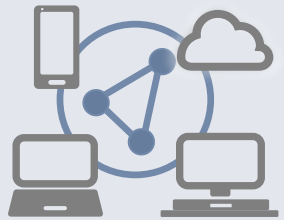
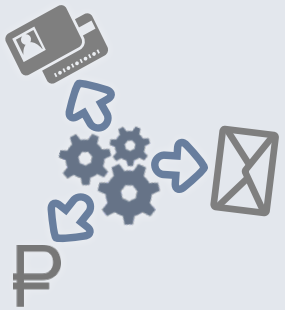
Область регулирования и контроля

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

Основные цели регулирования

- **Обеспечение киберустойчивости**
- **Защита потребителей финансовых услуг**
- **Содействие развитию инновационных финансовых технологий**

Общие подходы к регулированию вопросов защиты информации на финансовом рынке

Уровни ИБ	Методологическая составляющая	Надзорная составляющая
Инфраструктурный уровень 	**Защита инфраструктуры по комплексу ГОСТ** домен ***УР*** – управление киберриском домен ***ЗИ*** – защита информации домен ***ОН*** – обеспечение операционной надежности домен ***УА*** – управление киберриском при аутсорсинге и использовании сторонних информационных сервисов домен ***УИиСО*** – управление инцидентами ИБ и ситуационная осведомленность	**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 уязвимостей 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**

Указанные подходы уже заложены в проекты нормативных актов Банка России:

«Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

«Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

Адаптация общего подхода к конкретному предмету регулирования

Этап 1

Необходимость включения нового вида организации в контур надзора

- Кредитная организация
- Некредитная финансовая организация
- ФинТех-проект
- субъект национальной платежной системы

Комплекс подготовительных мероприятий к включению в контур надзора

- Определение типового состава показателей профиля риска поднадзорной организации
- Разработка методик применения надзорных мер реагирования
- Формирование нормативно-методологической базы знаний

Этап 2

Включение в контур надзора

Нормативное закрепление (часть 1):

- состава и содержания технологических мер обеспечения защиты информации;
- мер анализа уязвимостей программного обеспечения;
- уровня защиты по ГОСТ;
- правил протоколирования.

Этап 3

Нормативное закрепление (часть 2):

- требований проведения оценки соответствия по ГОСТ;
- правил претензионной работы;
- правил информирования ФинЦЕРТ о несанкционированных финансовых операциях.

Формирование профиля риска реализации информационных угроз

Осуществление дистанционного надзора (мониторинга) показателей:
ПНО – показатель уровня несанкционированных операций;
ПОН – показатель операционной надежности;
ПОС – показатель оценки соответствия требованиям ГОСТ;
ИФ – показатель уровня информационного фона.

Этап 4

Надзор за реализацией системы управления риском и капиталом с учетом профиля риска

Этап 5

Банк России

СПАСИБО
ЗА ВНИМАНИЕ

Пункт приема корреспонденции:
Москва, Сандуновский пер., д. 3, стр. 1, телефон +7 495 621-09-61
Почтовый адрес: 107016, Москва, ул. Неглинная, д. 12
Контактный центр: 8 800 250-40-72, +7 495 771-91-00
Факс: +7 495 621-64-65, +7 495 621-62-88
Сайт: www.cbr.ru
Электронная почта: fps@cbr.ru