



Банк России

**РЕАЛИЗАЦИЯ РИСК-ПРОФИЛИРОВАННОГО  
ПОДХОДА ПО ВОПРОСАМ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И  
КИБЕРУСТОЙЧИВОСТИ В ОТНОШЕНИИ  
ПОДНАДЗОРНЫХ ОРГАНИЗАЦИЙ КРЕДИТНО-  
ФИНАНСОВОЙ СФЕРЫ**

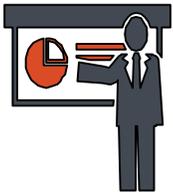
12.09.2019



## Основные цели:



**Обеспечение киберустойчивости**



**Защита прав потребителей финансовых услуг через мониторинг показателей уровня финансовых потерь**



**Содействие развитию инновационных финансовых технологий в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности**

## Цель Банка России в области обеспечения информационной безопасности организаций кредитно-финансовой сферы

Наименование целевого показателя	Целевое значение на <u>2017 год</u>	Фактическое значение за <u>2017 год</u>	Целевое значение на <u>2018 год</u>	Фактическое значение за <u>2018 год</u>	Целевое значение на <u>2020 год</u>
Уровень доверия*	30%	40%	60%	70%	80%
Доля объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт	0,005%	0,0016%	0,005%	0,0018%	0,005%



Показатель доли объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт, не должен превышать 0,005%

\* уровень доверия клиентов и контрагентов финансовых организаций к безопасности реализуемых электронных платежных сервисов



## Субъекты оценки



### Кредитные организации



### Некредитные финансовые организации

Управляющие компании инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда; Специализированные депозитарии инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда; Акционерные инвестиционные фонды (АИФ); Негосударственные пенсионные фонды (НПФ); Осуществляющие деятельность субъектов страхового дела; Осуществляющие брокерскую деятельность; Осуществляющие дилерскую деятельность; Осуществляющие деятельность по управлению ценными бумагами; Осуществляющие деятельность по ведению реестра владельцев ценных бумаг; Осуществляющие депозитарную деятельность; Осуществляющие деятельность организатора торговли; Осуществляющие деятельность по осуществлению функций центрального контрагента; Осуществляющие клиринговую деятельность; Осуществляющие деятельность центрального депозитария; Осуществляющие репозитарную деятельность



### Субъекты национальной платежной системы, не являющиеся кредитными организациями

## Нормативные акты Банка России

устанавливающие требования к обеспечению защиты информации (применяемые для формирования профиля риска)

- Положение Банка России от 17 апреля 2019 г. № 683-П «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»
- Положение Банка России от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России»
- Положение Банка России от 17 апреля 2019 г. № 684-П «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»
- Положение Банка России от 9 июня 2012 г. № 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»



### Формирование зон



Показатель уровня несанкционированных операций  
 ПНО

Показатель операционной надежности  
 ПОН

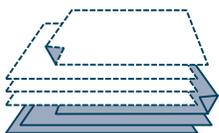
Показатель оценки соответствия  
 ПОС

Показатель качества управления риском  
 КУР

Потери (прямые и косвенные) от реализованного риска информационной безопасности

Степень выполнения требований по информационной безопасности

Степень выполнения требований к системе управления риском информационной безопасности



Формы отчетности (для кредитных организаций)

Вероятность реализации риска информационной безопасности



Оперативный информационный обмен с ФинЦЕРТ об инцидентах защиты информации (основной канал обмена информацией)

#### Установленные требования

- «Безопасность технологии»
- «Безопасность программного обеспечения»
- «Безопасность информационной инфраструктуры»

Показатель уровня информационного фона  
 ИФ

Дополнительный (не основной) показатель риска информационной безопасности



ПНО, ПОН	КО	НФО	СНПС
Подключение поднадзорных организаций к автоматизированной системе обработки инцидентов (АСОИ) для организации информационного обмена с Банком России	✓	✓	✓
Классификация инцидентов защиты информации	✓	✓	✓
Сбор информации об инцидентах защиты информации (ПНО, ПОН)	✓	4 квартал 2019 г.	✓

ПОС	КО	НФО	СНПС
Нормативное закрепление требований по обеспечению информационной безопасности	✓	✓	✓
ГОСТ по защите информации	✓	✓	✓
ГОСТ по обеспечению операционной надежности	2020 г.	2020 г.	2020 г.
Разработка методики оценки соответствия установленным требованиям	✓	✓	✓
Сбор информации по показателю (ПОС)	4 квартал 2019 г. в виде самооценки	4 квартал 2019 г. в виде самооценки	4 квартал 2019 г. в виде самооценки

КУР	КО	НФО	СНПС
Установление базовых требований по управлению риском информационной безопасности	✓	✓	✓
ГОСТ по управлению риском информационной безопасности	2020 г.	2020 г.	2020 г.



## 1. Выполнение расчета

Показатель достаточности капитала необходимого на покрытие потерь от реализации операционного риска, в том числе от риска информационной безопасности:

$$\text{Кнеоб}_{Ki,OP} > (\text{Пно} + \text{Пон} + \text{Побр}) + \text{Ппот}$$

где:

$\text{Кнеоб}_{Ki,OP}$  – капитал, необходимый на покрытие потерь от реализации операционного риска;

$\text{Пно}$  – сумма прямых потерь от реализации событий риска информационной безопасности за период, соответствующий четырем последним кварталам;

$\text{Пон}$  – сумма косвенных потерь от реализации событий риска информационной безопасности за период, соответствующий четырем последним кварталам;

$\text{Побр}$  – сумма денежных средств, по которой получены уведомления клиентов о переводе денежных средств без их согласия, за период, соответствующий четырем последним кварталам, и определяемая в соответствии с отчетностью Банка России по форме №0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств»;

$\text{Ппот}$  – показатель суммы потенциальных потерь от реализации событий риска информационной безопасности, оценка значения которого осуществляется  $\text{Ппот} = K * \sum \text{ССО}$ ,

где:

$K$  – интегральный коэффициент, значение которого зависит от показателя уровня оценки выполнения требований к обеспечению защиты информации;

$\sum \text{ССО}$  – сумма средних остатков за отчетный квартал на корреспондентских счетах кредитной организации, определяемых в соответствии с отчетностью Банка России по форме №0409603 «Сведения об открытых корреспондентских счетах и остатках средств на них».

## 2. Учет показателя риска информационной безопасности при оценке экономического положения финансовой организации

Указание Банка России от 03.04.2017 № 4336-У  
«Об оценке экономического положения банков»

Изменение (понижение) группы кредитной организации при повышении уровня риска





Банк России

СПАСИБО ЗА ВНИМАНИЕ!

