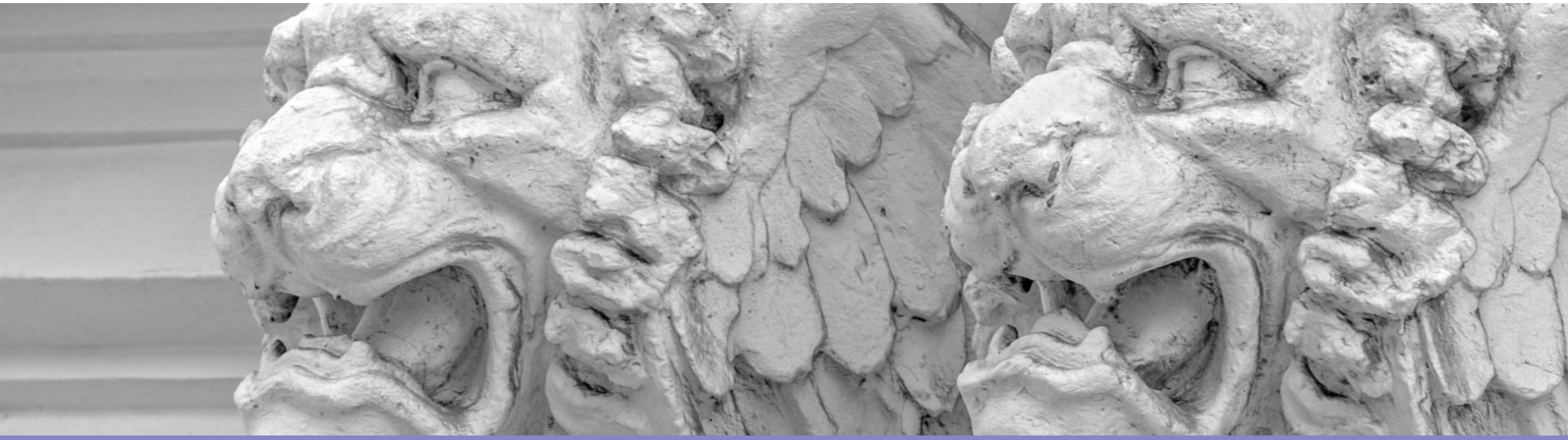
Банк России
Центральный банк Российской Федерации

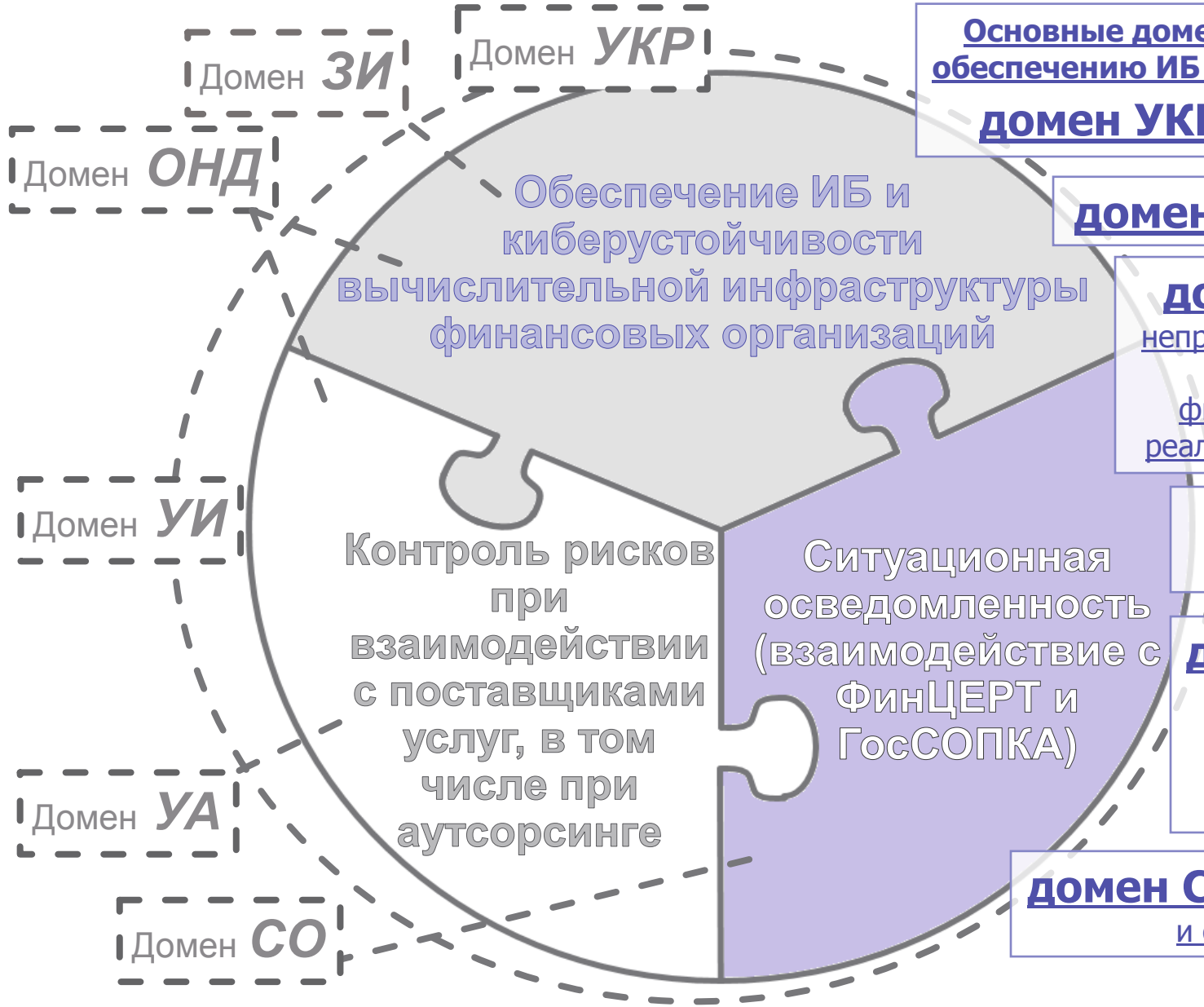


Киберустойчивость как стратегия развития банковской отрасли

Сычев Артем Михайлович

заместитель начальника
Главного управления безопасности и защиты информации
Банка России

13.02.2018



Основные домены видов деятельности по обеспечению ИБ и управлению киберриском:

домен УКР – «управление киберриском»

домен ЗИ – «защита информации»

домен ОНД – «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз»

домен УИ – «управление инцидентами ИБ»

домен УА – «управлением киберриском при аутсорсинге и использовании сторонних информационных услуг (сервисов)»

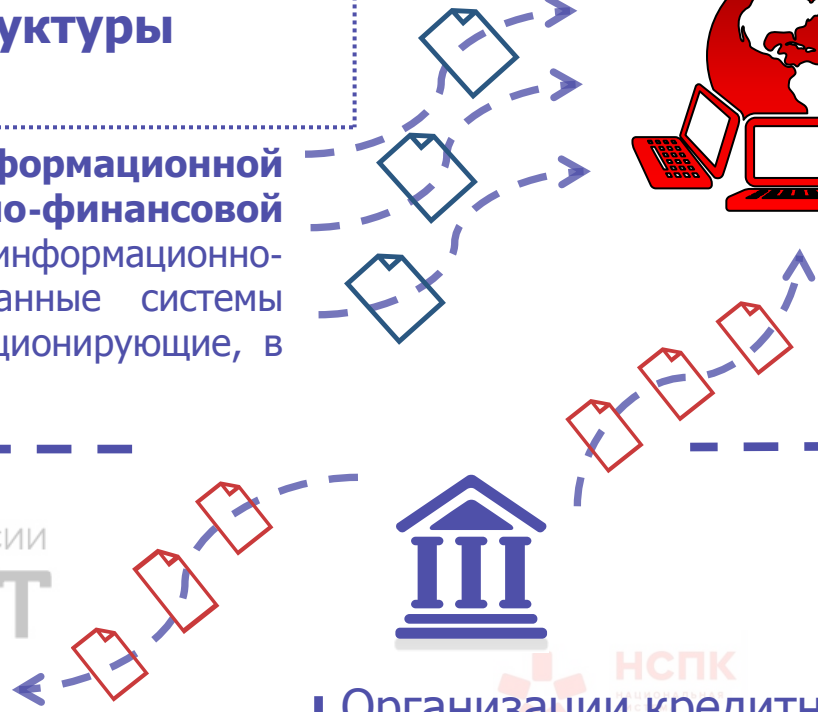
домен СО – «мониторинг киберрисков и ситуационная осведомленность»

ОБЩАЯ СТРУКТУРА ИНФОРМАЦИОННОГО ОБМЕНА

Федеральный закон от 26.07.2017 г. № 187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации

Объекты критической информационной инфраструктуры (объекты КИИ) кредитно-финансовой сферы — информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие, в кредитно-финансовой сфере.

ГосСопка



Банк России

БАНК РОССИИ ФИНЦЕРТ

Организации кредитно-финансовой сферы

НСПК

НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ

МОСКОВСКАЯ БИРЖА

VISA MasterCard Яндекс.Деньги WebMoney QIWI деньги@mail.ru PayPal

Согласно Доктрине информационной безопасности РФ:

- Банк России входит в организационную основу системы обеспечения информационной безопасности РФ;
- организации банковских и иных сфер финансового рынка участников данной системы.

ПРЕСПЕКТИВНЫЙ ИНФОРМАЦИОННЫЙ ОБМЕН

ГосСопка

Организации кредитно-финансовой сферы

Банк России

Регулирование и надзор

БАНК РОССИИ
ФИНЦЕРТ

Определение для каждого типа финансовой организации форм отчетности, предназначенных для получения на ежеквартальной основе информации о метриках (показателях), характеризующих уровень управления киберриском

Осуществление мониторинга, повышение ситуационной осведомленности и реагирование на компьютерные атаки, направленные на Банк России, и организации, поднадзорные Банку России

Закрепление обязанности по детализации экономических показателей, связанных уровнем несанкционированных финансовых операций (транзакций)

Участие в обеспечении информационной безопасности при осуществлении переводов денежных средств в национальной платежной системе.

Установление подходов к оценке качества системы управления рисками и капиталом, оценке экономического положения финансовых организаций на основе показателей операционного риска

Повышение уровня киберграмотности населения путем создания инструмента интерактивного взаимодействия с гражданами

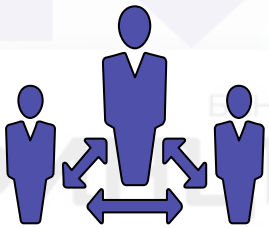
ВИДЫ ДЕЯТЕЛЬНОСТИ

Законотворческая деятельность

Разработан и внесен в Государственную Думу проект федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)»

Нормативная правовая деятельность

Проект указания Банка России «О внесении изменений в 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 обеспечением требований к обеспечению защиты информации при осуществлении переводов денежных средств»



Методологическая деятельность

Разрабатывается проект стандарта Банка России о технологии подготовки, направлении и форматах электронных сообщений для информирования Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Организационная деятельность

Реализация информационного обмена предполагается путем создания автоматизированной системы, используемой ФинЦЕРТ для повышения готовности противостоять информационным угрозам путем организации автоматизированного обмена информации:

об актуальных уязвимостях, информационных угрозах и компьютерных атаках;

о случаях совершения перевода (попытках совершения перевода) денежных средств без согласия клиента, включая обезличенную информацию о расчетных счетах физических лиц, используемых для «выведения» несанкционированно переведенных денежных средствах (счетах «дропов»).

НОРМАТИВНАЯ МЕТОДОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ

Методологическая деятельность

совершенствование комплекса отраслевых документов, устанавливающих требования к обеспечению ИБ и управлению киберриском, для обеспечения наличия отраслевой методологической основы деятельности Банка России и финансовых организаций по противодействию актуальным информационным угрозам и компьютерной преступности

Основные домены видов деятельности по обеспечению ИБ и управлению киберриском:

домен УКР – «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»

Разработано:

2 ГОСТ Р

4 СТО БР ИББС

8 РЕКОМЕНДАЦИЙ

Нормативная правовая деятельность

Область применения:

- защита информации при осуществлении переводов денежных средств;
- осуществление депозитарной деятельности;
- проведение организованных торгов;
- деятельность специализированных депозитариев;
- осуществление деятельности по ведению реестра владельцев ценных бумаг;
- создание и эксплуатация единой автоматизированной системы и перечнях видов информации, предоставляемой страховщиками;
- сохранность и защита информации, полученной в процессе деятельности кредитного рейтингового агентства;
- информационные технологии, используемые операторами услуг платежной инфраструктуры, для целей признания платежной системы национально значимой платежной системой
- обеспечение бесперебойности и непрерывности функционирования официальных сайтов страховщиков и профессионального объединения страховщиков в информационно-телекоммуникационной сети «Интернет» в целях заключения договоров обязательного страхования в виде электронных документов

НОРМАТИВНАЯ МЕТОДОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ

Домен «управление киберриском» (домен УКР)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение информационной безопасности и управление риском реализации информационных угроз. Общие положения» (ввод в действие в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение информационной безопасности и управление риском реализации информационных угроз. Методика оценки соответствия» (ввод в действие в 2020)

Домен «защита информации» (домен ЗИ)

ГОСТ Р «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер защиты информации» (ввод в действие в 2018)

ГОСТ Р «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (ввод в действие в 2018)

Домен «управление инцидентами ИБ» (домен УИ)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Требования и меры организации» (ввод в действие в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Сбор и анализ технических данных» (ввод в действие ГОСТ в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Требования к организации взаимодействия с ФинЦЕРТ Банка России» (ввод в действие ГОСТ в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Методика оценки соответствия» (ввод в действие ГОСТ в 2020)

Домен «управление киберриском при аутсорсинге и использование сторонних информационных услуг (сервисов)» (домен УА)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Аутсорсинг» (ввод в действие СТО в 2018, ввод в действие ГОСТ в 2020)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Использование информационных сервисов» (ввод в действие СТО в 2019, ввод в действие ГОСТ в 2021)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Методика оценки соответствия» (ввод в действие в 2021)

Домен «мониторинг киберрисков и ситуационная осведомленность» (домен СО)

ГОСТ Р «Безопасность финансовых (банковских) операций. Мониторинг киберрисков и ситуационная осведомленность. Требования и меры реализации» (ввод в действие СТО в 2019, ввод в действие ГОСТ в 2020)

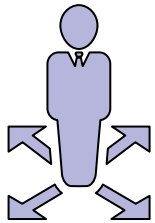
ГОСТ Р «Безопасность финансовых (банковских) операций. Мониторинг киберрисков и ситуационная осведомленность. Методика оценки соответствия» (ввод в действие ГОСТ в 2021)

Домен «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз» (домен ОНД)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение непрерывности выполнения бизнес и технологических процессов. Требования и меры реализации» (ввод в действие СТО в 2020, ввод в действие ГОСТ в 2022)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение непрерывности выполнения бизнес и технологических процессов. Методика оценки соответствия» (ввод в действие ГОСТ в 2021)

Количество участников информационного обмена



Всего: 621

425 - кредитные организации;

103 - некредитные финансовые организации;

7 - разработчики информационных систем;

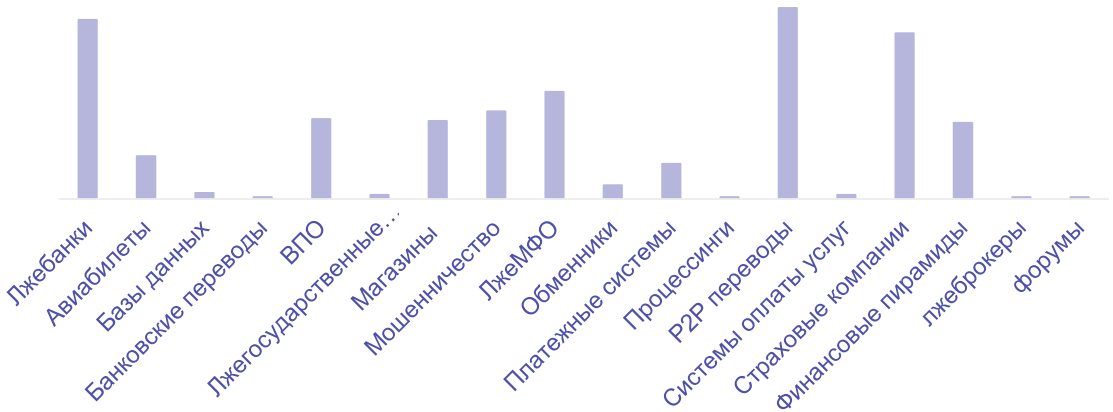
18 - небанковские кредитные организации;

6 - операторы связи; **3** - антивирусные компании;

правоохранительные органы и иные организации.

Взаимодействие и реагирование

Всего: 840



БАНК РОССИИ
ФИНЦЕРТ

По данным, официально предоставляемых кредитными организациями в Банк России, *объем несанкционированных операций*

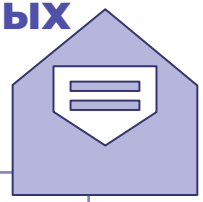
со счетов юридических лиц

- *по итогам за 2017 год составил порядка 1,57 млрд. руб.*
- *в 2016 году – порядка 1,9 млрд. руб.*
- *в 2015 году – порядка 3,8 млрд. руб.*

с использованием платежных карт

- *по итогам за 2017 год составил порядка 0,96 млрд. руб.*
- *в 2016 году – порядка 1,08 млрд. руб.*
- *в 2015 году – порядка 1,15 млрд. руб.*

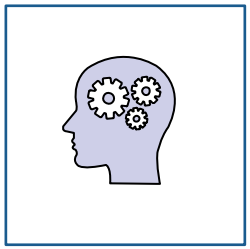
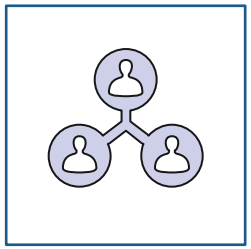
Количество разосланных бюллетеней

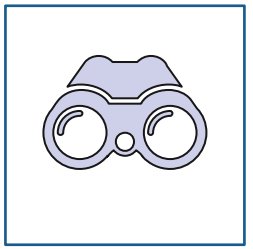


Всего: 337

За 2017: 119

ОБОБЩЕННЫЕ ЦЕЛЕВЫЕ ИНДИКАТОРЫ РЕАЛИЗАЦИИ МЕРОПРИЯТИЙ СТРАТЕГИИ ИБ



Наименование целевого показателя	Текущее значение	2018 год	2020 год
Уровень доверия*	30%	60%	80%
Уровень (удельный вес) несанкционированных финансовых операций (транзакций)** не более	0,005%	0,005%	0,005%

Значение показателей по итогам 2017 года **30% и 0,0016%**

* уровень доверия клиентов и контрагентов финансовых организаций к безопасности реализуемых электронных платежных сервисов (далее – уровень доверия). В перспективе до 2020 года ГУБиЗИ полагает целесообразным достижения 80% уровня доверия клиентов и контрагентов, с последующим сохранением достигнутого уровня

** уровень (удельный вес) несанкционированных финансовых операций (транзакций) по отношению к их общему объему

Банк России
Центральный банк Российской Федерации

Благодарю за внимание!