



АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ:
ПРОТИВОДЕЙСТВИЕ СОВЕРШЕНИЮ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ
КЛИЕНТОВ

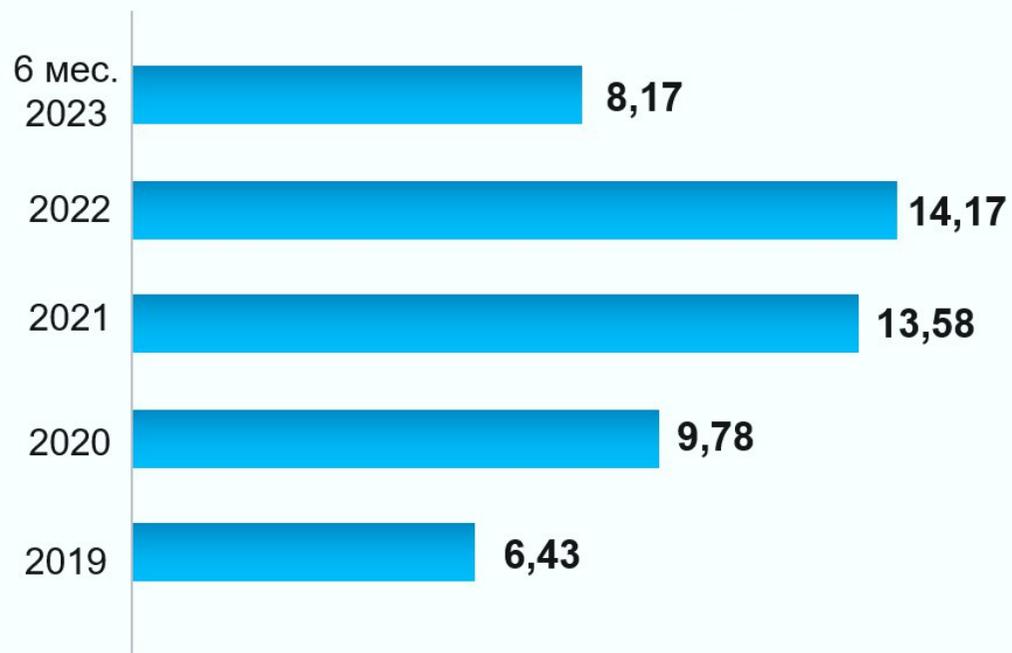
ГРЕБЕННИКОВА ИННА ДМИТРИЕВНА

И.О. УПРАВЛЯЮЩЕГО ОТДЕЛЕНИЕМ ПО БЕЛГОРОДСКОЙ ОБЛАСТИ ГЛАВНОГО
УПРАВЛЕНИЯ БАНКА РОССИИ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

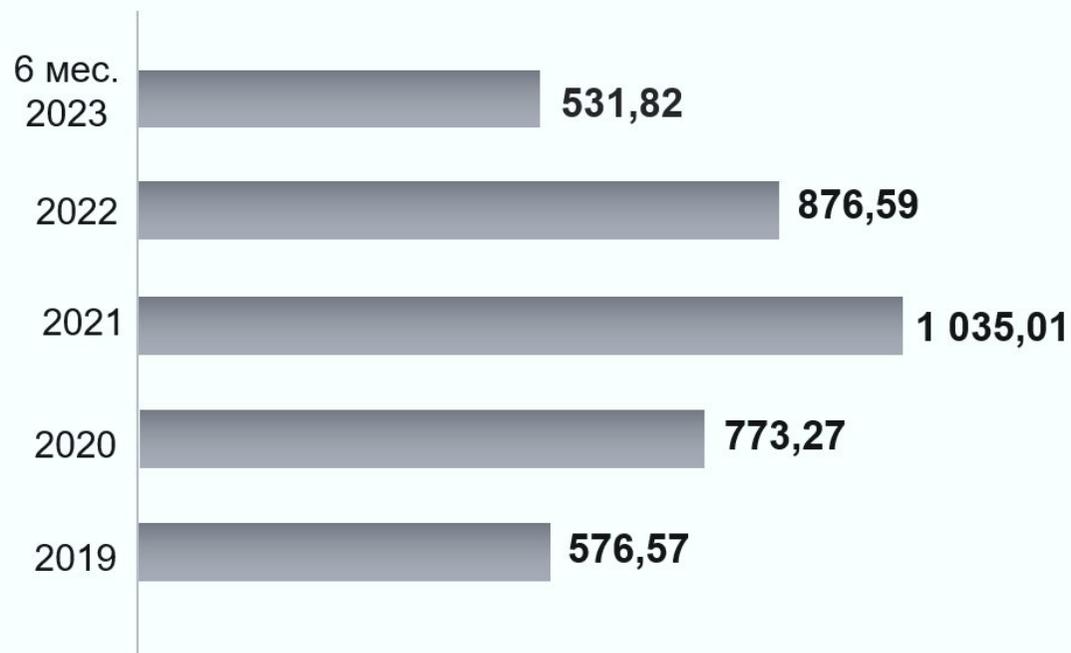
2023 г.

ДИНАМИКА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ (ФИЗИЧЕСКИЕ И ЮРИДИЧЕСКИЕ ЛИЦА)

Объем ОБС, млрд руб.

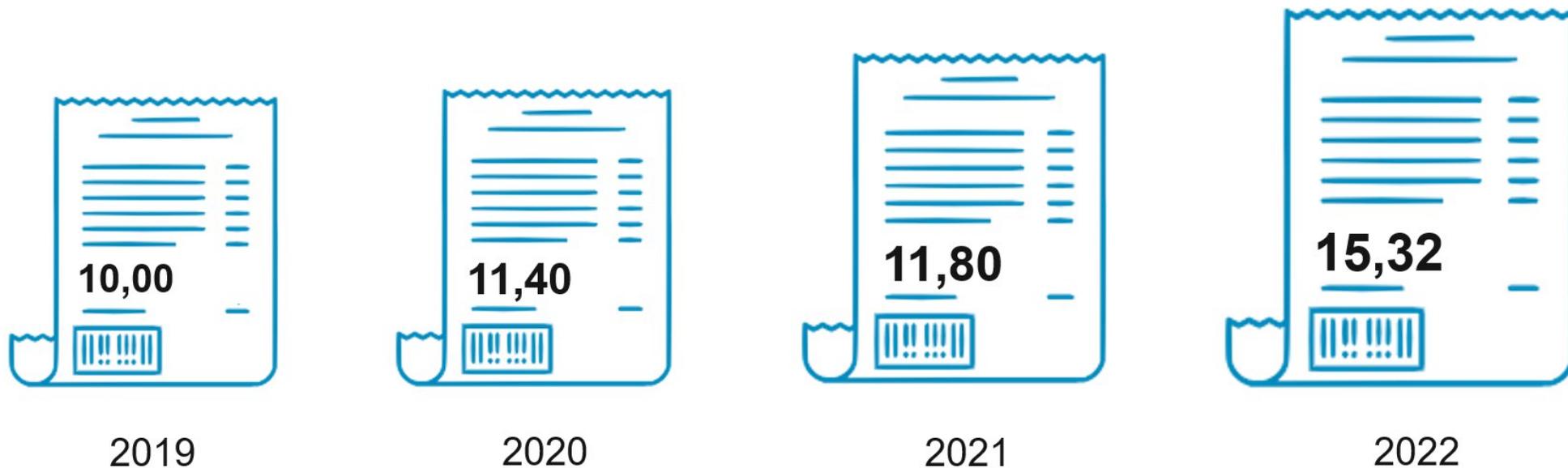


Количество ОБС, тыс. ед.



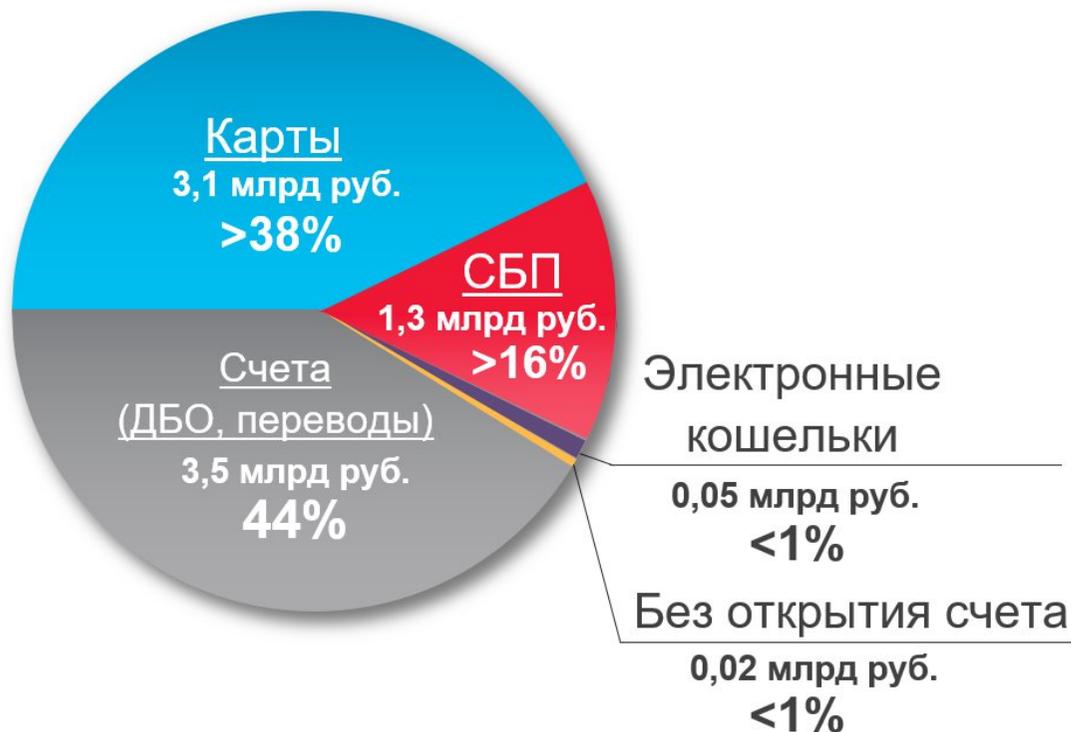
ПРЕДОТВРАЩЕННЫЕ ОБС: 9,3 млн попыток на 1 623,13 млрд руб.

СРЕДНИЙ ЧЕК ХИЩЕНИЙ, ТЫС. РУБ. (ФИЗИЧЕСКИЕ ЛИЦА)

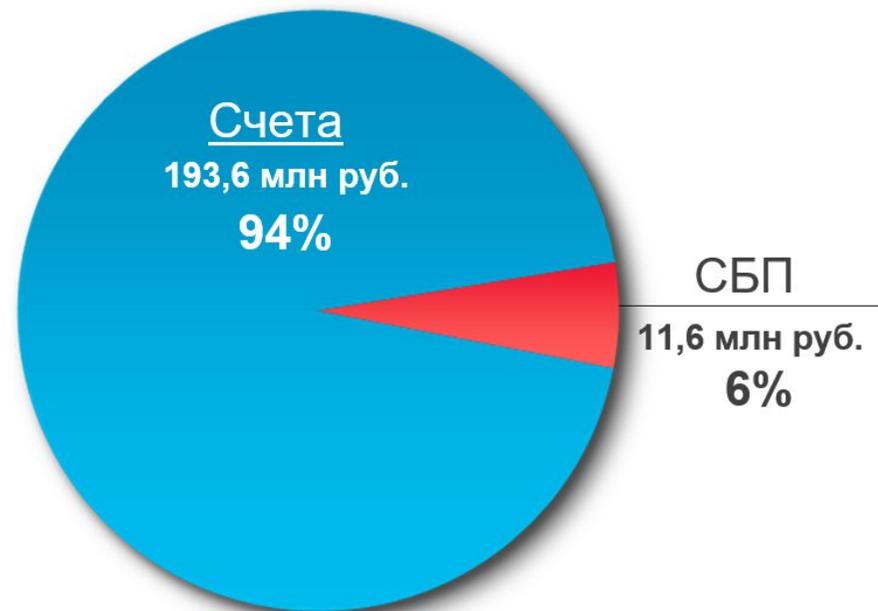


ТИПЫ СОВЕРШЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ (ЗА 6 МЕСЯЦЕВ 2023 ГОДА)

Физические лица

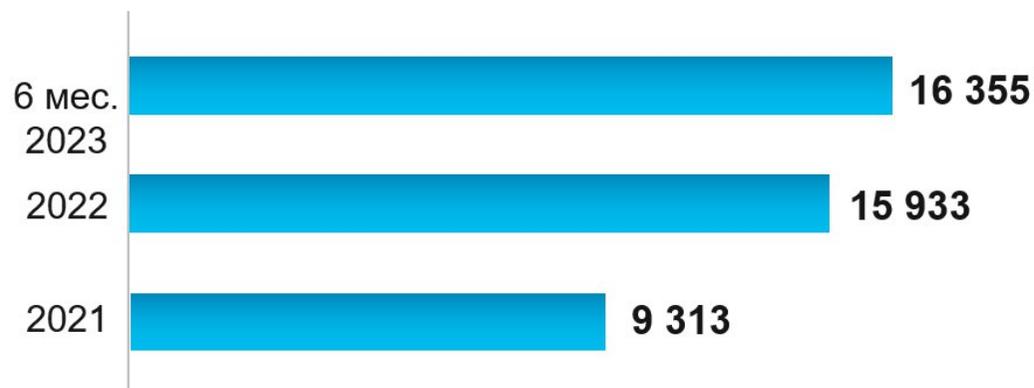


Юридические лица

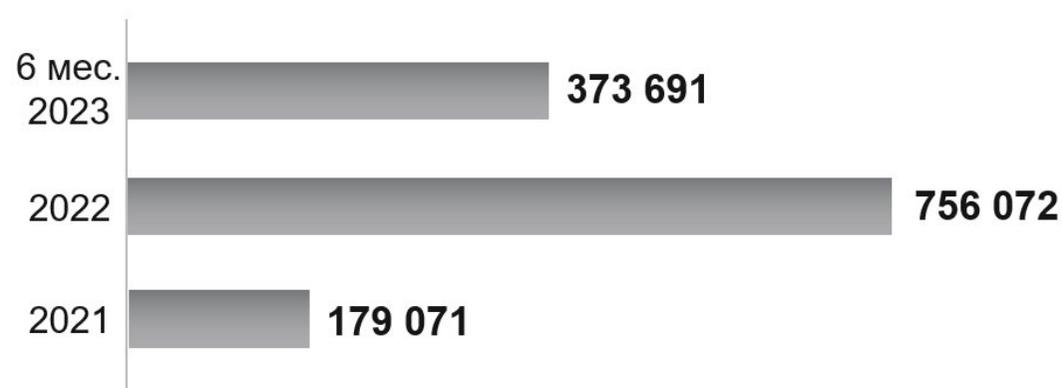


МЕРЫ РЕАГИРОВАНИЯ БАНКА РОССИИ

Количество доменов, направленных на блокировку в ГП РФ и регистраторам доменных имен, ед.



Количество телефонных номеров, направленных операторам связи в целях блокировки, ед.



КИБЕРУЧЕНИЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ



вероятность реализации сценария



организация эшелонированной системы защиты информации

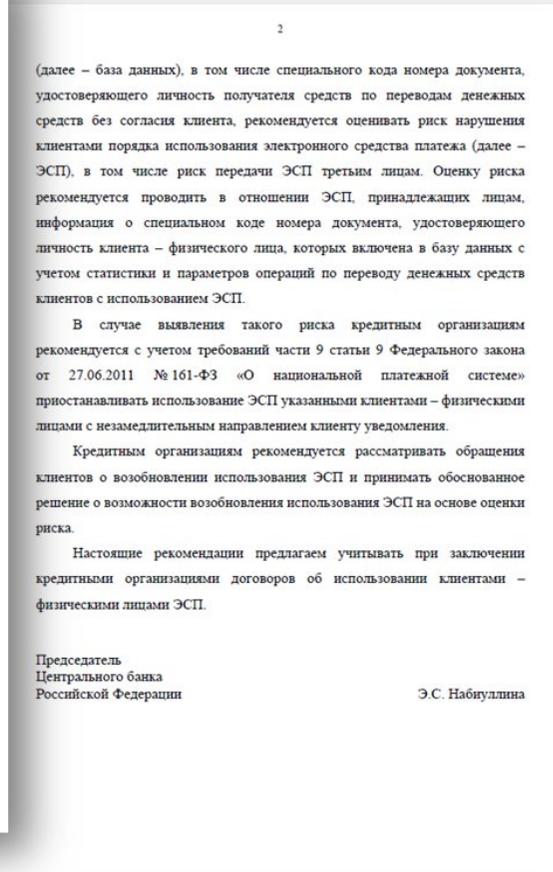
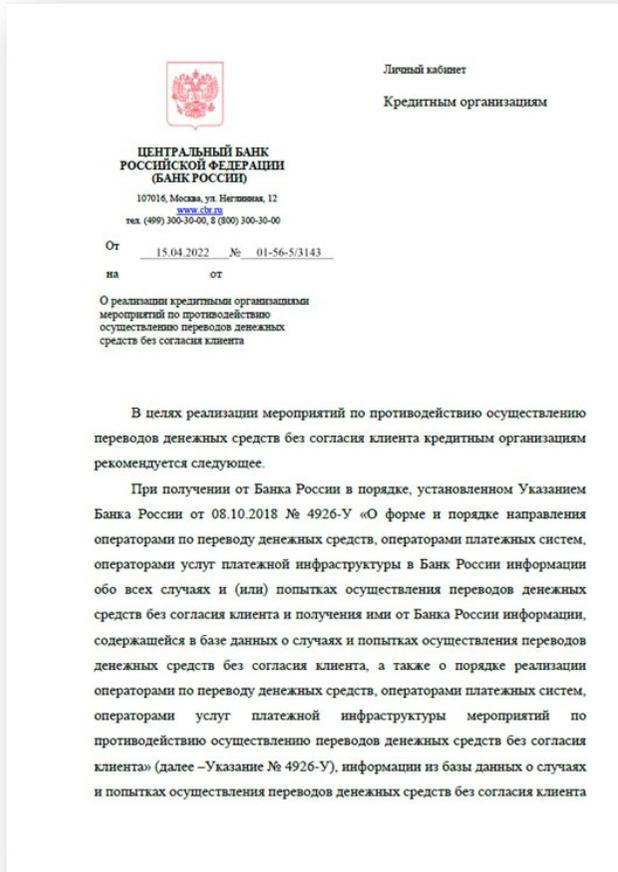


возможность своевременно выявить и классифицировать события ИБ



обеспечение своевременной осведомленности персонала и иных служб

РЕКОМЕНДАТЕЛЬНОЕ ПИСЬМО БАНКА РОССИИ ОБ ОТКЛЮЧЕНИИ КАНАЛОВ ДБО ДРОППЕРАМ



Банкам рекомендуется оценивать риск нарушения клиентами порядка использования электронного средства платежа

В случае выявления такого риска банкам рекомендуется с учетом требований ФЗ № 161-ФЗ приостанавливать использование ЭСП указанным клиентам – физическим лицам с незамедлительным направлением клиенту уведомления

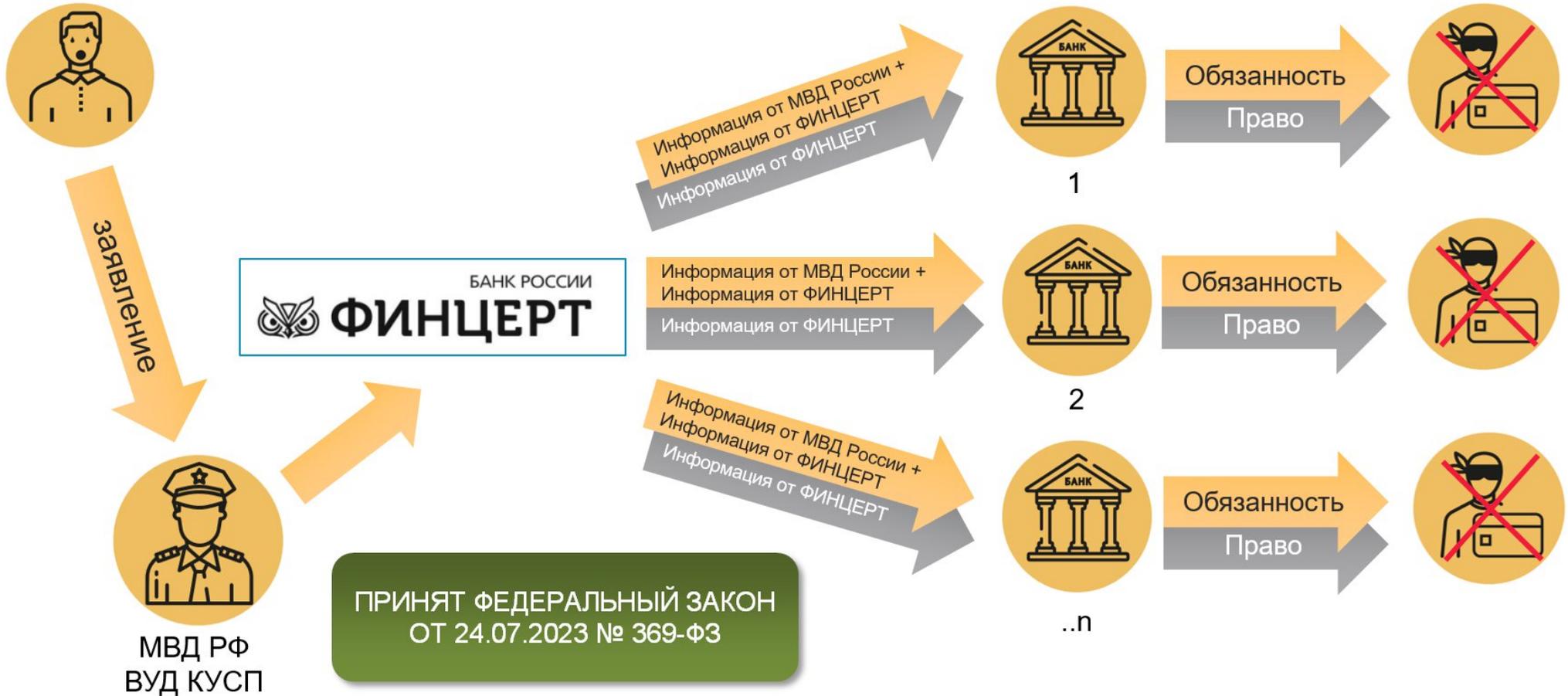
ИЗМЕНЕНИЯ В 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»: ОБМЕН ИНФОРМАЦИЕЙ С МВД РОССИИ



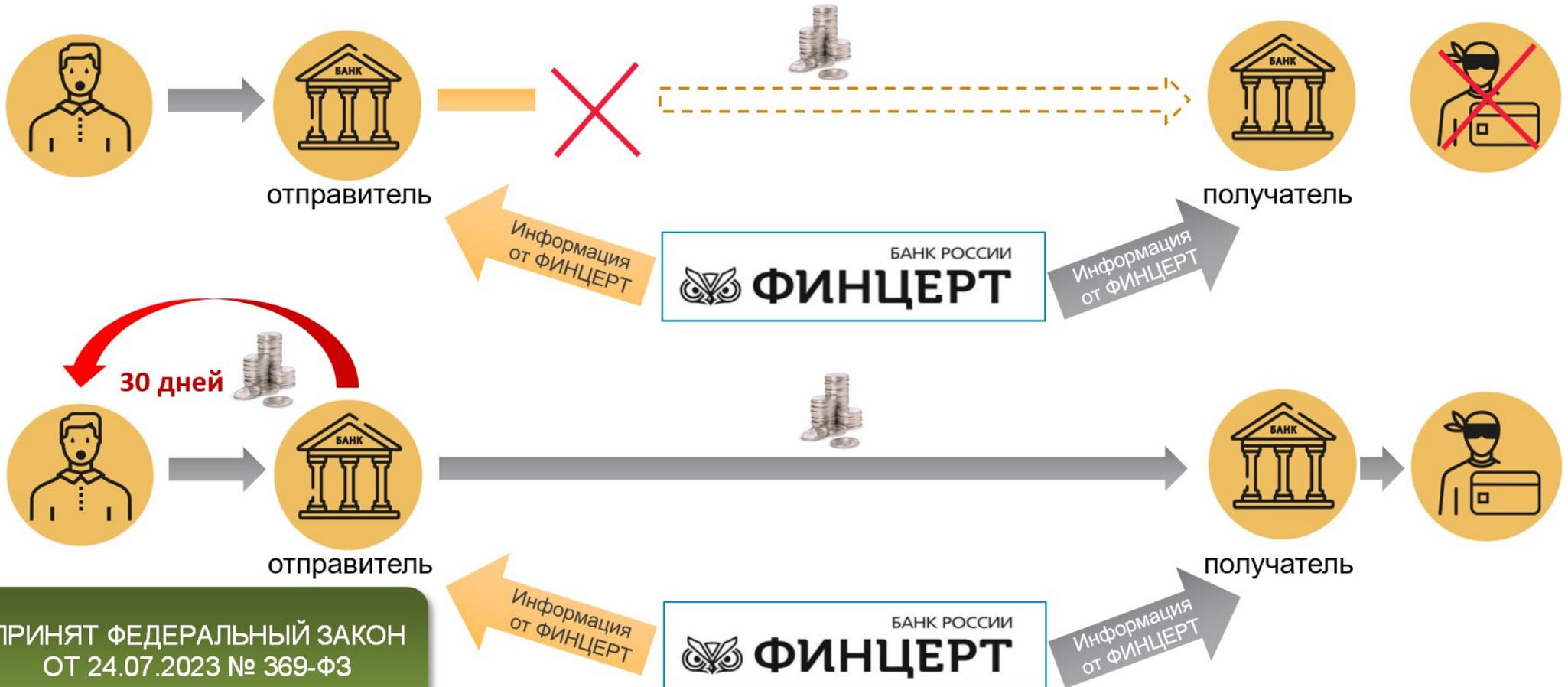
ИЗМЕНЕНИЯ В 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»: ВНЕДРЕНИЕ «ПЕРИОДА ОХЛАЖДЕНИЯ»



ИЗМЕНЕНИЯ В 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»: ОТКЛЮЧЕНИЕ КАНАЛОВ ДБО ДРОППЕРАМ



ИЗМЕНЕНИЯ В 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»: НОВЫЙ ПОРЯДОК ВОЗВРАТА ПОХИЩЕННЫХ СРЕДСТВ



ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ?



1

**Заблокируйте
карту**

- в мобильном приложении банка
- звонком на горячую линию банка
- личным обращением в отделение банка

 **сразу же**

2

**Сообщите
в банк**

 **в течение
суток**

3

**Напишите
заявление в
ПОЛИЦИЮ**

- при личном обращении
в ближайший отдел ОВД

 **как можно
скорее**

Денежные средства с моего счета
№ _____

*(указать номер(а) счета(ов) получателя(лей) денежных
получателя(лей) денежных средств и/или номер(а) банковской(их) и
средств)*

Причиненный мне ущерб оцениваю в разм
(прописью) рублей, который является для меня

(значительным/не значительным, крупн

Учитывая изложенное, прошу провести по
заявлению фактам процессуальную поверку, во
привлечь виновных лиц к уголовной ответственнОб уголовной ответственности по ст. 30
заведомо ложного доноса мне известно.

Приложение:

(выписка по лицевому счету заявителя из банка плательщика, рекви

_____, _____.20 ____ г.

(под

В _____
(наименование отдела полиции)

от гражданина _____

_____,
(ФИО заявителя полностью)

проживающего/зарегистрированного по адресу: _____

_____,
_____тел.: _____
*(контактный телефон заявителя)*Заявление
о хищении денежных средств

Прошу привлечь к уголовной ответственности неизвестное мне лицо
(если известно, то указать его ФИО, номер телефона и иные известные
данные), которое (число, месяц, год, примерное время хищения) похитило
денежные средства в сумме _____ (прописью)
рублей с моего счета

№ _____

(номер лицевого счета заявителя, дата и место его открытия, № банковской карты заявителя)

В _____ банке

*(наименование банка плательщика, регистрационный номер банка плательщика, фактический адрес банка
плательщика или его структурного подразделения, в котором открыт счет заявителя).*

Хищение денежных средств совершено при следующих
обстоятельствах:

(краткое описание происшествия)

Форма «Сообщения-запроса о хищении денежных средств с банковского счета», в рамках новой модели

Наименование и адрес
кредитной организации
(банка)

СООБЩЕНИЕ-ЗАПРОС о хищении денежных средств с банковского счета

Настоящим сообщая Вам о поступлении сообщения о хищении денежных средств с банковского счета граждан (организации)

	Данные МВД	Примечание
Территориальный ОВД		
Дата и номер регистрации в КУСП		
Ф.И.О. заявителя (данные организации, в т.ч. ИНН/ОГРН)		
№ счета заявителя (отправителя, плательщика), дата и место открытия		
Фабула хищения		
Дата и время операции		
Сумма перечисленных (похищенных) денежных средств		

Указанная операция совершена без согласия лица - клиента Вашей кредитной организации с использованием сервиса дистанционного банковского обслуживания, включая интернет-банкинг (далее - ДБО), то есть денежные средства получены третьими лицами преступным путём.

Эффективным способом противодействия указанным мошенническим действиям является отключение кредитными организациями в порядке, предусмотренном договором, клиентов / приостановление обслуживания клиентов через ДБО при поступлении соответствующей информации.

На основании изложенного и, руководствуясь ст. 13 ФЗ «О Полиции», ст.ст. 4, 7, 7.2, 7.3 Федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Письмом ЦБ РФ от 27.04.2007 № 60Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)», сообщая об изложенном,

ПРОШУ:

1. Принять меры в соответствии с требованиями ст.ст. 4, 7, 7.2, 7.3 Федерального закона от 07.08.2001 № 115-ФЗ;
2. Рассмотреть вопрос о приостановлении/прекращении доступа к ДБО по счету получателя денежных средств, в том числе направить указанное сообщение в кредитную организацию (банк) получателя денежных средств для принятия мер;
3. По установлению счета получателя похищенных денежных средств, в том числе открытого на «дропа», направить информацию в кредитную организацию (банк), обслуживающий указанный счет, для принятия мер и уведомления о принятых мерах правоохранительного органа по месту регистрации сообщения;
4. О принятых Вами мерах, в том числе подробные сведения об использовании третьими лицами платежных карт (иных электронных средств платежа), оформленных на подставных физических лиц (дропов), а также онлайн-сервисов с применением не принадлежащего кредитной организации специального программного обеспечения, которое в автоматическом режиме заполняет необходимые данные для осуществления перевода денежных средств, электронных денежных средств, прошу уведомить нас **в срок 5 суток** с момента поступления указанного сообщения .

Должность

Звание
Контактный номер телефона сотрудника

И.О. Фамилия

КАРТА СВЯЗИ

сотрудников правоохранительных органов и работников кредитных организаций, уполномоченных взаимодействовать при выявлении фактов мошеннических действий и хищений денежных средств с банковских счетов клиентов, в рамках новой модели

5	ПАО «Сбербанк»
6	ПАО «Банк ВТБ»
7	АО «Россельхозбанк»

КАРТА СВЯЗИ
 сотрудников правоохранительных органов и работников кредитных организаций, уполномоченных взаимодействовать при выявлении фактов мошеннических действий и хищений денежных средств с банковских счетов клиентов

№ п/п	Наименование организации	ИНН, количество подразделений в субъекте	Ф.И.О.	Занимаемая должность	Контактный телефон	E-mail
1	УМВД России по Белгородской области					
2	Прокуратура Белгородской области					
3	Отделение по Белгородской области ГУ Банка России по Центральному федеральному округу					
4	АО УКБ «Белгородсоцбанк»					

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ

-  Не сообщайте никому личную и финансовую информацию (данные карты)
-  Установите антивирусные программы на все свои гаджеты и регулярно обновляйте их
-  Не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам
-  Не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы
-  Заведите отдельную банковскую карту для покупок в Интернете

**Будьте бдительны: не действуйте
второпях и проверяйте информацию!**



ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ



Самостоятельно звоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка



Установите двухфакторный способ аутентификации – например, логин и пароль + подтверждающий код из СМС



Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с

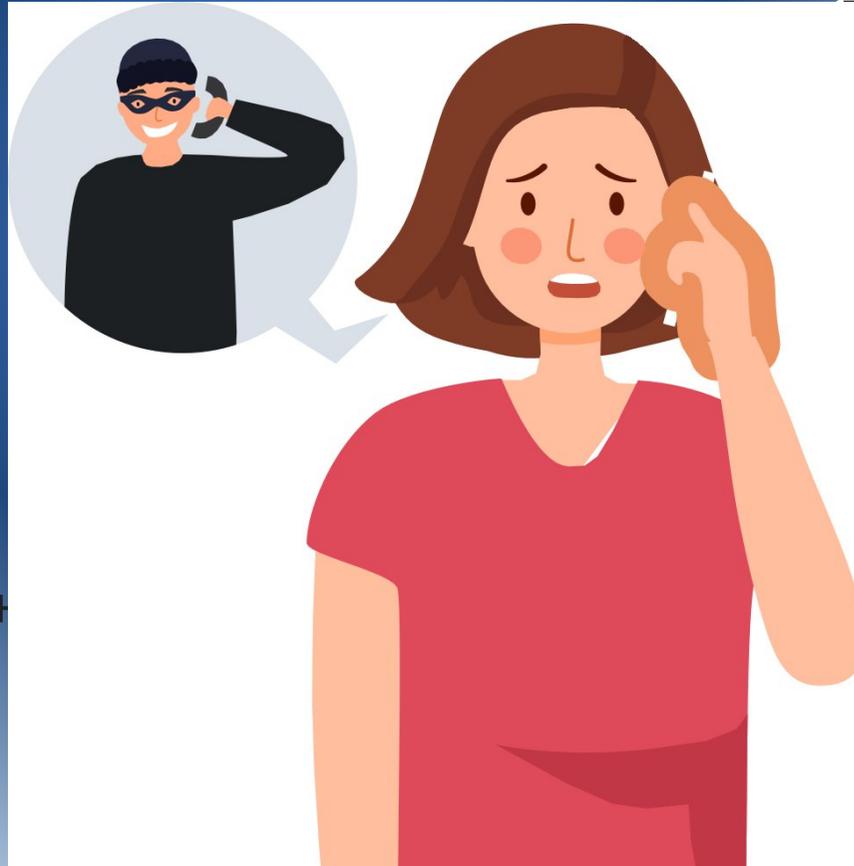


Будьте бдительны: не действуйте второпях и проверяйте информацию!

Расскажите эти правила поведения своим друзьям и знакомым!

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

- 1** Не отвечайте на звонки с незнакомых номеров
- 2** Прервите разговор, если он касается финансовых вопросов
- 3** Не торопитесь принимать решение
- 4** Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам



Самостоятельно позвоните близкому человеку / в банк / в организацию

Не перезванивайте по незнакомым номерам



- ПРИНЯТЬ ПРЕДЛАГАЕМУЮ ОТДЕЛЕНИЕМ БЕЛГОРОД ГУ БАНКА РОССИИ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ К ВНЕДРЕНИЮ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ, ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И КРЕДИТНЫХ ОРГАНИЗАЦИЙ.
- ОТДЕЛЕНИЮ БЕЛГОРОД НАПРАВИТЬ СООТВЕТСТВУЮЩИЕ ТИПОВЫЕ ФОРМЫ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ И КРЕДИТНЫЕ ОРГАНИЗАЦИИ.
- ЗАИНТЕРЕСОВАННЫМ УЧАСТНИКАМ ВЗАИМОДЕЙСТВИЯ В РАБОЧЕМ ПОРЯДКЕ ОРГАНИЗОВАТЬ ОБМЕН ИНФОРМАЦИЕЙ ДЛЯ МОНИТОРИНГА РЕЗУЛЬТАТИВНОСТИ И ВЫЯВЛЕНИЯ ПРОБЛЕМ ПРИМЕНЕНИЯ НОВОЙ МОДЕЛИ.



СПАСИБО ЗА ВНИМАНИЕ!