Банк России

Финтрек

5 апреля, 10:00

Кибермошенничество. Актуальные схемы и меры противодействия

Алексей Голенищев

Начальник Центра мониторинга и анализа информационной безопасности и киберустойчивости, Департамент информационной безопасности, Банк России

Какие темы мы разберём сегодня?

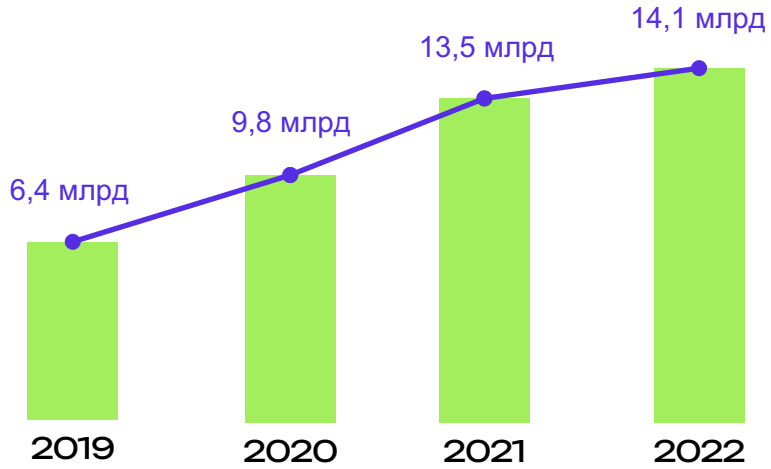
1. Кибермошенничество
2. Схемы мошенничества
3. Как не стать жертвой злоумышленников

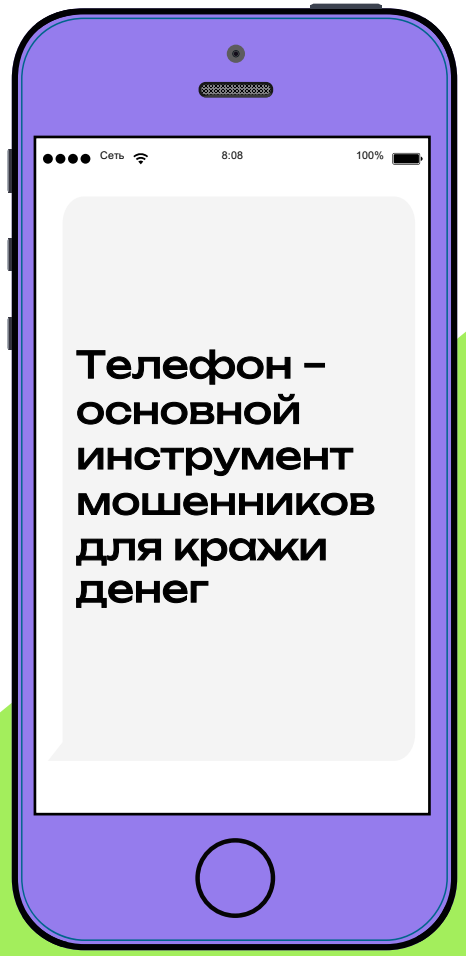
Кибермошенничество

Сумма потерь

15 300 ₽

в среднем злоумышленники похищают
у человека за одну операцию





Банк России

Финтрек

Схемы мошенничества

Как распознать телефонного мошенника

Мошенники пытаются вывести человека из спокойного состояния и отключить у него логическое мышление. Они торопят и оказывают давление.

В основе методов лежит манипулирование отрицательными эмоциями человека: страх, паника, нервозность

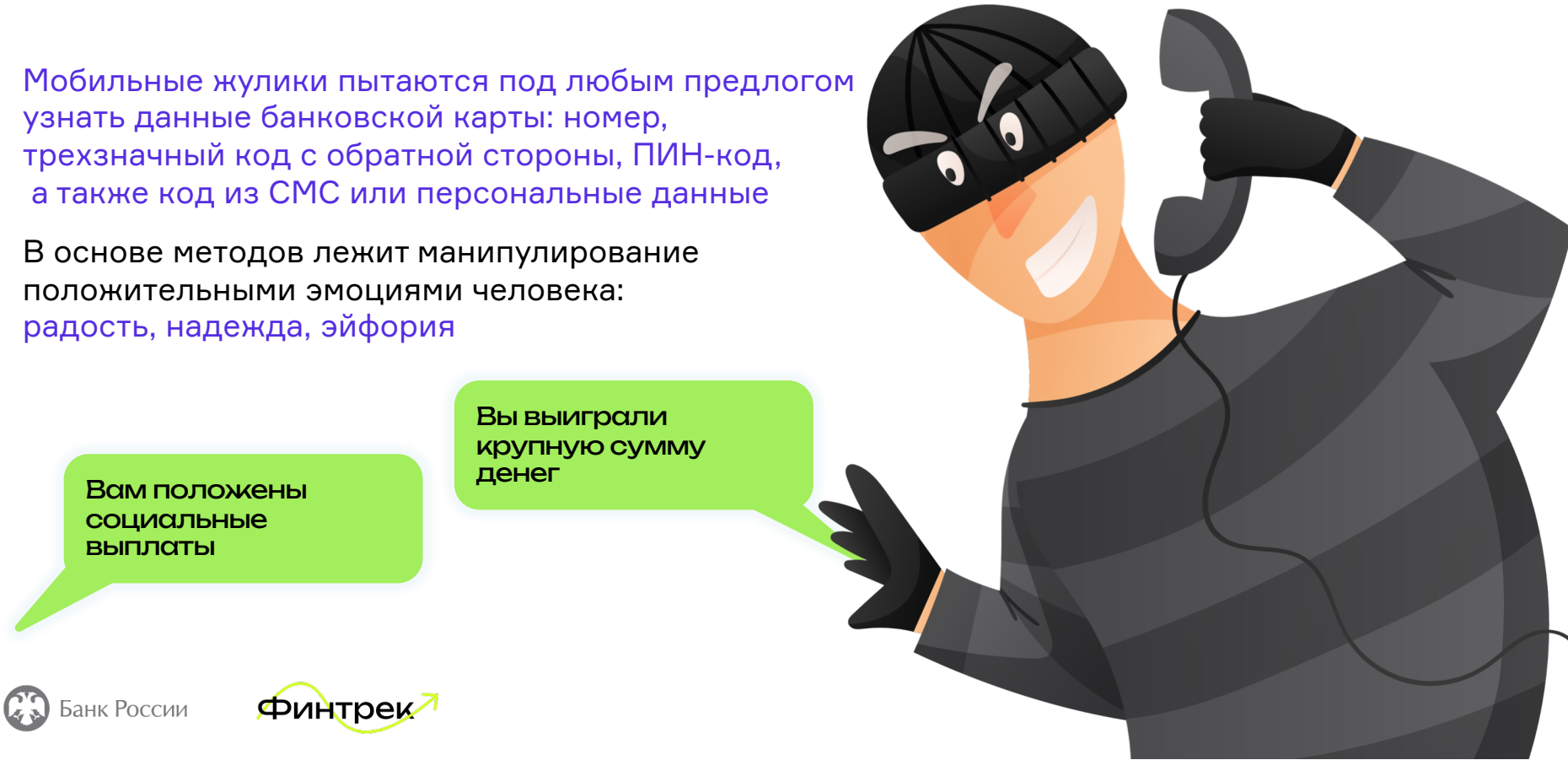
Банк России

Финтрек

Как распознать телефонного мошенника

Мобильные жулики пытаются под любым предлогом узнать данные банковской карты: номер, трехзначный код с обратной стороны, ПИН-код, а также код из СМС или персональные данные

В основе методов лежит манипулирование положительными эмоциями человека: радость, надежда, эйфория



Банк России

Финтрек

Схемы аферистов часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события

- Представляются работниками Центрального банка Российской Федерации
- Представляются сотрудниками правоохранительных органов
- Звонят гражданам под видом сотрудников службы поддержки оператора сотовой связи
- Представляются сотрудниками кредитных организаций
- Предлагают перевести деньги на «безопасный» (защищенный) счет

Финтрек

Как не стать жертвой мошенников

Банк России

Финтрек

Телефонные мошенники

Правила поведения

- Не отвечайте на звонки с незнакомых номеров
- Положите трубку
- Не торопитесь принимать решения
- Проверьте информацию в официальных источниках
- Позвоните сами близкому человеку или в организацию
- Не перезванивайте по незнакомым номерам

Мошенники в Интернете

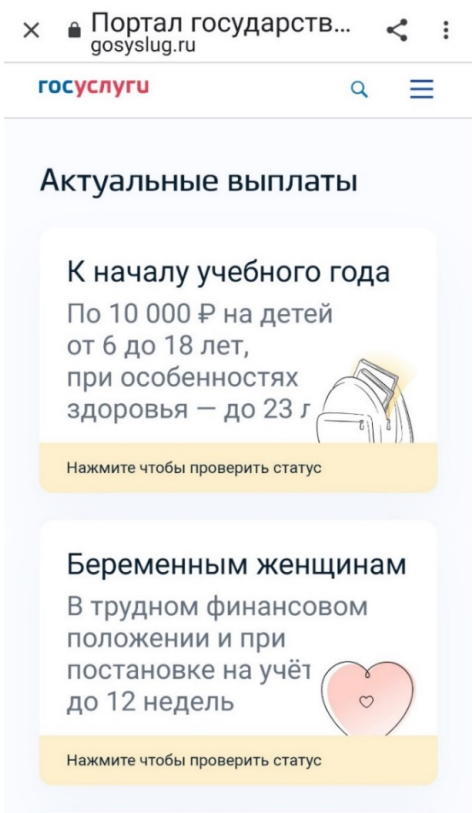
Признаки фишинговых сайтов

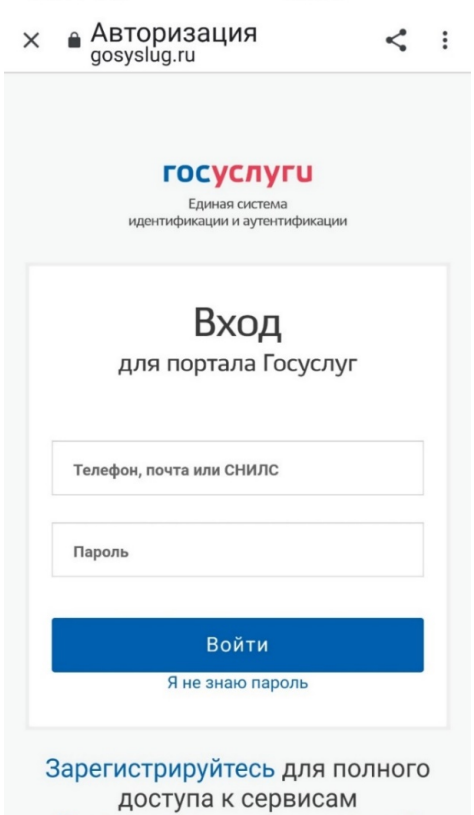
- Ошибки в адресе сайта
- Сайт состоит из 1 страницы, предназначенной **только для ввода данных**
- Отсутствует замочек
- В названии сайта нет **https**
- **Ошибки** в тексте и дизайне
- Побуждают ввести свои личные/финансовые данные
- Побуждают скачать файл, установить программу

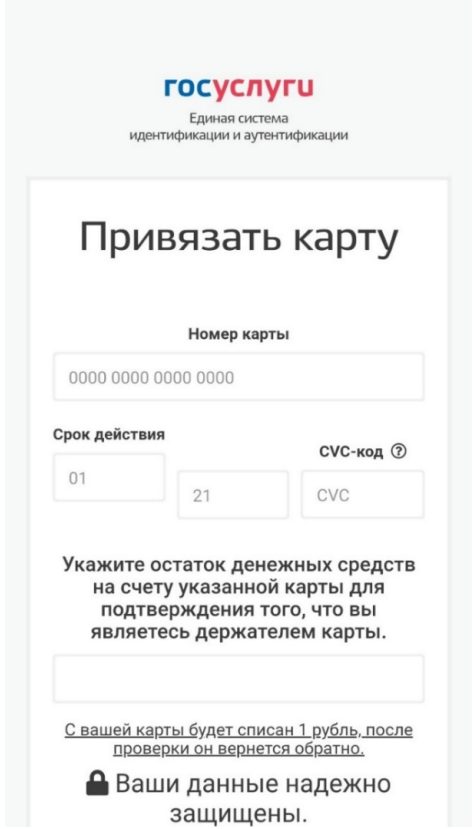
Виды мошенничества в интернете

- Кража информации о кредитных карточках
- «Нигерийские письма»
- Туризм
- Интернет-магазины и аукционы
- Предложение работы
- Сбор пожертвований
- Восстановление кредитной истории
- Льготные кредиты
- Инвестиции

Сайты, маскирующиеся под Госуслуги







Новостной фишинг

Безопасное использование мобильных устройств

1. Старайтесь не использовать облачные хранилища и не храните там резервные копии ваших телефонов

2. Используйте **2-х факторный** способ аутентификации (логин\пароль + вход по коду из SMS)

3. В личном кабинете сотового **оператора установите вход по одноразовому паролю**

4. При получении сообщения о том, что ваша **SIM-карта перевыпущена**, сразу обратитесь в ваш банк для блокировки счета

5. Номер телефона для получения одноразовых паролей от банка **не должен быть в открытом доступе** (на сайтах, в соцсетях, объявлениях). Для этих целей купите отдельную SIM-карту

6. Если вам звонят из банка, у вас **никогда не спросят** номер карты, кодовое слово и пароли из SMS

7. Если вам предлагают прислать задаток, отменить операцию, разблокировать карту и прочее – **никогда не сообщайте пароли из SMS и CVV карт**

Чек-лист

Как не стать жертвой мошенников

- Не сообщайте никому и никогда свои паспортные данные и банковские сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код
- Не совершайте операции по счету по просьбе незнакомых людей
- Самостоятельно звоните в свой банк по номеру телефона, указанному на обратной стороне карты или на его сайте
- Совершайте покупки в Интернете только на проверенных сайтах, для онлайн-покупок заведите отдельную карту
- По возможности установите антивирус на все устройства и обновляйте его
- Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и т.д.

Совет

Банк России

Финтрек

1 Заблокировать карту

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

Срочно

2 Сообщить в банк

В течение суток

3 Написать заявление в полицию

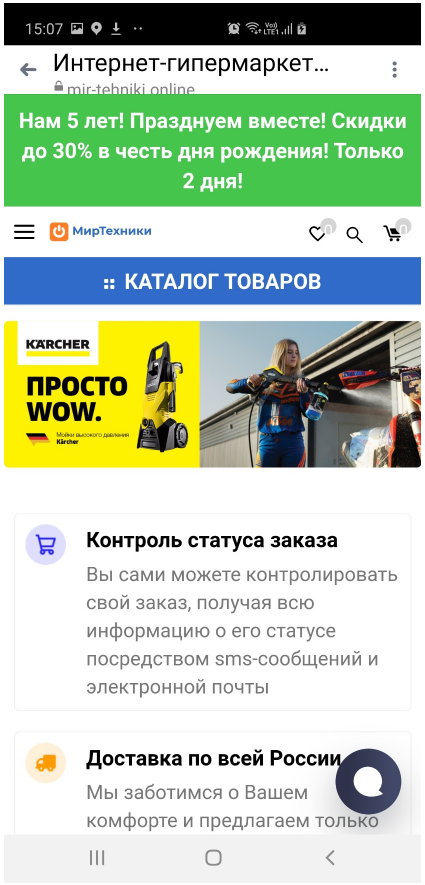
личное обращение в ближайший отдел ОВД

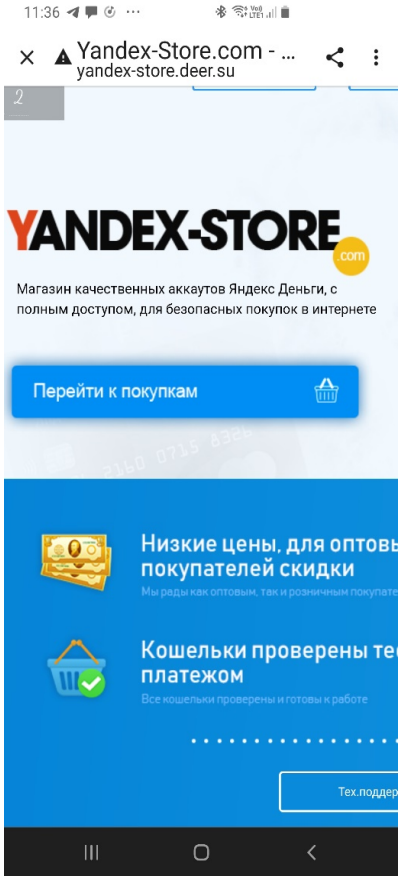
Как можно скорее

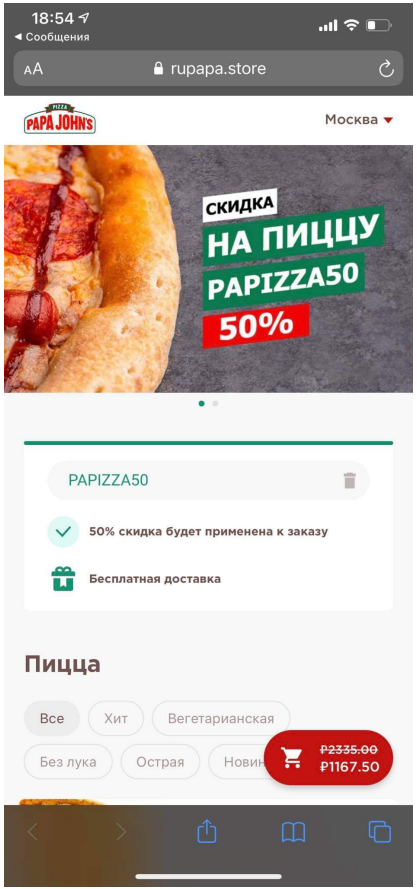
Разбор кейсов

Банк России

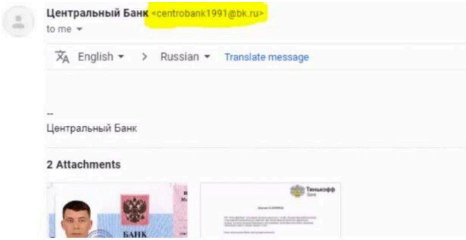
Финтрек


15:07
Интернет-гипермаркет...
mir-tehniki.online
Нам 5 лет! Празднуем вместе! Скидки до 30% в честь дня рождения! Только 2 дня!
МирТехники
:: КАТАЛОГ ТОВАРОВ
KÄRCHER
ПРОСТО WOW.
Контроль статуса заказа
Вы сами можете контролировать свой заказ, получая всю информацию о его статусе посредством sms-сообщений и электронной почты
Доставка по всей России
Мы заботимся о Вашем комфорте и предлагаем только


11:36
Yandex-Store.com - ...
yandex-store.deer.su
YANDEX-STORE
.com
Магазин качественных аккаутов Яндекс Деньги, с полным доступом, для безопасных покупок в интернете
Перейти к покупкам
Низкие цены, для оптовы
покупателей скидки
Кошельки проверены те
платежом
Все кошельки проверены и готовы к работе
Тех.поддер


18:54
Сообщения
AA
rupapa.store
PAPA JOHN'S
Москва
СКИДКА
НА ПИЦЦУ
PAPIZZA50
50%
PAPIZZA50
50% скидка будет применена к заказу
Бесплатная доставка
Пицца
Все
Хит
Вегетарианская
Без лука
Острая
₽2335.00
₽1167.50

Социнженерия стала более «подготовленной»



Фейковое удостоверение сотрудника службы безопасности

Тинькофф Банк

Документ № 2547899125

АО "Тинькофф Банк" настоящим письмом уведомляет, что Вы, Лекарев Евгений Евгеньевич, стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договора банковского обслуживания, необходимо выполнить процедуру обновления единого номера лицевого счета.

Ниже представлены Ваши действующие реквизиты:

Обновленный счет: 408[redacted]20
Срок действия обновленных реквизитов составляет 24 часа.

Специалист Службы Безопасности Центрального Банка: Волков Илья Сергеевич
Финансово-ответственное лицо: Волков Илья Сергеевич

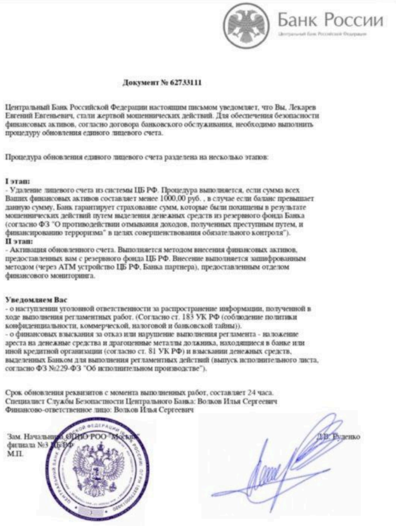
** Обращаем Ваше внимание, получатель является финансово-ответственным лицом.*
** После обновления реквизитов все финансовые активы, которые находились на счетах клиента до мошеннических действий будут восстановлены.*

Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: АО "Тинькофф Банк"
БИК: 044525974
ИНН: 7710140679
Корр.сч.: 30101810014525000974
Расчетный счет(лицевой): 30232810100000000004

Зам. Начальника ОПЮ РОО "Москва" Тинькофф (АО)
М.П.

А.М. Колесников



Банк России

Документ № 62733111

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы, Лекарев Евгений Евгеньевич, стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договора банковского обслуживания, необходимо выполнить процедуру обновления единого лицевого счета.

Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Удаление лицевого счета из системы ЦБ РФ. Процедура выполняется, если сумма всех Ваших финансовых активов составляет менее 1000,00 руб. , в случае если баланс превышает данную сумму, Банк гарантирует страхование сумм, которые были похищены в результате мошеннических действий путем выделения денежных средств из резервного фонда Банка (согласно ФЗ "О противодействии отмывания доходов, полученных преступным путем, и финансированию терроризма" в целях совершенствования обязательного контроля").

II этап:
- Активация обновленного счета. Выполняется методом внесения финансовых активов, предоставленных вам с резервного фонда ЦБ РФ. Внесение выполняется зашифрованным методом (через АТМ устройство ЦБ РФ, Банка партнера), предоставленным отделом финансового мониторинга.

Уведомляем Вас
- о наступлении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (Согласно ст. 183 УК РФ (соблюдение политики конфиденциальности, коммерческой, налоговой и банковской тайны)).
- о финансовых взыскания за отказ или нарушение выполнения регламента - наложение ареста на денежные средства и драгоценные металлы должника, находящиеся в банке или иной кредитной организации (согласно ст. 81 УК РФ) и взыскании денежных средств, выделенных Банком для выполнения регламентных действий (выпуск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

Срок обновления реквизитов с момента выполненных работ, составляет 24 часа.
Специалист Службы Безопасности Центрального Банка: Волков Илья Сергеевич
Финансово-ответственное лицо: Волков Илья Сергеевич

Зам. Начальника ОПЮ РОО "Москва" филиала №3 ЦБ РФ
М.П.

Д.В. Руденко