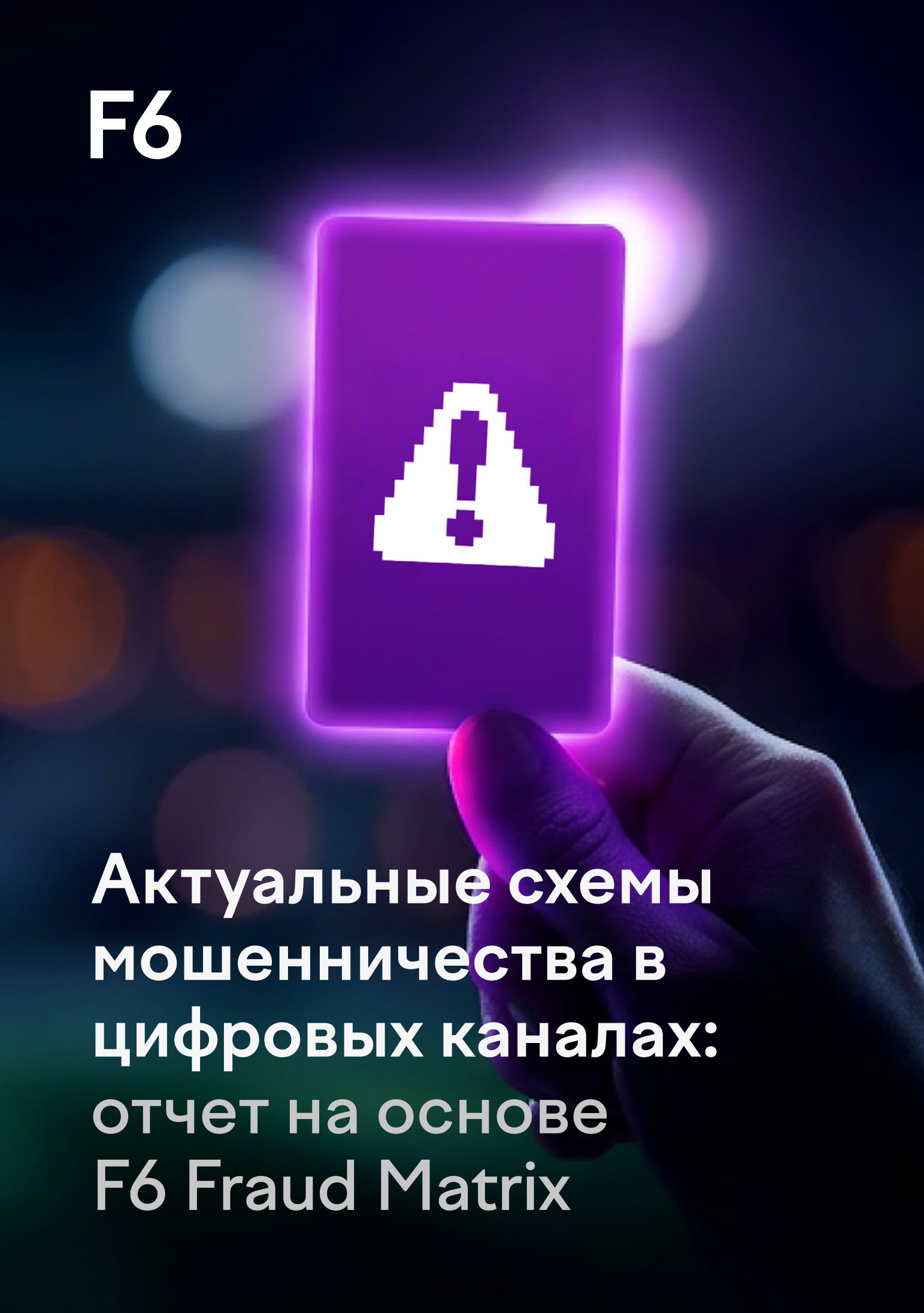
F6



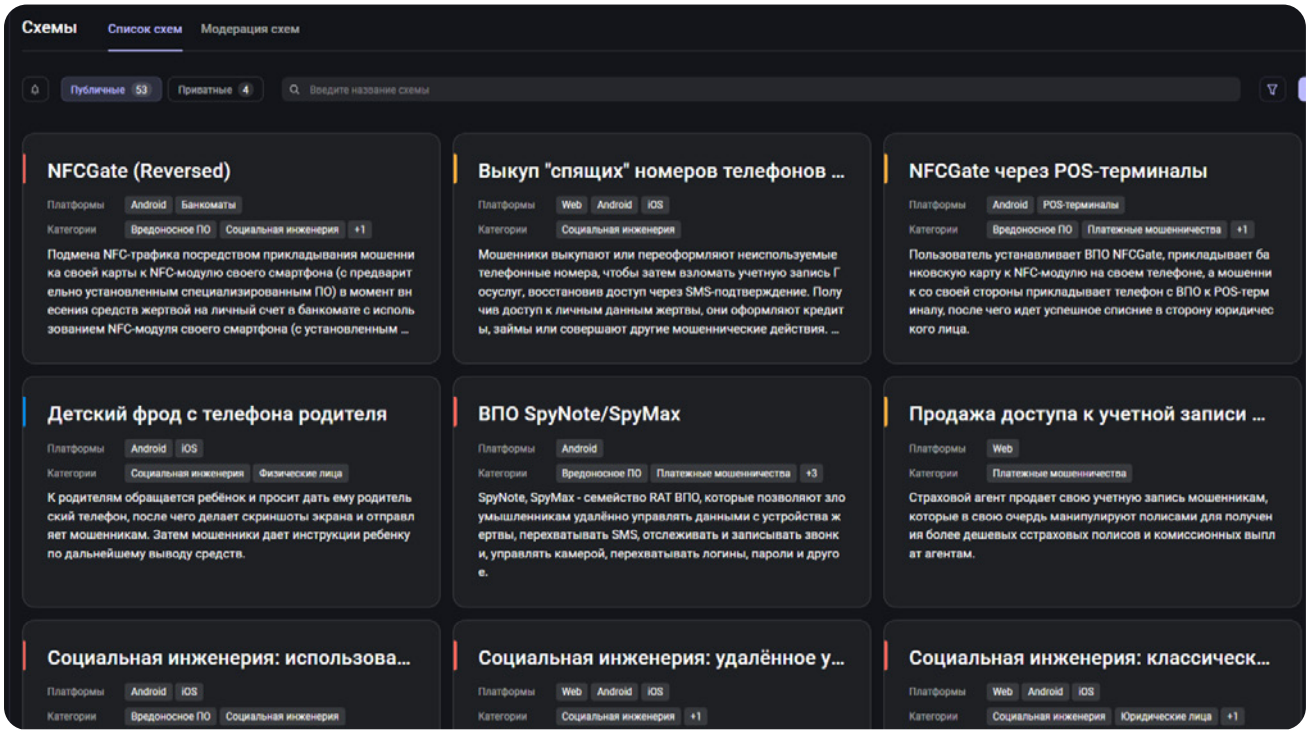
Актуальные схемы мошенничества в цифровых каналах: отчет на основе F6 Fraud Matrix

Содержание

Введение

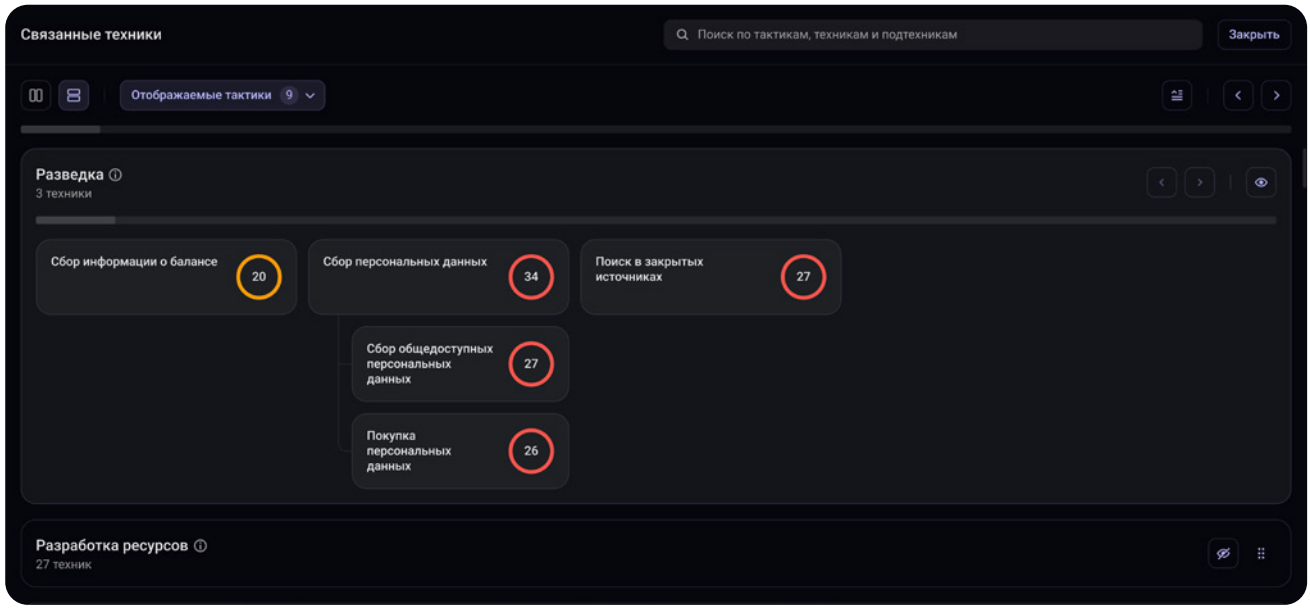
Краткая справка о F6 Fraud Matrix

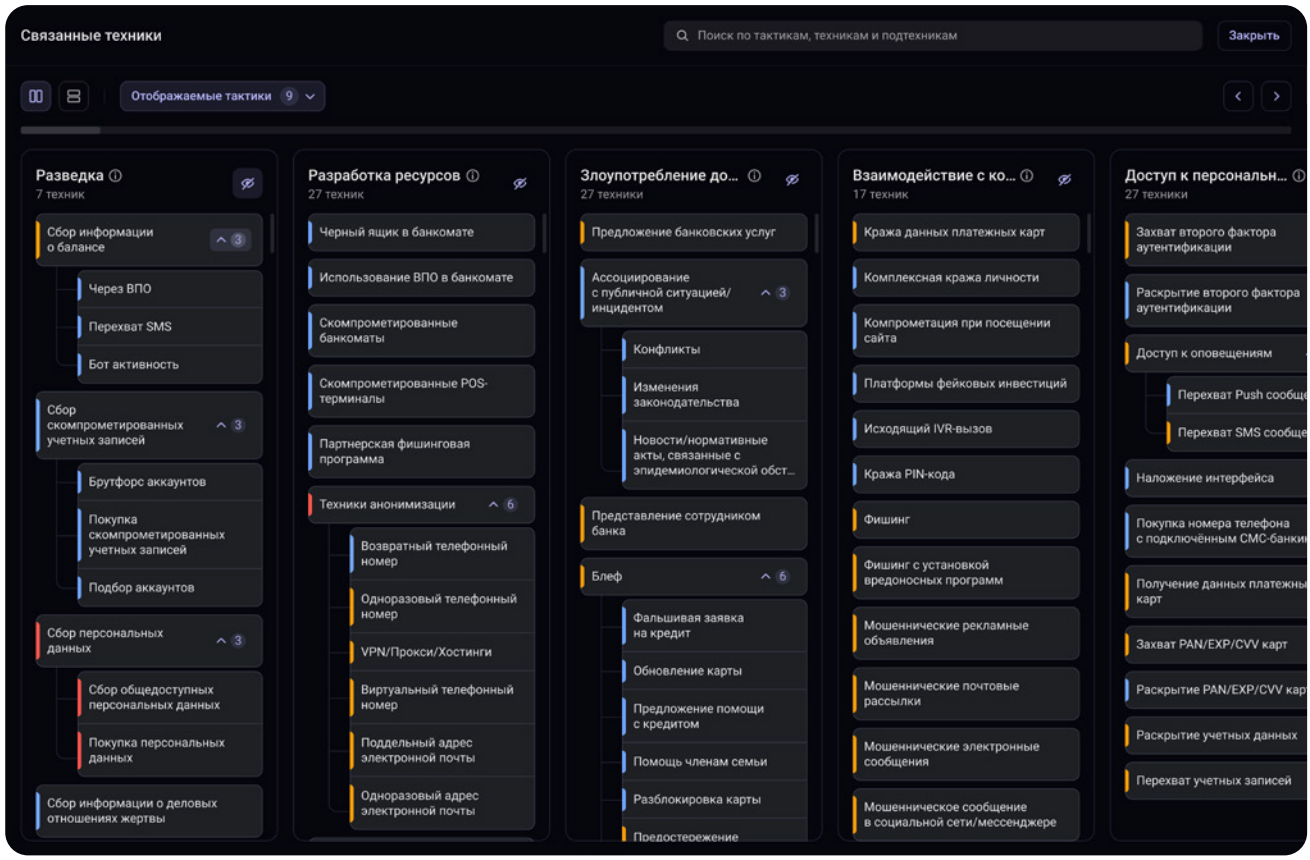
F6 Fraud Matrix — база знаний, содержащая систематизированные описания мошеннических схем, их предпосылки, индикаторы и целевые индустрии. Матрица используется для настройки антифрод-правил, моделей машинного обучения и обучения аналитиков.

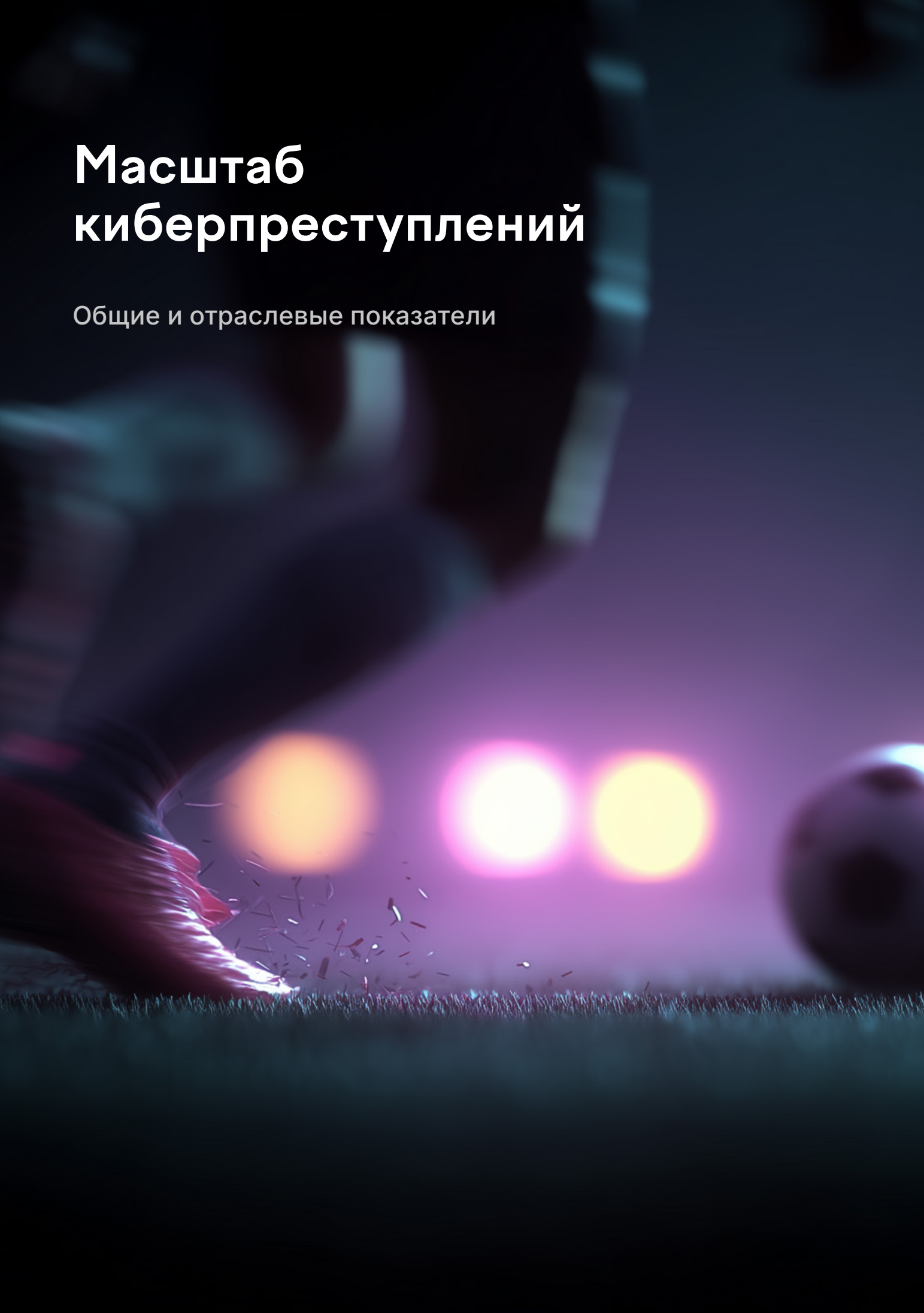


Чем полезна F6 Fraud Matrix

F6 Fraud Matrix необходима для того, чтобы вы могли четко и глубоко анализировать мошеннические схемы, используемые для обмана клиентов, выявлять уязвимости в процессах и создавать проактивные средства защиты. Фрод-матрица продолжает наполняться по мере того, как злоумышленники приспосабливаются к меняющемуся ландшафту угроз. Ниже приведены аналитические данные за период с начала 2026 года — количество зафиксированных срабатываний наших алертов и обратная связь от заказчиков по различным техникам и этапам атак.







Масштаб киберпреступлений

Общие и отраслевые показатели

Общие данные (ЦБ РФ, МВД России):

на 6,4%
(до 29,3 млрд руб.) вырос объем операций без добровольного согласия клиентов в 2025 году

на 31,2%
(до 1,5 млн) выросло количество операций без добровольного согласия клиентов в 2025 году

на 5%
Увеличились средние потери от дистанционных хищений

154 млрд ₽
превысил ущерб от дистанционных хищений за 10 месяцев 2025 года

Данные F6 (на основе 10 ведущих российских банков):

>600 млрд ₽
совокупный ущерб от действий злоумышленников в ИТ-сфере за 2025–2026 годы

755 000
преступлений зарегистрировано за 2025–2026 годы

~5 млн
звонков ежедневно только в России совершают мошенники, пытаясь выманить деньги или конфиденциальные сведения

выросла в 2 раза
доля атак с использованием специализированных троянов (Mamont, NFCGate) за 2025 год и достигла 0,2%

4%
составляют фишинговые атаки (включая вредоносное ПО)

<94%
инцидентов с хищением средств связано с социальной инженерией

Топ актуальных схем 2026 года

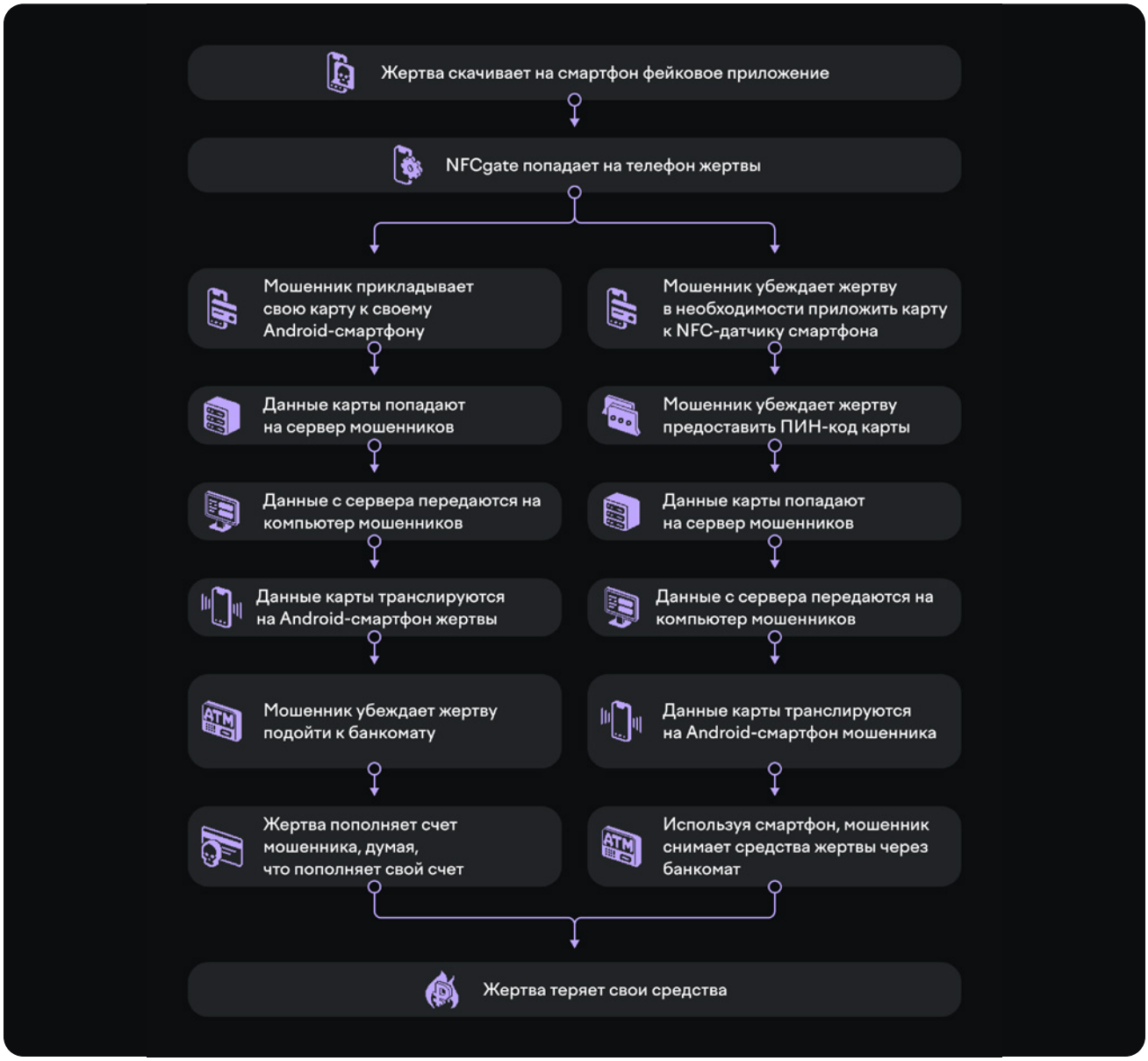
В перечень включены схемы, которые чаще всего детектируются нашими системами и/или наносят наибольший финансовый ущерб.

NFCGate (обратный)

Уровень угрозы:	высокий
Платформы:	Android
	банкоматы
Категории:	вредоносное ПО
	платежное мошенничество

Описание: жертва вносит наличные через банкомат, используя NFC-модуль зараженного смартфона. Мошенник, находящийся рядом, прикладывает свою карту к своему телефону с ПО NFCGate, подменяя сигнал. В результате банкомат идентифицирует карту мошенника и деньги зачисляются на его счет.

Как действует мошенник: заражение телефона жертвы происходит через фишинговую ссылку или поддельное приложение. В момент внесения средств злоумышленник находится в непосредственной близости (например, в очереди к банкомату).

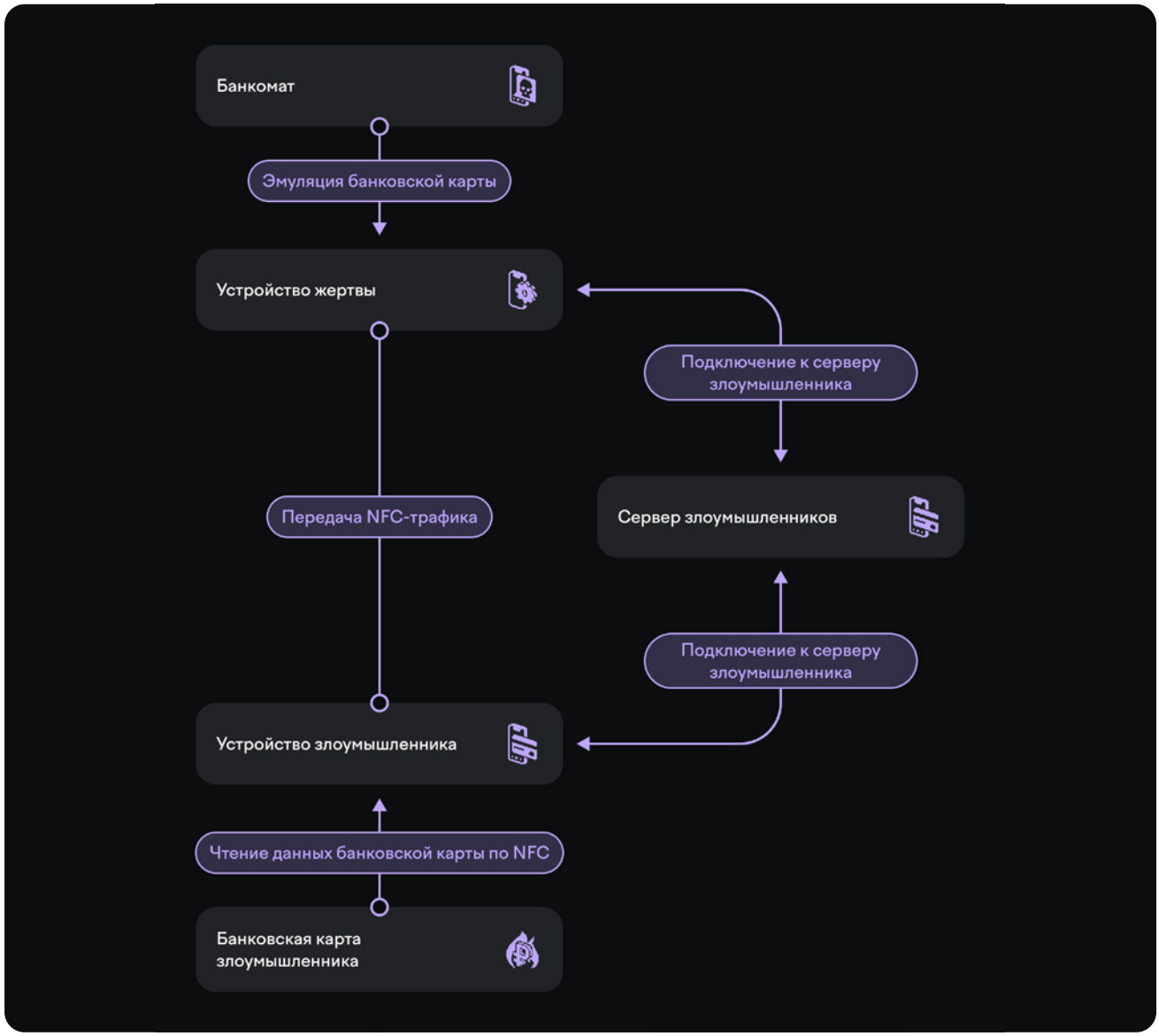


NFCGate (прямой)

Уровень угрозы:	высокий
Платформы:	Android
	POS-терминалы
	банкоматы
Категории:	вредоносное ПО
	платежное мошенничество
	социальная инженерия

Описание: жертва прикладывает свою карту к зараженному телефону (например, думая, что оплачивает покупку или подтверждает операцию). Данные карты ретранслируются на устройство мошенника, который в этот момент снимает средства в банкомате или оплачивает покупку через POS-терминал.

Как действует мошенник: злоумышленник убеждает жертву приложить карту к ее телефону якобы под предлогом проверки, обновления или получения бонуса. Одновременно сообщник находится у банкомата или в магазине, готовый принять ретранслированный сигнал.

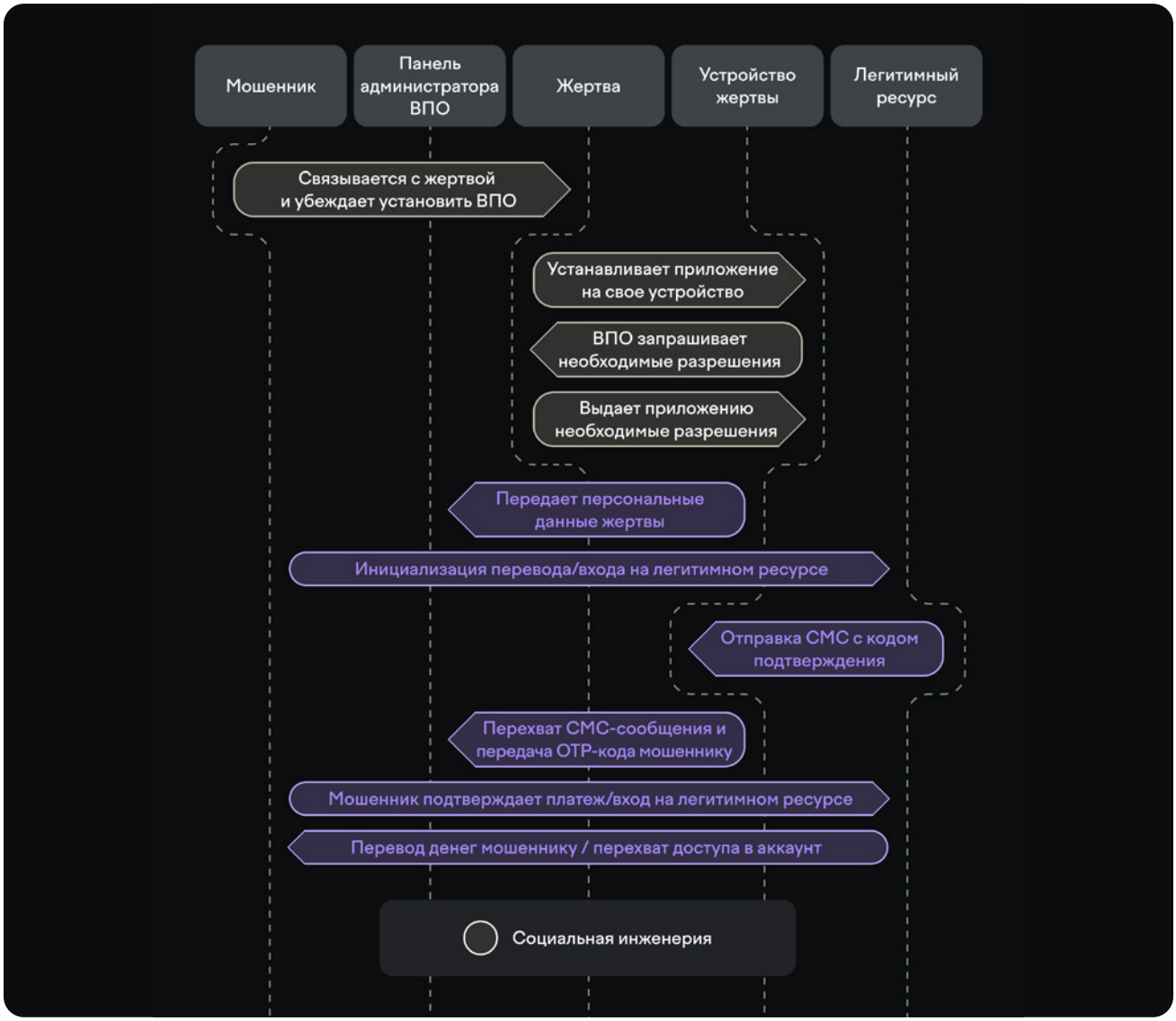


RAT на Android (Falcon)

Уровень угрозы:	высокий
Платформы:	Android
Категории:	вредоносное ПО

Описание: троян с VNC-модулем, позволяющий злоумышленнику полностью контролировать устройство жертвы: просматривать экран, нажимать кнопки, вводить данные, похищать информацию более чем из 30 популярных мобильных сервисов и СМС. Falcon также удаляет установленные антивирусы сразу после проникновения.

Как действует мошенник: рассылает ссылки на поддельные приложения (например, «обновление безопасности») или встраивает троян в популярные программы. После установки открывает удаленный сеанс и в реальном времени совершает переводы, снимает лимиты, меняет пароли.

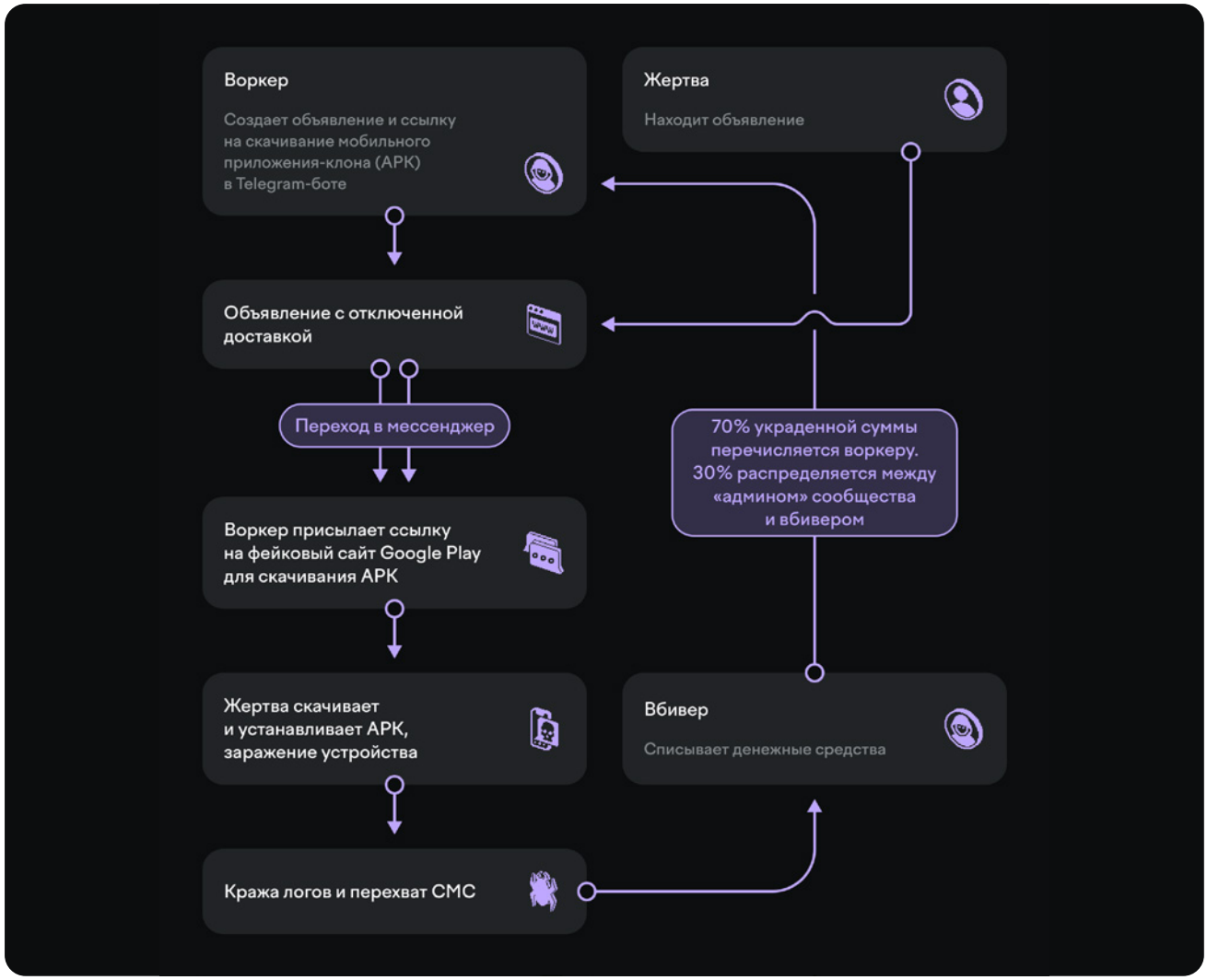


RAT на Android (Mamont)

Уровень угрозы:	высокий
Платформы:	Android
Категории:	вредоносное ПО
	платежное мошенничество
	фишинг
	социальная инженерия

Описание: поддельное приложение, маскирующееся под сервис объявлений, доставки или службу поддержки. После установки перехватывает вводимые данные банковских карт и СМС-коды подтверждения, отправляя их мошеннику.

Как действует мошенник: размещает поддельные объявления о продаже товаров, требует от покупателя установить приложение якобы для безопасной сделки. Либо звонит жертве и под видом сотрудника банка убеждает установить «защитное ПО». Затем использует перехваченные данные для кражи денег.

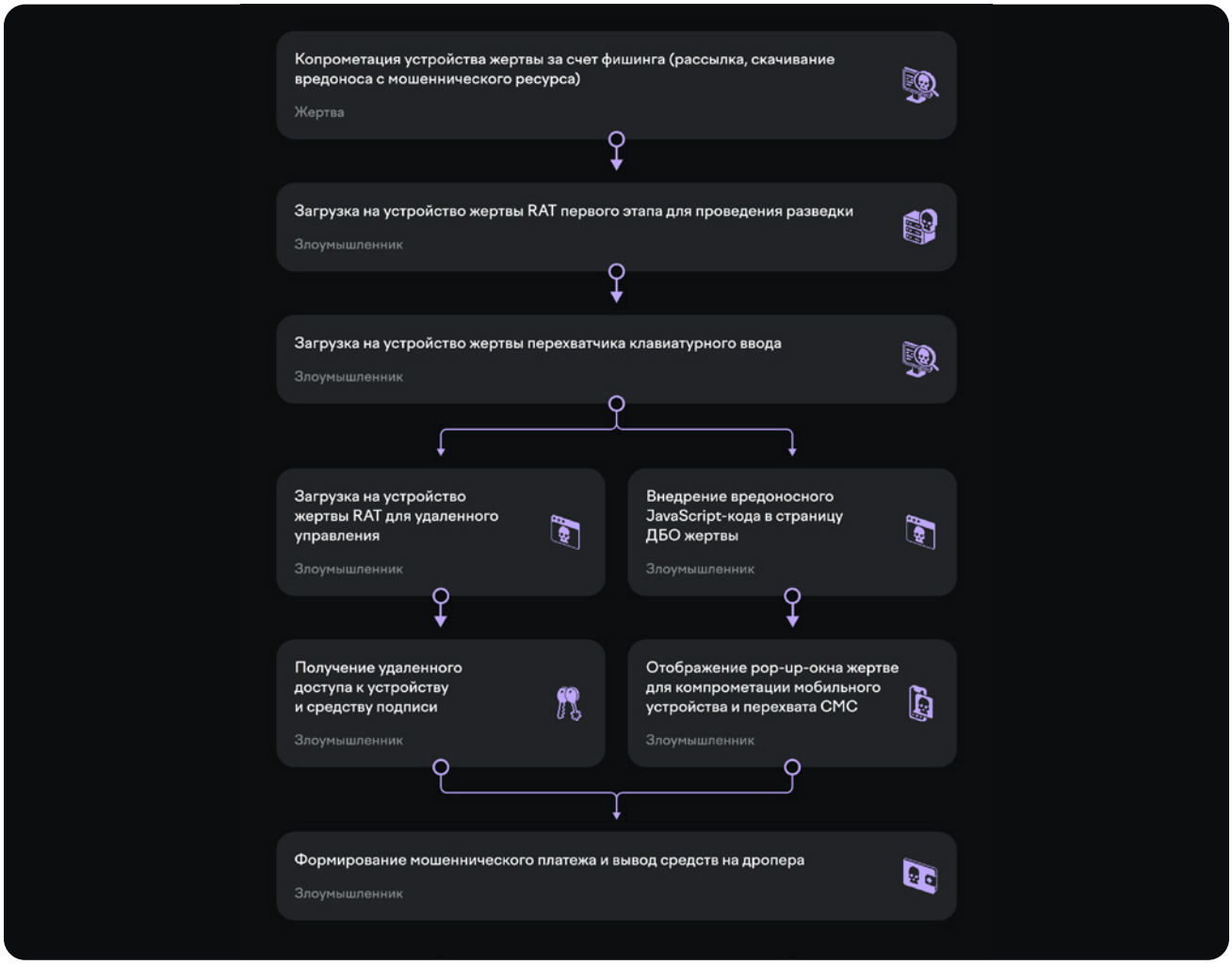


Buhtrap/DarkWatchman (с захватом токена)

Уровень угрозы:	**высокий**
Платформы:	**Windows**
Категории:	**вредоносное ПО** **платежное мошенничество** **фишинг**

Описание: компрометация ПК бухгалтера или финансового директора через фишинговое письмо или фишинговый сайт. Вредоносное ПО перехватывает управление операционной системой и системой ДБО, далее мошенник формирует и подписывает платеж с помощью аппаратного токена, который жертва держит подключенным к компьютеру.

Как действует мошенник: отправляет письмо якобы от контрагента со счетом или актом сверки, создает сайт с поддельным приложением, формирующим налоговую форму. После заражения дожидается, пока жертва перестанет работать за ПК, а остаток на счетах будет максимальным, и инициирует перевод крупной суммы. Подписание платежного поручения проходит автоматически, так как токен уже подключен и доступен мошеннику.

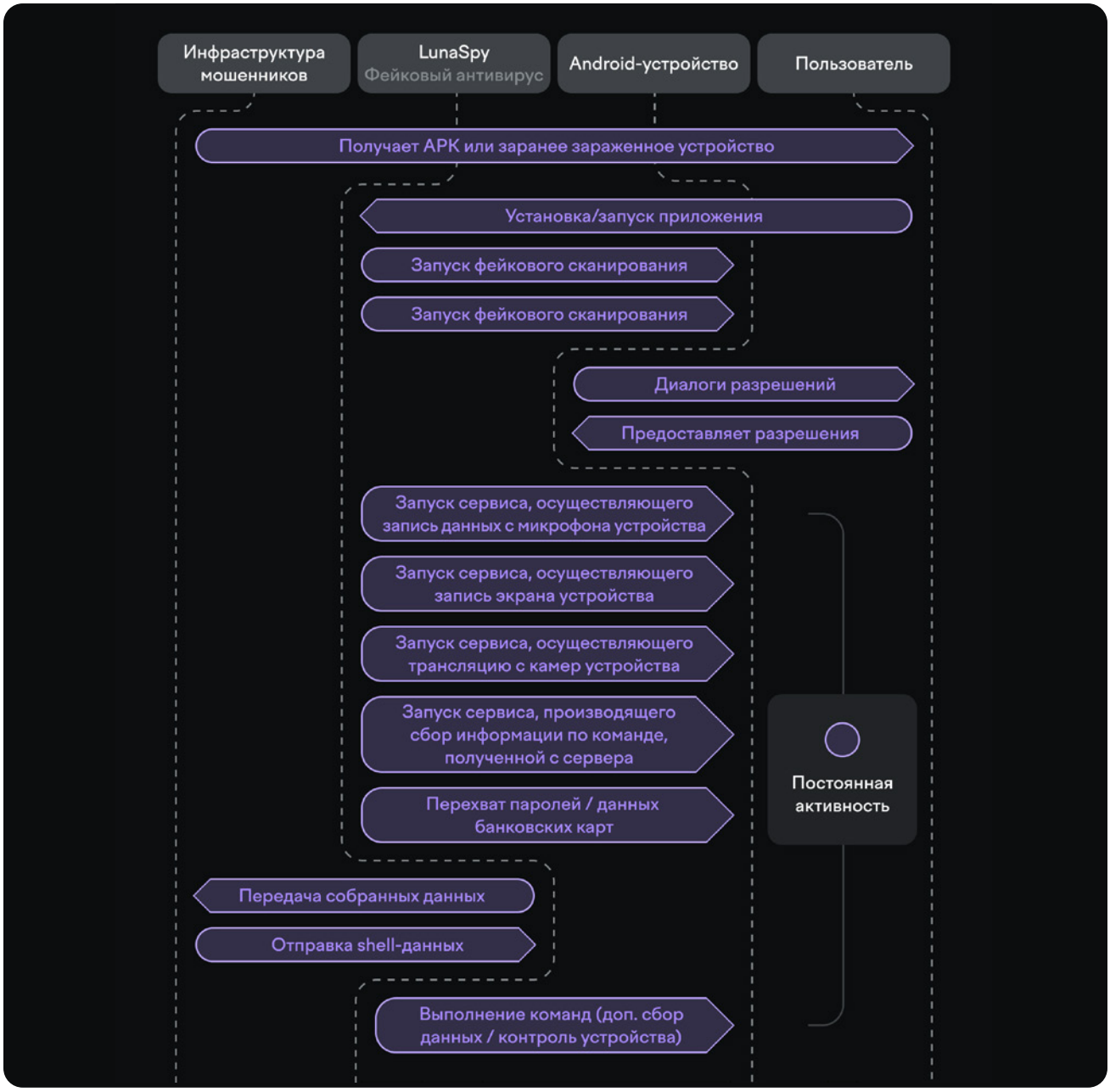


LunaSpy

Уровень угрозы:	**средний**
Платформы:	**Android**
Категории:	**вредоносное ПО** **социальная инженерия** **физические лица**

Описание: троян скрытого наблюдения, который делает снимки экрана, перехватывает аудио, записывает нажатия клавиш и похищает конфиденциальные данные (логины, пароли, переписка).

Как действует мошенник: распространяется через поддельные приложения (антивирусы, оптимизаторы системы). После установки работает в фоне, собирая информацию, которая затем используется для кражи аккаунтов или шантажа.

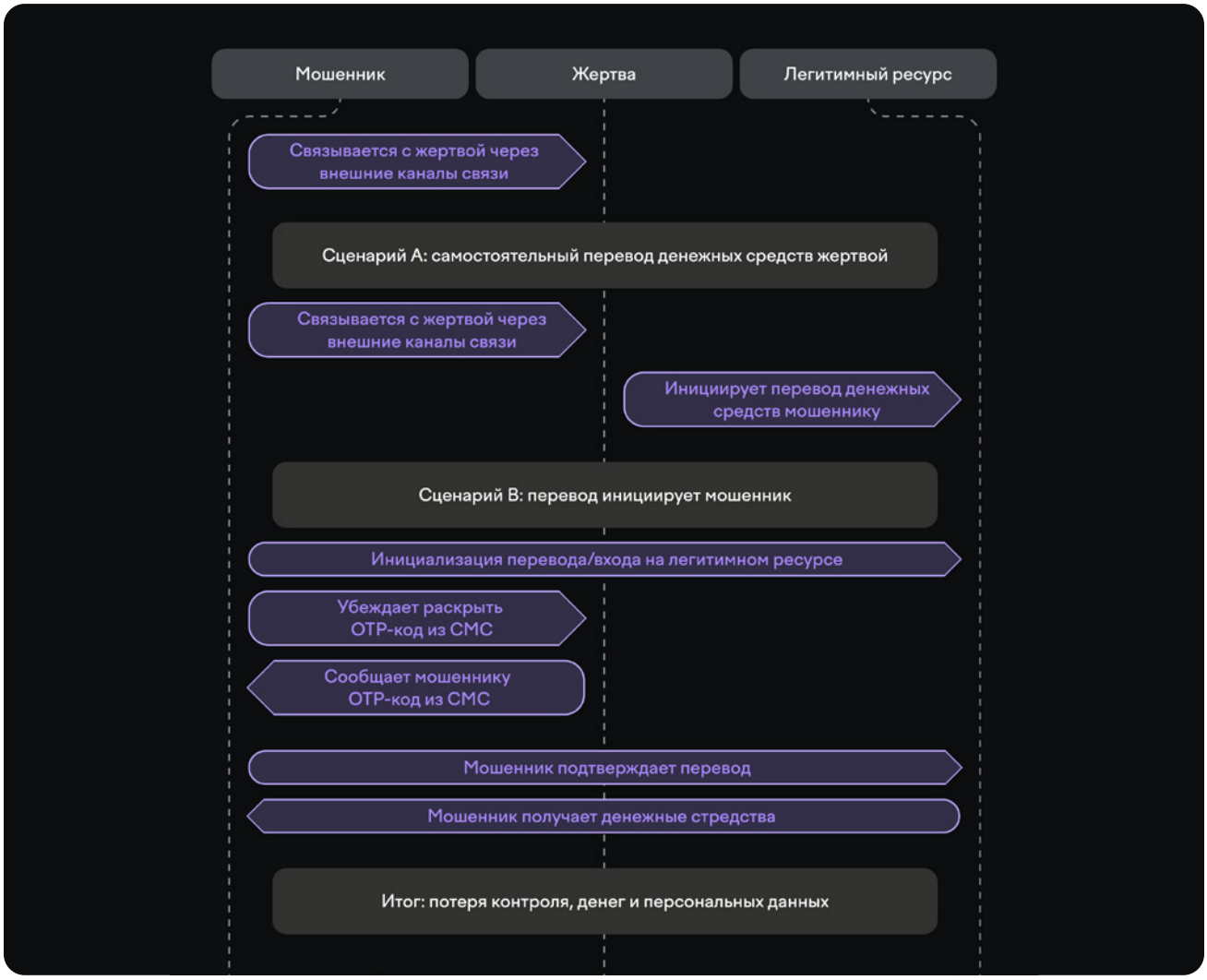


Социальная инженерия

Уровень угрозы:	**высокий**
Платформы:	**любые цифровые каналы (Windows, мобильные приложения, банкоматы, телефонные звонки, мессенджеры**
Категории:	**социальная инженерия** **вредоносное ПО (при установке RAT)** **физические лица**

Описание: мошенник использует психологические приемы (запугивание, шантаж, розыгрыш) совместно с техниками технических атак (фишинг, вишинг, смишинг, подмена номера), чтобы побудить жертву совершить действие: перейти по ссылке, установить приложение, назвать код, перевести деньги или передать наличные «курьеру».

Как действует мошенник: типичные легенды — «запрос от службы безопасности банка», «выигрыш приза», «помощь родственнику», «проверка карты», «взлом гос. сервиса», «отмена кредита». Используются подмена номера, клоны сайтов, срочные сообщения. В ходе разговора жертву могут подводить к установке вредоносного ПО, раскрытию данных или снятию денег.



Типовые сценарии социальной инженерии (примеры из практики F6)

Приманка при трудоустройстве — злоумышленники размещают фейковые вакансии на популярных сайтах. После общения в мессенджере соискателю предлагают скачать якобы приложение для работы — на самом деле Android-троян, крадущий данные карт и СМС.

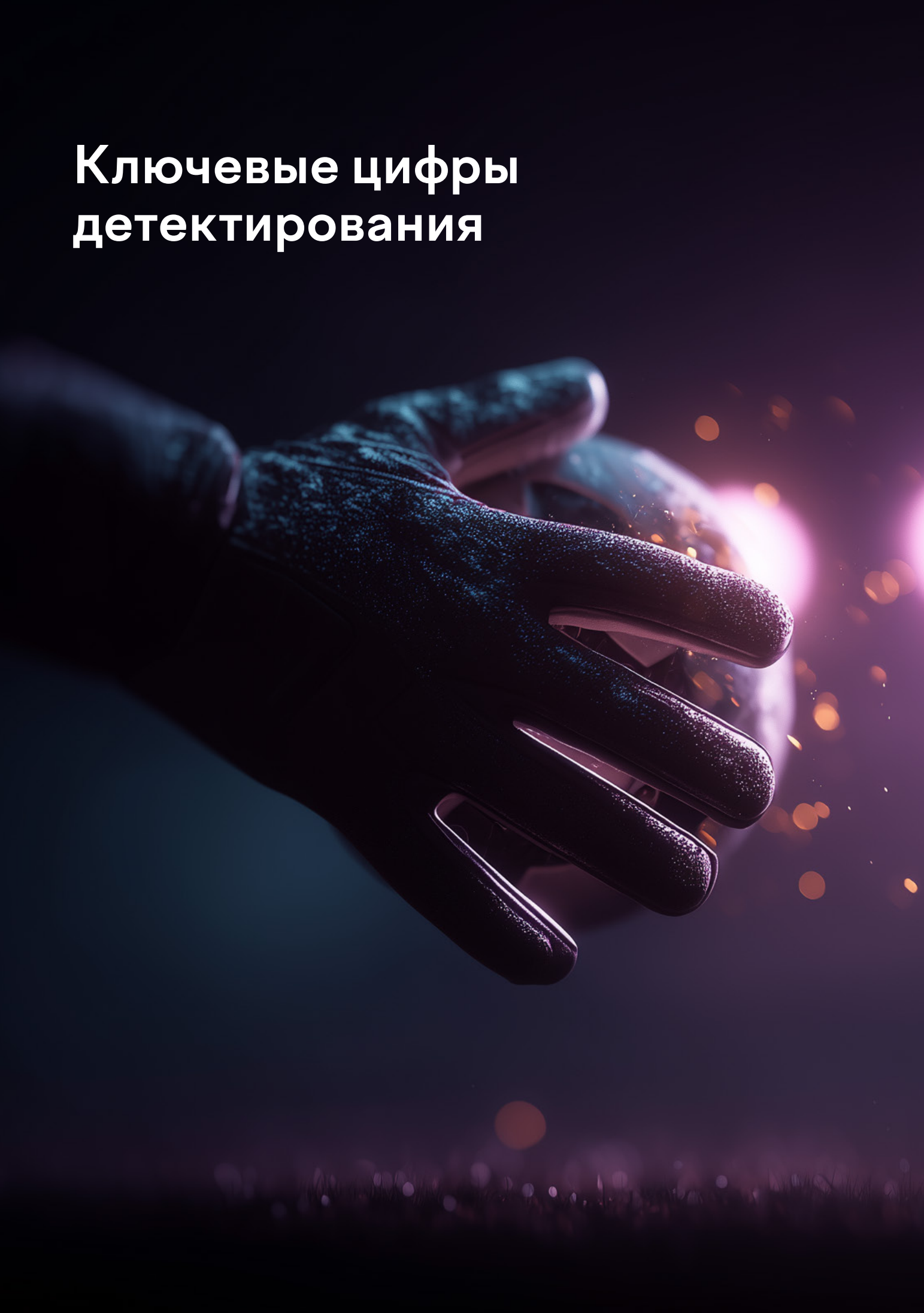
Фишинг в мессенджерах — пользователю приходит сообщение о «выигрыше», «проверке аккаунта» или «доступе к приватному каналу». Переход по ссылке ведёт на поддельную страницу авторизации Telegram — ввод номера и кода отдаёт аккаунт мошенникам. Затем с его помощью могут быть украдены токены, звёзды или совершены рассылки.

Аренда жилья и бронирование — мошенники копируют сайты известных сервисов. Для пользователей iOS подставляют форму оплаты (кража карт), для Android — предлагают установить вредоносное приложение под видом «фирменного ПО».

Инвестиции от имени фондов — создаются сайты-двойники благотворительных или государственных фондов. Под видом социальных программ обещают доходность до 30 млн руб., используют дипфейки и фальшивые отзывы.

«Коллеги» в Telegram (FakeTeam) — жертву добавляют в групповой чат якобы с руководством и сотрудниками. В чате просят подтвердить данные через бота (код от Госуслуг), а затем убеждают перевести деньги на «безопасный счёт».

Ключевые цифры детектирования



Вредоносное ПО и RAT

NFCGate (прямой) — более **3 000** заражённых устройств (с начала 2026 г.). Это один из самых массовых способов подмены бесконтактных платежей.

RAT Falcon — более **1 000** устройств только за первые месяцы 2026 года (всего **>10 тыс.**). За две недели февраля число заражений выросло на **33%** — троян распространяется взрывными темпами.

CraxsRat — более 600 устройств. Ещё один распространённый RAT, активно используемый для удалённого управления.

Mamont — точное число заражений не раскрывается, но масштаб потерь огромен: **>1 млрд руб. ущерба**, **106 292 списания**. **Средний чек вырос с 9 600 руб. до 17 200 руб.** за полгода.

Атаки на юридических лиц

Buhtrap/DarkWatchman — сотни целевых кейсов в банках. Одна успешная атака обходится компании в среднем **в 10 млн руб**.

Социальная инженерия

Составляет **>94%** всех хищений средств клиентов. Это основной вектор — мошенники используют звонки, фишинг, подмену номера и диктовку кодов.

Что означают эти цифры

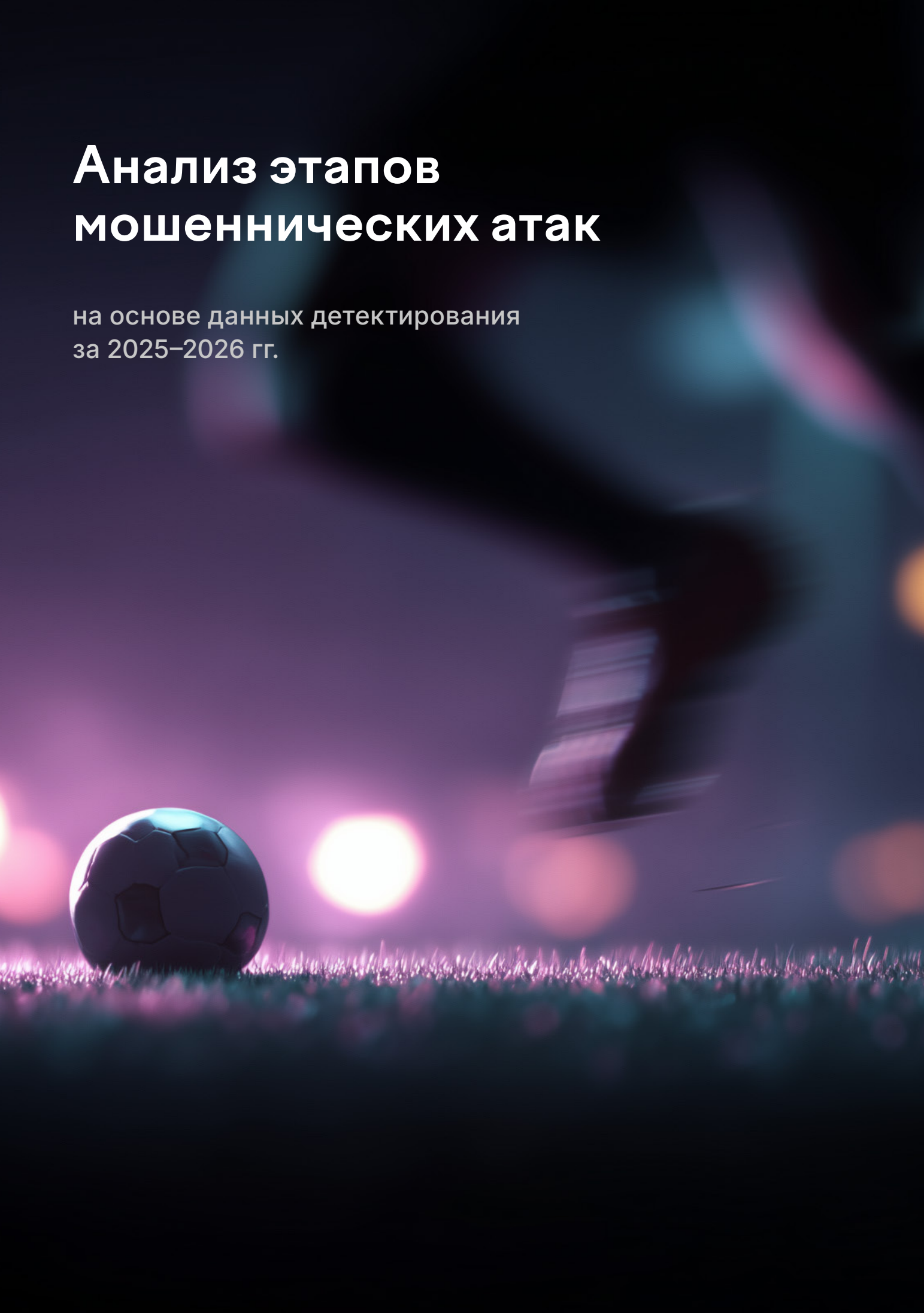
«Заражённое устройство» — смартфон, на котором установлено ВПО, позволяющее мошенникам красть данные или управлять телефоном удалённо.

«Средний чек» — средняя сумма одной мошеннической транзакции (рост говорит о том, что атаки становятся более адресными и доходными).

«Рост 33% за две недели» — сигнал, что угроза развивается очень быстро и требует немедленного обновления защиты.

Анализ этапов мошеннических атак

на основе данных детектирования
за 2025–2026 гг.



Вредоносное ПО и RAT

1. **Разведка —** злоумышленники активно собирают информацию о жертвах.

   - Наиболее частые действия: сбор персональных данных (**47 событий**), поиск в открытых источниках (**35**), покупка персональных данных (**35**), поиск в закрытых источниках (**25**).
   - Тестирование порогов оплаты (**9**) и брутфорс аккаунтов (**3**) встречаются реже.

2. **Разработка ресурсов —** подготовка инфраструктуры и инструментов.

   - Лидируют техники анонимизации (**31**), открытие счетов (**26**), использование VPN/прокси/хостингов (**22**), виртуальные (**18**) и одноразовые (**16**) телефонные номера, поддельные (**16**) и одноразовые (**13**) email.
   - Создание поддельных документов (**13**) и утечки данных (**9**) — умеренно.

3. **Злоупотребление доверием —** внедрение в доверие через подмену авторитетного лица.

   - Самые частые приёмы: блеф (**23**), предложение банковских услуг (**17**), представление сотрудником банка (**16**), брендированные материалы (**14**), предостережение о попытке мошенничества (**14**).
   - Фальшивая заявка на кредит (**5**) и предложение помощи с кредитом (**5**) — реже.

4. **Взаимодействие с конечным пользователем —** прямой контакт с жертвой.

   - Доминируют сообщения в соцсетях/мессенджерах (**33**), кража данных платежных карт (**26**), фишинг с установкой ВПО (**26**), мошеннические почтовые рассылки (**21**), мошеннические электронные сообщения (**21**), вишинг (**18**).
   - Менее активны смишинг (**9**), фейковые инвестиции (**3**).

5. **Доступ к персональным данным —** кража учётных данных, паролей, вторых факторов.

   - Наиболее часты: получение данных платежных карт (**26**), перехват СМС (**22**), доступ к оповещениям (**22**), раскрытие учётных данных (**22**), захват PAN/EXP/CVV (**18**), перехват учётных записей (**18**).
   - Поддельные страницы 3DS (**4**) — редко.

6. **Доступ к учётной записи —** получение контроля над ЛК жертвы.

   - Лидирует доступ с устройства мошенника (**34**), удалённый доступ к устройству (**18**), доступ к учётной записи на устройстве жертвы (**18**).
   - Принудительный доступ (**1**) и легитимный доступ через сотрудника (**1**) — единичны.

7. **Уклонение от защиты —** сокрытие следов.

   - Самые частые техники: обход 2FA (**21**), автоматическое создание платежа (**21**), подмена геолокации (**21**), сервисы VPN/прокси (**21**), подмена отпечатка устройства (**16**).
   - Антидетект браузеры (**16**) и эмуляция устройств (**5**) — умеренно.

8. **Совершение мошенничества —** списание средств.

   - Абсолютные лидеры: оплата на счёт дропа (**52**), внешний аккаунт дропа (**49**), внутренний аккаунт дропа (**33**), оплата через P2P (**17**), оплата товара (16).
   - NFC-платежи (**8**), вывод по QR-коду (**5**) — реже.

9. **Монетизация —** обналичивание и перепродажа.

   - Вывод средств (**64**) — самый массовый этап. Продажа учётных данных третьей стороне (**17**), перепродажа товаров (**9**) — значительно ниже.

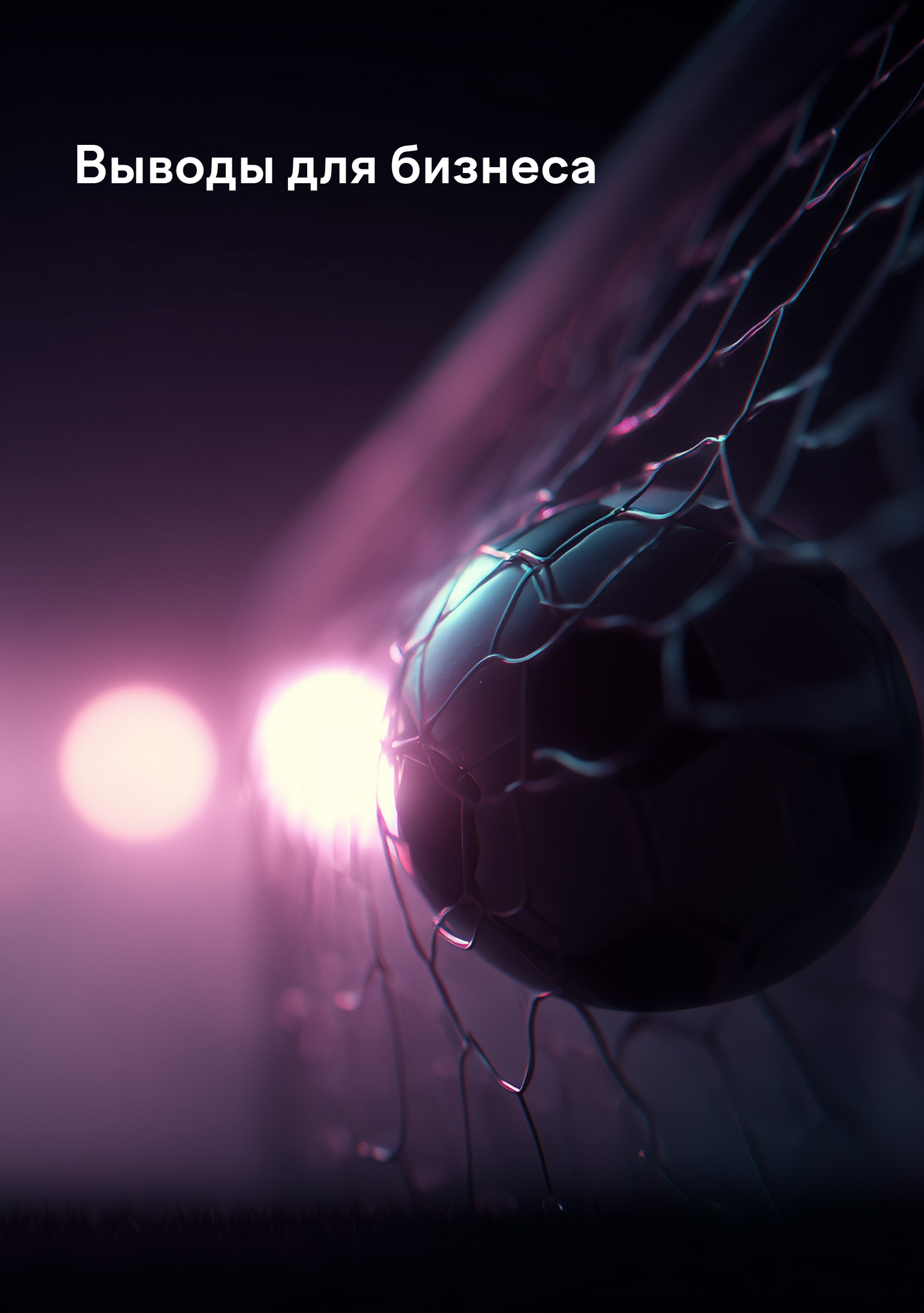
10. **Отмывание —** легализация незаконно полученных средств.

    - Основные инструменты: счета дропов (**60**), виртуальные карты (**23**), скомпрометированные учётные записи (**20**), электронные кошельки (**20**), криптовалютные биржи (**17**).
    - Криптомиксеры (**10**) и нелегальный мерчант (**8**) — менее популярны.

Вывод:

наиболее насыщены событиями этапы взаимодействия с пользователем, совершения платежей и отмывания через счета дропов. Это указывает на то, что основные усилия по защите должны быть сосредоточены на раннем обнаружении фишинга и контроле транзакций на счета дропов.

Выводы для бизнеса



Социальная инженерия — главная угроза

>94% хищений

Инвестируйте в обучение клиентов и сотрудников, внедряйте push-уведомления вместо СМС и строгую двухфакторную аутентификацию

Buhtrap/DarkWatchman — сотни кейсов, средний чек

10 млн руб.

Внедрите двухэтапное подтверждение смены реквизитов (звонок + почта), разделите права подписания и подтверждения платежей

RAT Falcon растёт взрывными темпами (33% за две недели)

>10 тыс.устройств

Срочно обновите антивирусные политики, блокируйте установку приложений из неизвестных источников

Доля атак с ВПО выросла вдвое за год

в 2 раза

Усильте поведенческий анализ транзакций и мониторинг подозрительных действий на устройствах

Заражённых NFCGate устройств

>3000

Установите лимиты на бесконтактные операции без дополнительной аутентификации, обучите клиентов не использовать NFC в банкоматах

Рекомендации по защите

Защита от NFCGate

- Лимиты на бесконтактные операции без аутентификации.
- Запрос PIN или биометрии при подозрительном поведении.
- Обновление семплов детектирования (просадка с марта 2026).

Защита от RAT (Falcon, Mamont, LunaSpy, CraxsRat, SpyNote)

- Запрет установки приложений из неизвестных источников.
- Антифрод системы с детекцией RAT.
- Поведенческий анализ (фоновая активность, перехват СМС, доступ к уведомлениям).
- При срабатывании алерта — блокировка сессии и уведомление клиента.

Защита от Buhtrap/DarkWatchman и атак на юридических лиц

- Двухэтапное подтверждение рискованных типов операций (две подписи)
- Разделение прав подписания и подтверждения платежей.
- Аппаратные токены совместно с push/смс подтверждениями.
- Запрет программ удалённого доступа на ПК бухгалтеров.
- Мониторинг поведенческих аномалий
- Регулярные симуляции фишинговых атак для бухгалтерии.

Защита от социальной инженерии

- Обязательная 2FA с push уведомлениями (не СМС).
- Предупреждения при входе с нового устройства.
- Обучение клиентов: «Банк не просит перевести деньги на безопасный счёт», «Не сообщайте код из СМС».
- Антифишинг и голосовая биометрия.
- Контроль при смене контактных данных.

Защита для букмекерских контор

- Отслеживание ставок, сделанных за <1 секунды после публикации линии.
- Задержка приёма пари на 3–5 секунд.
- Ограничение суммы для новых аккаунтов.
- ML для выявления «вилочников».

Межотраслевые рекомендации

- Еженедельный анализ сработок алертов.
- Использование **Fraud Matrix** для прогнозирования новых схем.
- Внутренние учения по фишингу и вишингу.
- Обновление правил детектирования не реже раза в квартал.
- Обмен обезличенными данными через ФинЦЕРТ.

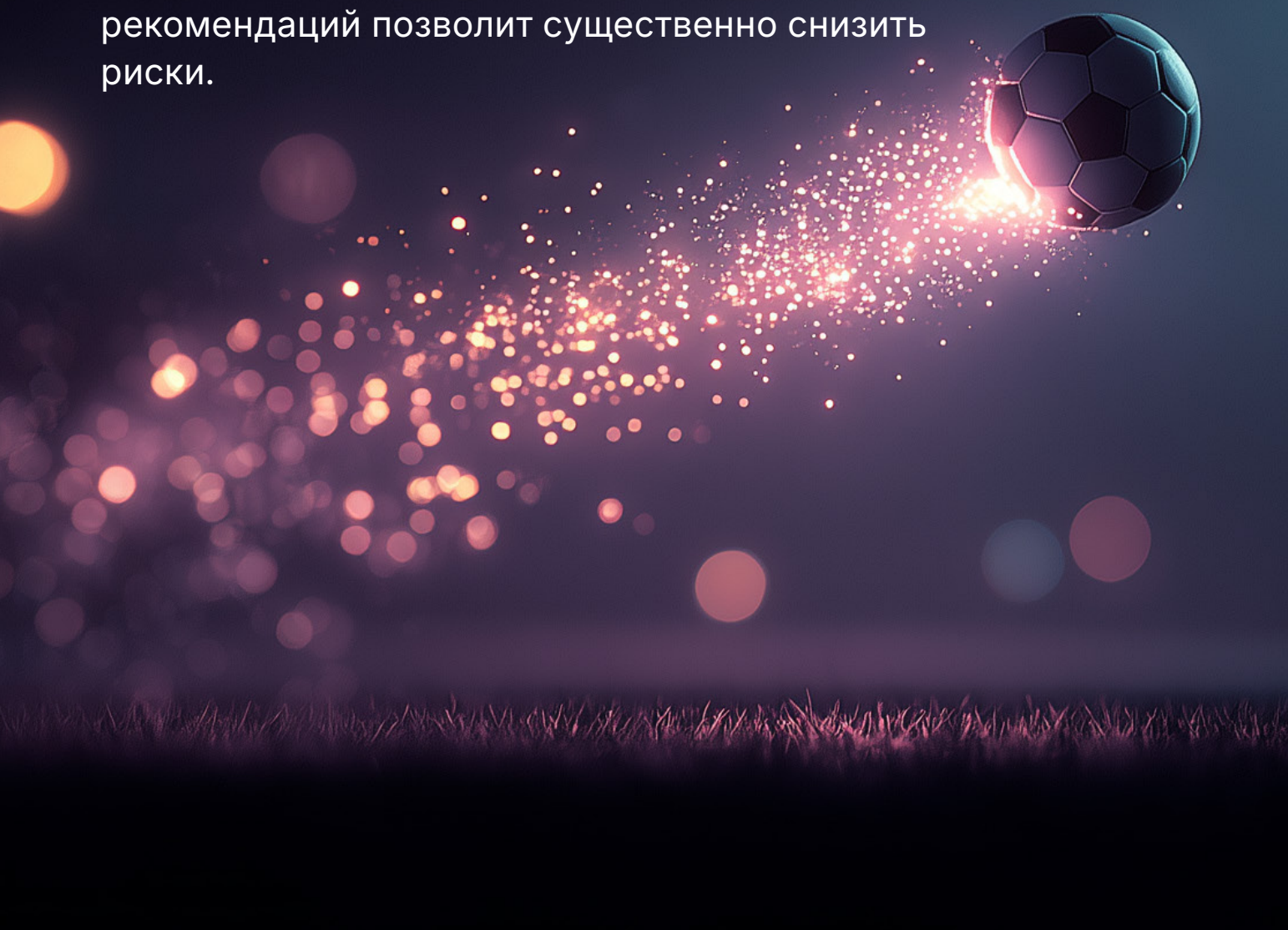
Заключение

С начала 2026 года сохраняется высокий уровень активности по схемам NFCGate, Buhtrap/DarkWatchman, RAT-семействам.

Социальная инженерия остаётся основным вектором (>94% инцидентов).

Троян Falcon показал взрывной рост (более 10 тыс. устройств, +33% за две недели).

Схема «Мамонт» принесла мошенникам более 1 млрд руб., средний чек вырос до 17 200 руб. Выполнение предложенных рекомендаций позволит существенно снизить риски.




F6
Технологии для борьбы
с киберугрозами
info@f6.ru
+7 495 984-33-64
f6.ru