Полномочный представитель Президента России
в Центральном федеральном округе

ДИАЛОГ

Центр
Управления
Регионом
Тамбовская область

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГИГИЕНА:

## Как не стать жертвой мошенников в 2025 году

Тамбовская область

# ТЕКУЩАЯ СИТУАЦИЯ

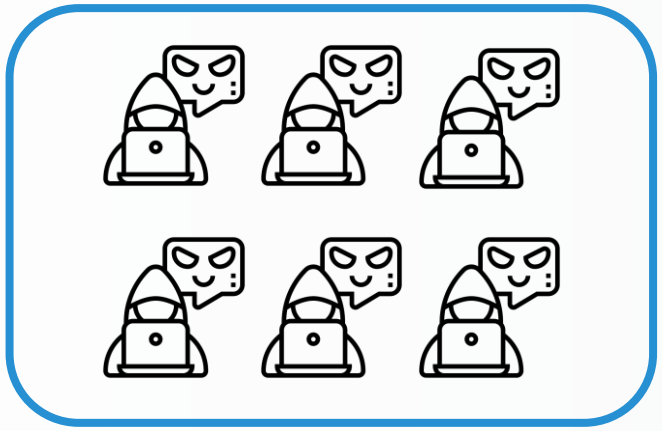
За прошлый год в Тамбовской области отмечен значительный рост случаев кибермошенничества: рост составил более 15%

**Каждое второе преступление, совершаемое в Тамбовской области — это преступление в сфере IT-технологий.**

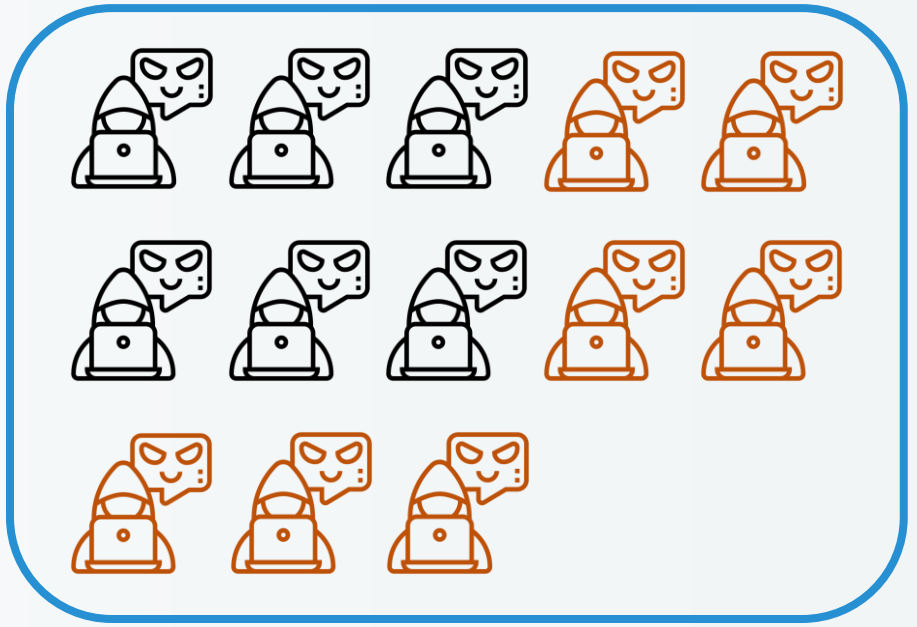
**В основном эти преступления связаны с кражами с банковских карт, мошенничеством, вымогательством**

# ТЕКУЩАЯ СИТУАЦИЯ

## 2023



## 2024



За минувший год значительно выросло количество преступлений, совершённых в сфере компьютерной информации—на **237%.**

# ТЕКУЩАЯ СИТУАЦИЯ (ПРИМЕР)

ТОП 68

## Мошенники погубили жизнь инженера завода «Комсомолец» Дмитрия Полковникова

Гендиректор предприятия рассказал, как негодяи лишили жизни честного человека.

# АКТУАЛЬНОСТЬ

## Ежедневные действия в интернете

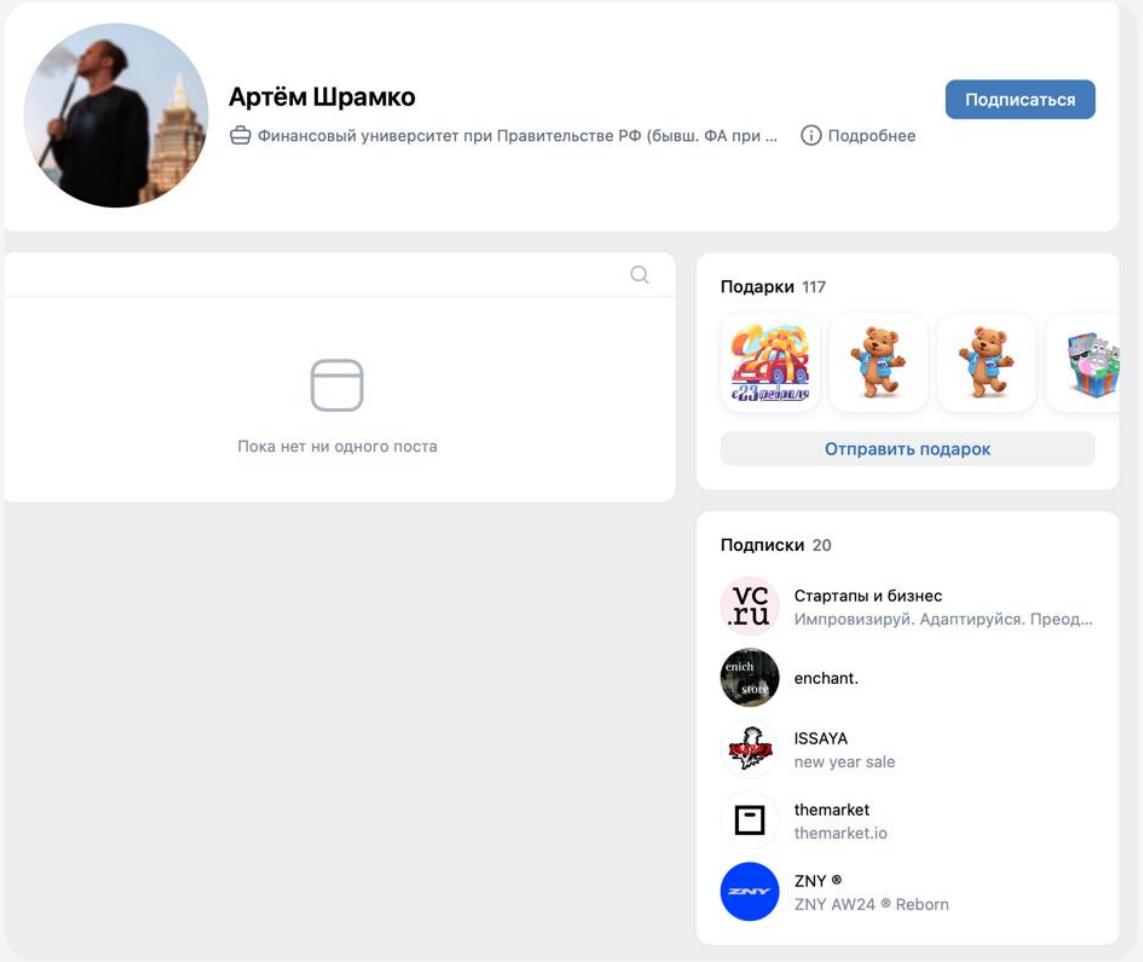
- **Регистрируемся в социальных сетях**
- **Делаем покупки на маркетплейсах**
- **Смотрим видео, слушаем музыку**
- **Пользуемся поисковиками**

***«Цифровой след» из персональных данных***

↓

**Желание его обезопасить**

# ЧТО МОЖЕТ СКАЗАТЬ ПРОФИЛЬ В СОЦИАЛЬНОЙ СЕТИ




## Страница открытая:

- ФИ + дата рождения
- Интересы

## Страница закрытая:

- Местоположение
- Устройство
- Просмотренный контент
- Контакты

Социальная сеть  Партнеры → цифровая «витрина» данных

# ПОЧЕМУ ЭТИ ДАННЫЕ ВАЖНЫ И КАК ОНИ ПРИМЕНЯЮТСЯ


Президентская кампания Дональда Трампа использовала открытые данные для создания психографических профилей граждан.

Она определяла черты личности пользователей на основе их активности в социальных сетях.

Далее эту информацию они использовали в качестве метода микротаргетинга.
И отображали индивидуальные сообщения о Трампе различным американским избирателям на различных цифровых платформах.

# ЧТО НА САМОМ ДЕЛЕ ИБ?


Информационная безопасность—

практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Информационная безопасность—

правильная защита «цифровых следов».

Злоумышленник может украсть вашу жизнь!

# УРОВНИ УГРОЗ В ИНТЕРНЕТЕ

## I уровень

мошенник получает общедоступные данные (низкая угроза)

Данные: ФИО, электронная почта

Виды мошенничества: телефонные звонки, фишинг, социальная инженерия

## II уровень

мошенник получает критически важные данные (средняя угроза)

Данные: дата рождения, паспорт, прописка

Виды мошенничества: сталкеринг, регистрация фиктивных компаний

## III уровень

мошенник получает доступ к финансовым данным (высокая угроза)

Данные: банковская карта, доступ к ЛК в банках

Виды мошенничества: кража денег, оформление кредитов

## IV уровень

мошенник получает полный контроль над личностью

Данные: биометрия, секретные ключи и кодовые слова, логины и пароли

Виды мошенничества: оформление документов, использование личность в преступных схемах

# ТИПЫ УГРОЗ ИБ

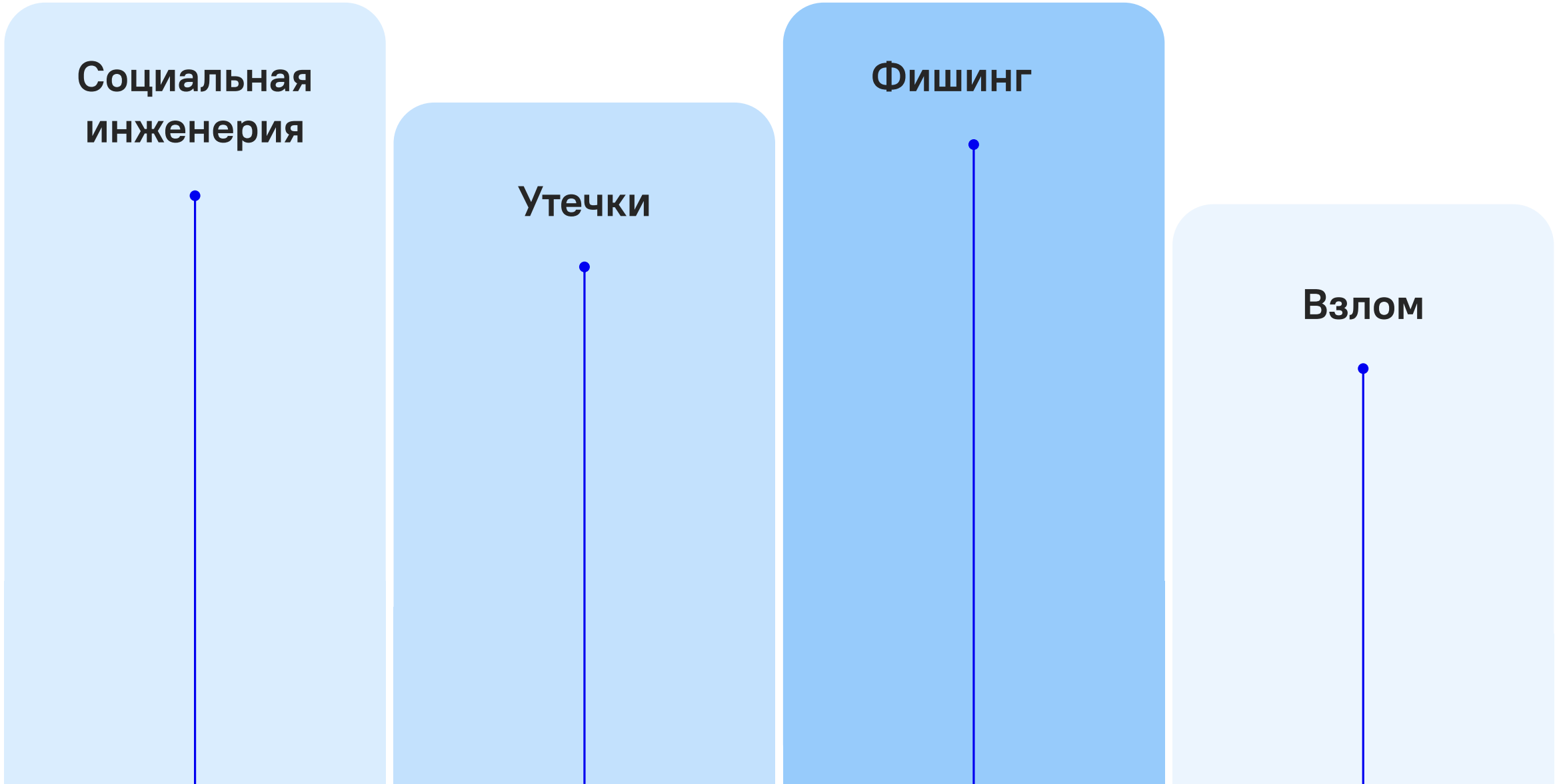
## Внутренние

Инсайдеры, ошибки персонала, технические сбои

## Внешние

Хакерские атаки, социальная инженерия, вредоносное ПО

# ОСНОВНЫЕ ВИДЫ УГРОЗ



# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

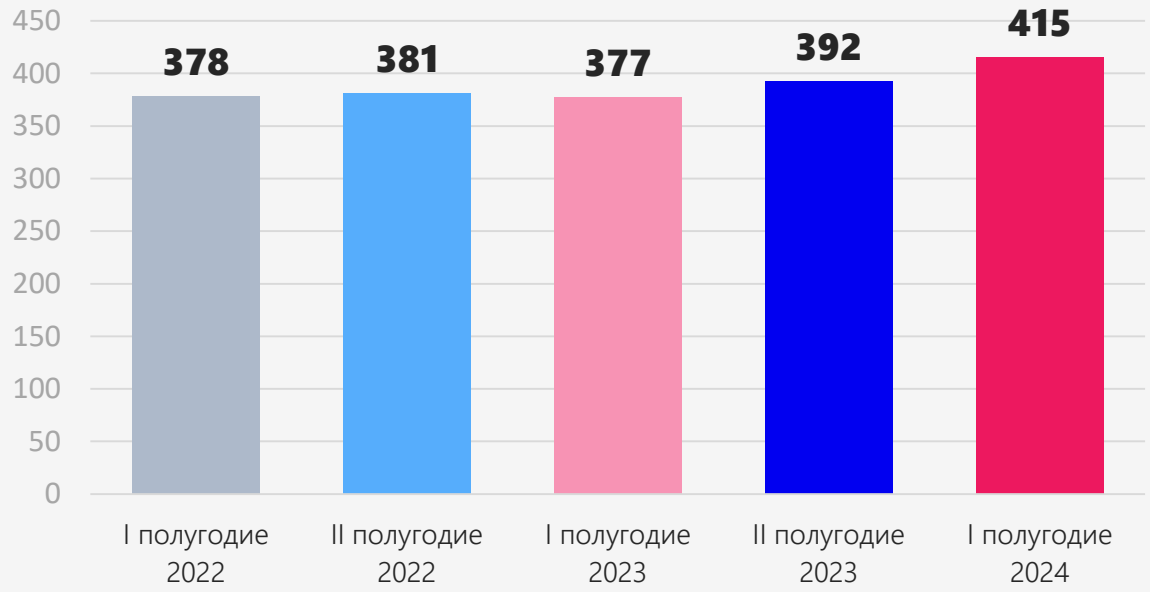
Набор методов и практик, которые заставляют человека выполнить какие-либо действия — необязательно в его интересах

Термин без негативного оттенка. Может и не быть манипуляцией человеком, хотя чаще всего так и есть

# УТЕЧКИ

- ФИО
- Телефоны
- Адреса
- Почта
- Паспорт (редко)
- Платежные данные (редко)

Россия



# КРУПНЕЙШИЕ УТЕЧКИ ДАННЫХ В РОССИИ

| Организация | Утечка | Содержание |
|---|---|---|
| СДЭК | 822 млн записей | ФИО, телефоны, адреса |
| Яндекс.Еда | 50 млн | ФИО, телефоны, адреса |
| СберСпасибо | 52 млн записей | ФИО, телефоны, платежные данные |
| Спортмастер | 46 млн записей | ФИО, телефоны, почта, дата рождения |

# УТЕЧКИ ДАННЫХ В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ РОССИИ

| Организация | Утечка | Содержание |
| --- | --- | --- |
| Силовые ведомства (МВД) | 20 тысяч записей | ФИО, телефоны, адреса |
| Межведомственный оборот | 500 тысяч записей | ФИО, телефоны, контакты |
| Региональные МФЦ | 300 тысяч записей | ФИО, телефоны, почта, дата рождения |

# КАК ИСПОЛЬЗУЮТ УТЕЧКИ?

- Интернет-расследования
- Выслеживание человека через социальные сети и в реальном мире. Угрозы и запугивания.
- Взлом цифровых ресурсов
- Клонирование цифровой личности. Репутационные риски.
- Финансовое мошенничество

# ПРИЧИНЫ УТЕЧЕК

## Не зависят от нас

Инсайдер, кража информации, взлом

## Зависят от нас

Отсутствие цифровой гигиены

# ФИШИНГ

**Фишинг—**

основной вид интернет-мошенничества
и основной способ для злоумышленников
проникнуть в локальные сети компании

Используется для кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации

# АТАКИ ПО КОЛИЧЕСТВУ ЖЕРТВ

## Массовые—

злоумышленники берут за основу несколько самых популярных интернет-сервисов, формируют легенду и рассылают тысячи писем через различные адреса

**Добрый день!**

Вчера мы пытались до вас дозвониться: Писали на почту и звонили на телефон.

Вы зарегистрировались у нас на сайте и получили подарок.

**Новый iPhone 16 Pro** практически ваш!

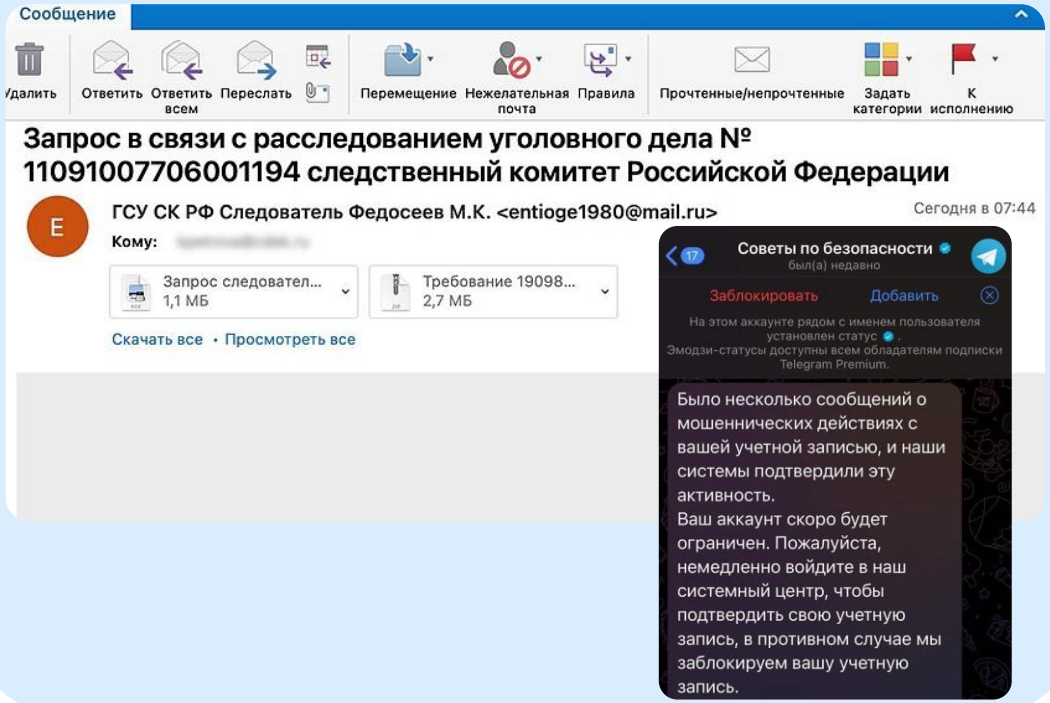
У вас остался последний день, для того чтобы воспользоваться всеми привилегиями

**Перейти на сайт и попробовать**

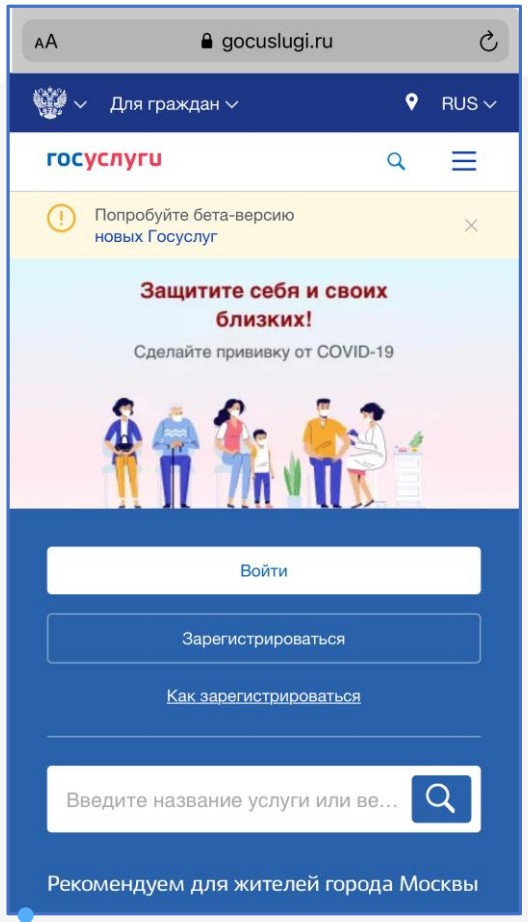
Поддержка **WILDBERRIES**

## Таргетированные—

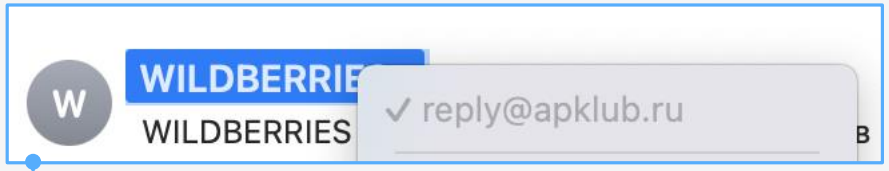
персонифицированные и целенаправленные атаки. Сбор и систематизация данных на жертву



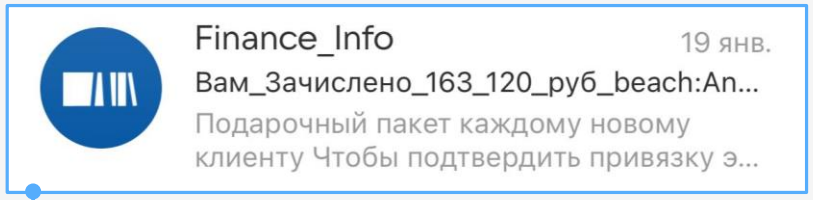
# ПРИЕМЫ ЗЛОУМЫШЛЕННИКОВ



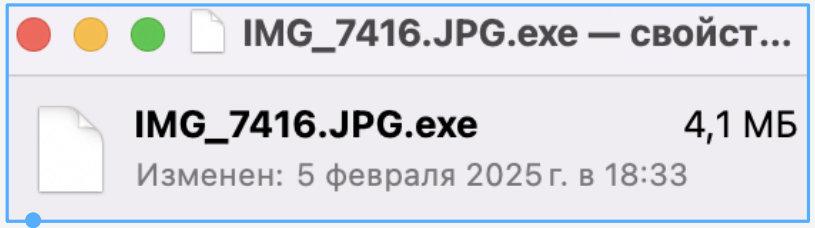

манипуляции со ссылками



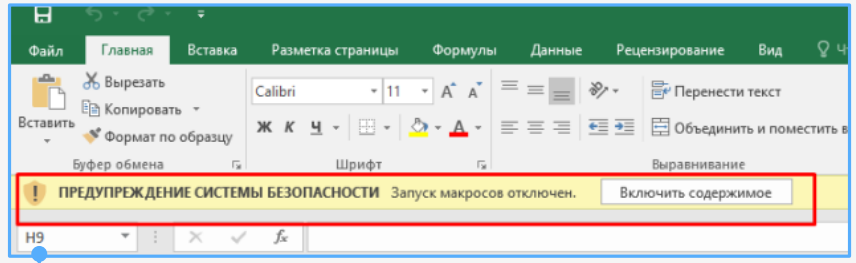

подмена отправителя (спуфинг)



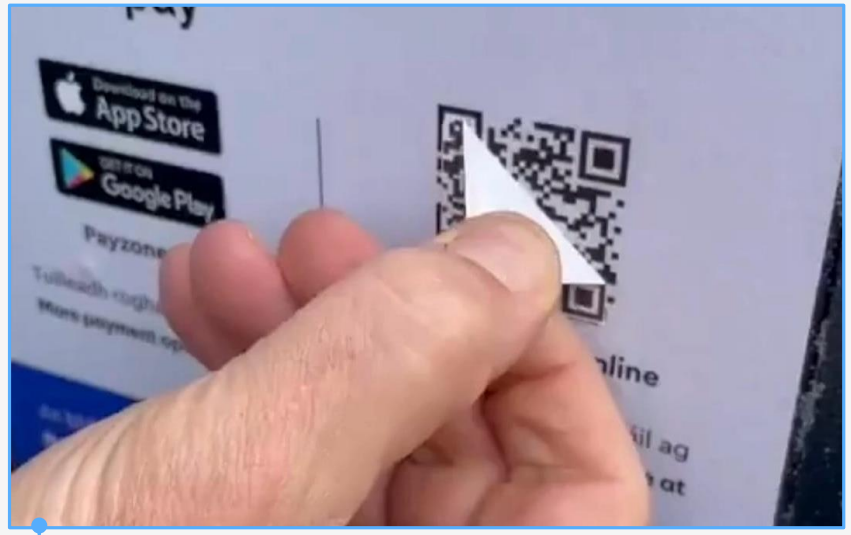

брендирование




манипуляции с типом файла




запуск вредоносного ПО




использование QR-кодов

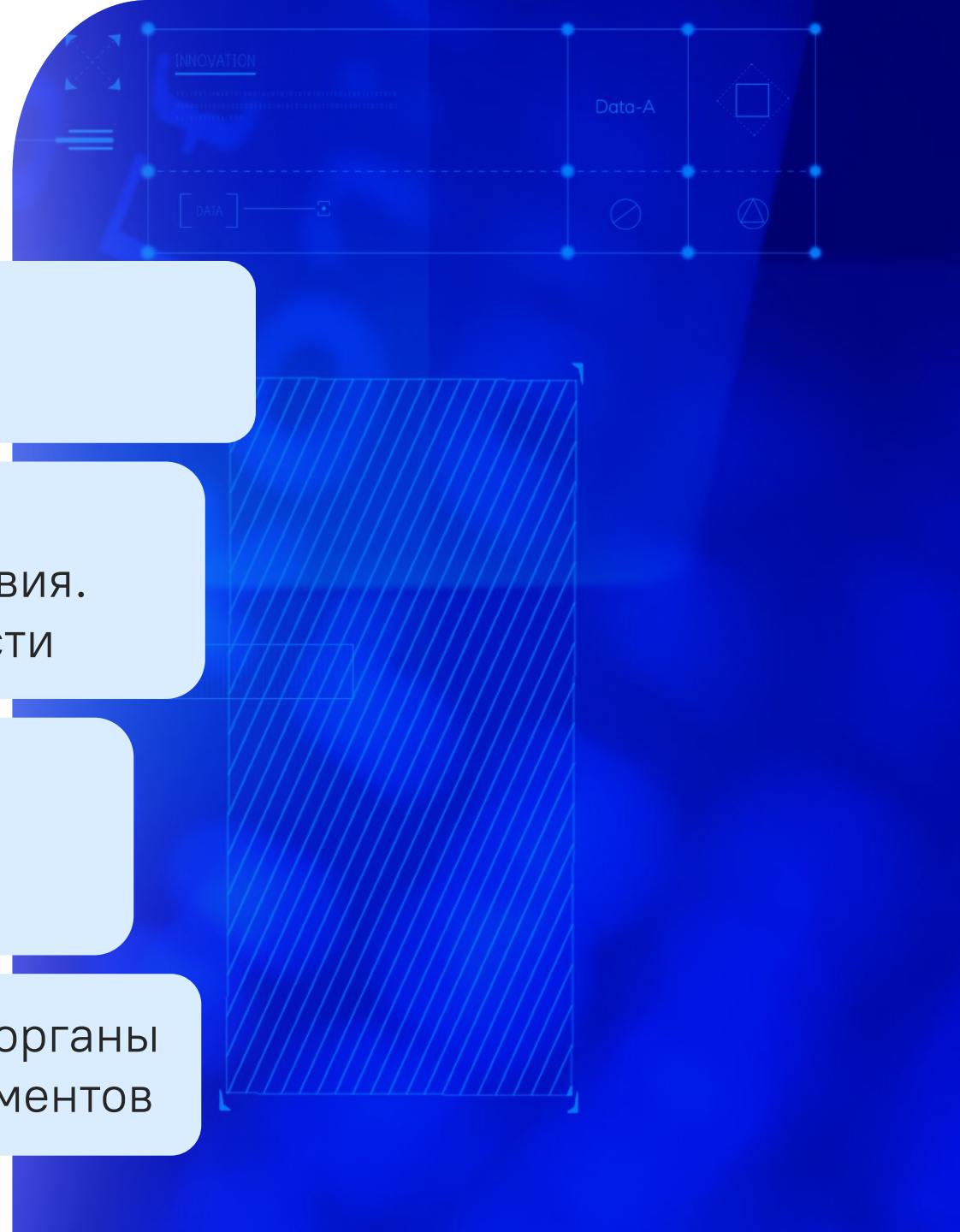
# ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ

Ваша учетная запись была или будет заблокирована/отключена

В вашей учетной записи были обнаружены подозрительные или мошеннические действия. Требуется обновления настроек безопасности

Вы получили важное сообщение. Перейдите в личный кабинет, чтобы ознакомиться

Вам пишет МВД и прочие государственные органы в момент, когда истекает срок у ваших документов

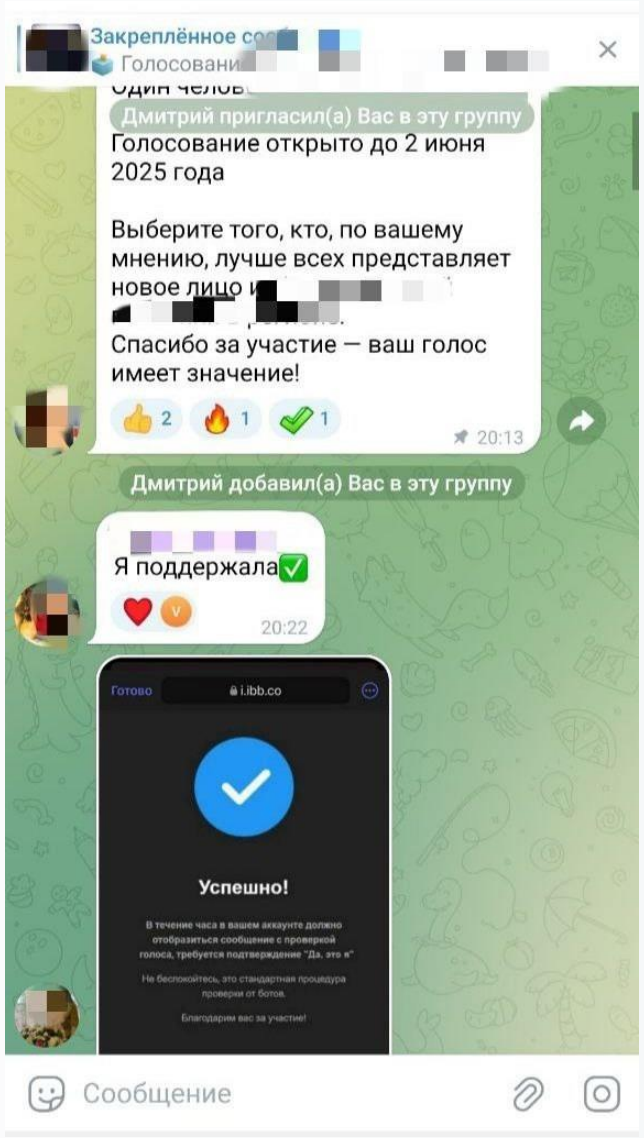


# ПРИМЕР

Сегодня в 9:01

Уважаемые родители и учащиеся будьте бдительны! Появился новый способ мошенничества. Мошенники звонят учащимся от лица администрации школы, чтобы подтвердить доступ в электронный дневник, затем требуют назвать код из отправленной смс, тем самым получая доступ к различным аккаунтам. Если не уверены, что вы общаетесь с представителем школы просто позвоните сами классному руководителю или в приёмную школы.
Правила безопасности:
1. Не называйте никаких кодов из SMS
2. Прервите разговор
Администрация школы не запрашивает данную информацию.

09:02




Сегодня, 21 февраля

привет 21:07

Добрый вечер 21:08

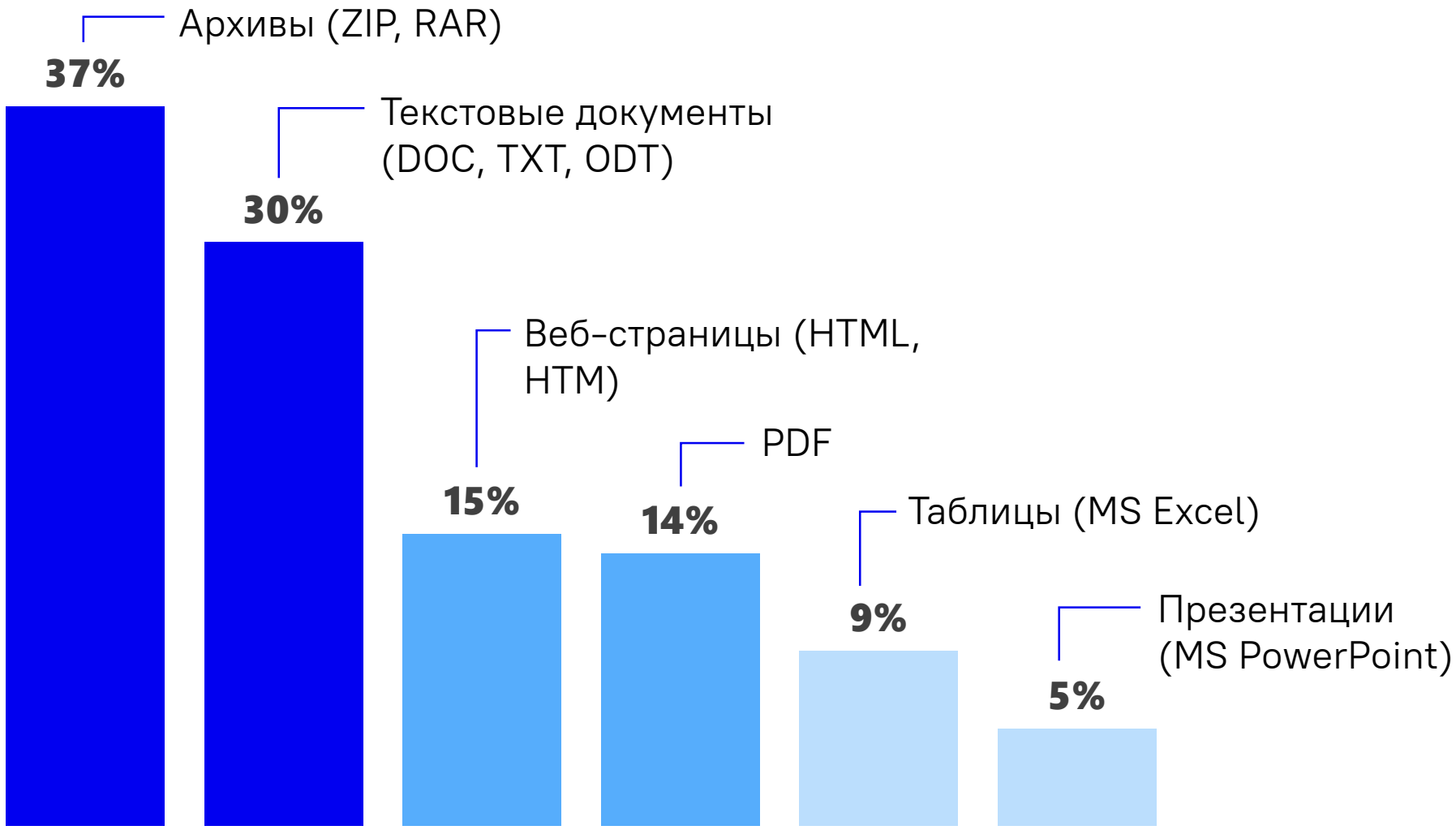
Проголосуй за Анжелику в вотсап голосовании пожалуйста. Это моя племянница
http://tinyurl.com/future-artists 21:10

А можно я вам позвоню, чтобы убедиться, что ссылка безопасна? 21:11

# КАК РАСПОЗНАТЬ ФИШИНГ

- Критическое мышление и здравый смысл
- Анализ получаемой информации от приложения, средства защиты информации (антивируса) или операционной системы
- Анализ предлагаемой гиперссылки
- Структура URL
- Анализ почтовых заголовков

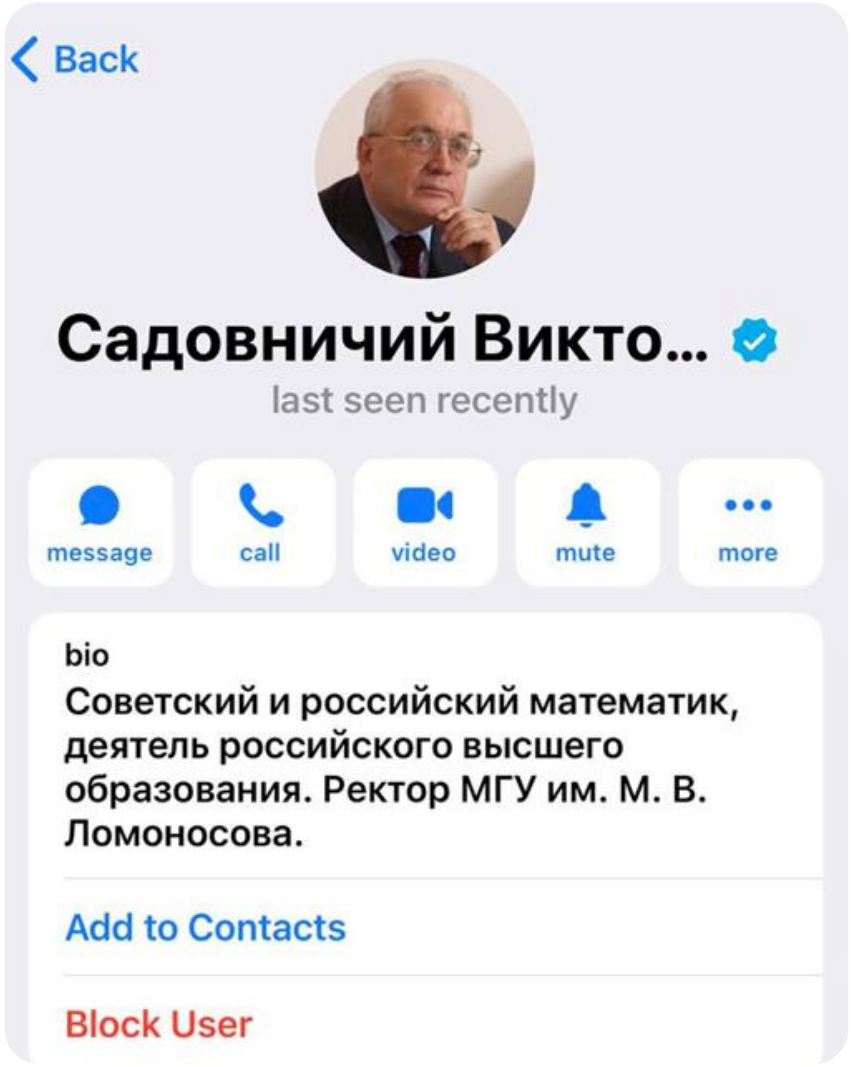
# НА КАКИЕ ВЛОЖЕНИЯ ОБРАТИТЬ ВНИМАНИЕ



DEEPFAKE

**В начале 2024 года мошенники с помощью дипфейков заставили финансиста гонконгского филиала транснациональной компании перевести им с корпоративного счета более 25 млн долларов**

# DEEPFAKE В СОЦИАЛЬНЫХ СЕТЯХ




- DeepFake в голосовых сообщениях
- DeepFake в «кружочках»
- Цифровой двойник (полная копия профиля)

# КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА?

**90%** психология

**10%** методы

# ПСИХОЛОГИЧЕСКИЕ ВЕКТОРЫ АТАК

**93%** атак

Усилители реакции

### Страх

Ваш компьютер заражен и заблокирован. Кликните здесь.

### Невнимательность

www.sbernbank.ru
www.gmall.com

### Раздражение

Чтобы отписаться, перейдите по ссылке.

### Срочность

Отчет прислать сегодня до 15:00

### Любопытство

Смотри как ты отжигаешь на видео!

### Жадность

Скидка 50% при оплате прямо сейчас!

### Желание помочь

Ваш коллега потерял свои вещи. Дайте его номер.

### Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

## Не вестись на эмоциональные триггеры – ЖАДНОСТЬ, СТРАХ, СРОЧНОСТЬ, АВТОРИТЕТ, ГНЕВ

Вопросы для самопроверки

- Ожидаю ли я это сообщение?
- Есть ли смысл в том, что от меня требуют?
- Знаю ли я автора?
- Если я это сделаю, какие могут быть последствия?
- Похоже ли это поведение на автора письма?

# ИИ И ЕГО ИСПОЛЬЗОВАНИЕ

**Генеративный искусственный интеллект—**

это тип ИИ, который может создавать новый контент и идеи, включая диалоги, истории, изображения, видео и музыку. Как и любой ИИ, он основан на моделях машинного обучения, предварительно обученных на огромных объемах данных

# БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ

Использовать для повседневных задач –

ДА

Использовать для решения конфиденциальных

НЕТ

Кейс №1

# ТЕЛЕФОННЫЕ МОШЕННИКИ

Телефонные мошенники похитили у бывшего первого замглавы аппарата Госдумы Безверхова более 44 млн рублей

1 шаг: **получили номер телефона жертвы**

Вероятно, номер Юрия Безверхова был найден в одной из баз данных, попавших в утечку

2 шаг: **установили контакт через мессенджер**

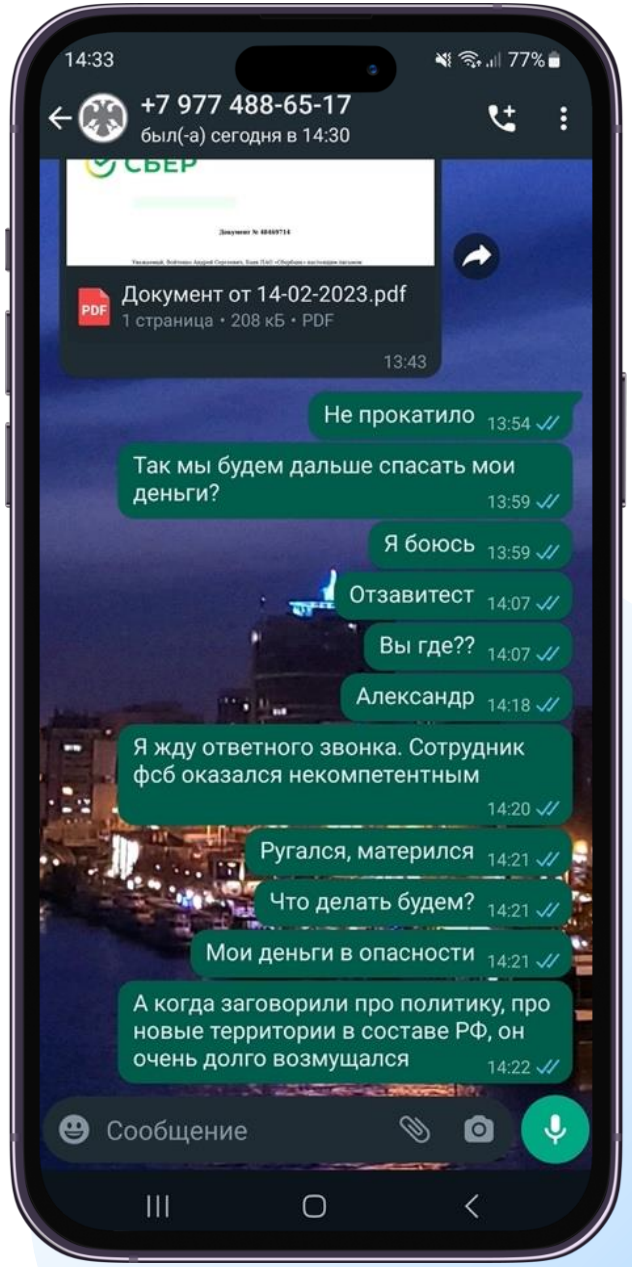
По статистике пользователи больше доверяют «неизвестным» контактам WhatsApp, чем «неизвестным» номерам телефона

3 шаг: **получили личные данные и коды подтверждения**

Под предлогом «возврата средств» или «проверки безопасности» выманили у жертвы чувствительную информацию: паспортные данные, логины, СМС-коды, возможно, данные карты и CVV-код.

4 шаг: **перевели деньги с его счета на счета сообщников**

5 шаг: **исчезли, заблокировав контакт**



# Кейс №2

## ФИШИНГ

На электронную почту поступает сообщение якобы от Федеральной службы судебных приставов (ФССП) с «предсудебным уведомлением».

1 шаг: **отправка письма с поддельного адреса**

Жертве на электронную почту приходит письмо якобы от ФССП (или другого госоргана), но с обычного адреса на mail.ru, а не официального домена.

2 шаг: **приложение PDF-документа с «электронной подписью»**

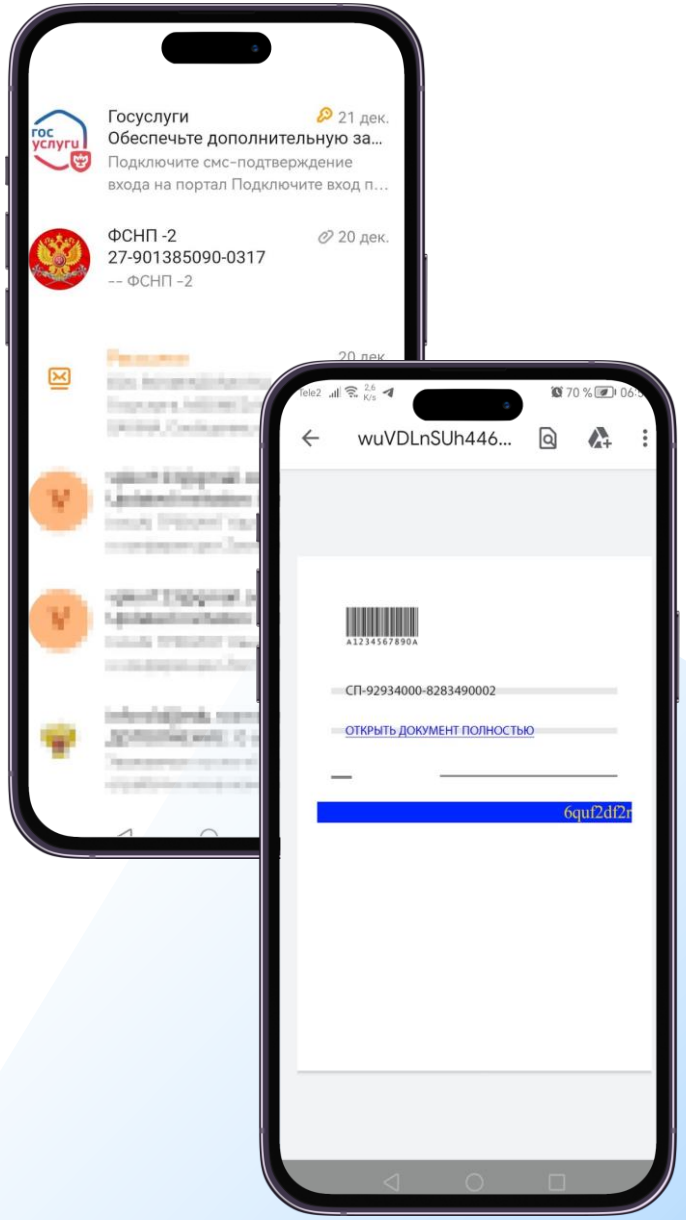
Во вложении—формально оформленный PDF-файл, якобы подписанный ЭЦП. Это придает письму видимость официальности.

3 шаг: **создание чувства срочности и давления**

Пользователю сообщают о «долге» в 300 рублей и пугают последствиями: блокировка банковских карт, запрет на выезд и т. п.

4 шаг: **ввод данных и подтверждение оплаты**

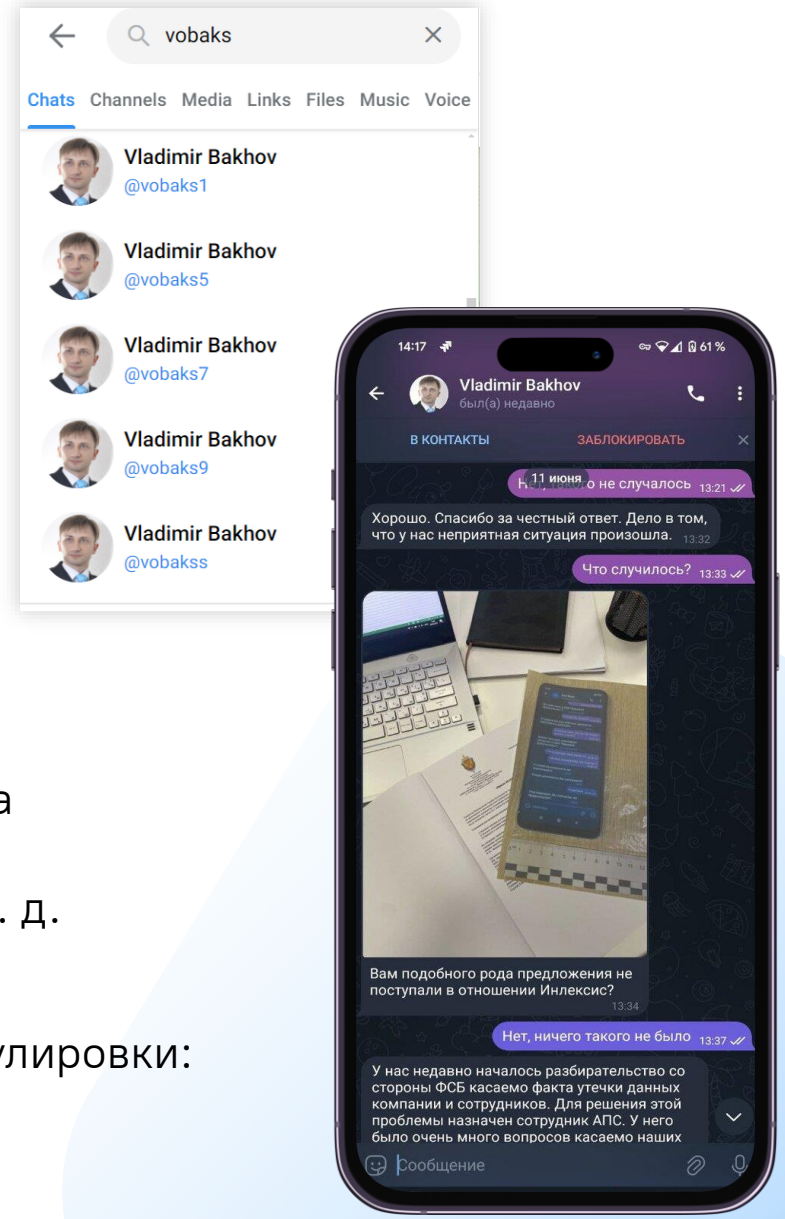
5 шаг: **настоящее списание — уже на другую сумму и другому получателю**



# Кейс №3

## FakeBoss

> Мэр Благовещенска в своем телеграм-канале предупредил, что от его имени коллегам пишет клон—и что это мошенники. Для фейкового аккаунта мэра Белогорска аферисты раскошелились на Premium-статус и синюю галочку верификации профиля.




### 1 шаг: сбор информации о компании

Мошенники изучают структуру организации: кто за что отвечает, кто подчиняется кому, кто занимается финансами.

### 2 шаг: подделка контакта руководителя

- Создают e-mail или аккаунт в мессенджере, визуально похожий на адрес директора (например: ivan.petrov@companiy.ru).
- Выдают себя за начальника—через почту, WhatsApp, Telegram и т. д.

### 3 шаг: контакт с сотрудником и давление

Пишут бухгалтеру или менеджеру от имени "шефа", используя формулировки:
— «Это срочно»
— «Не обсуждай с коллегами»
— «Я на встрече, просто сделай»
Задача—вызвать стресс и вынудить действовать без проверок.

# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

ПО и устройства:

01

Устанавливать только официальное ПО, своевременно обновлять

02

Использовать антивирусы

03

Работать из непривилегированных учеток, не «взламывать» устройства

04

Устанавливать пароли на вход в устройство

05

Подключить удаленное уничтожение информации при пропаже устройства

06

Не оставлять устройства без присмотра, блокировать экран

# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Социальные сети и мессенджеры:

01

Парольная политика

02

Изучить вкладку «безопасность» во всех сервисах, подключить 2FA

03

Не выкладывать документы в открытый доступ

04

Не выкладывать то, что может (и будет!) использовано против вас (в том числе семейные аккаунты)

05

Постараться максимально почистить историю о себе

06

Помнить про фишинг через любые каналы доставки

# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Деанонимизация:

01

Чистить метаданные в документах при необходимости их пересылки или размещения в открытые источники информации (убирать автора у документа word, геолокацию с фотографий)

02

Не использовать онлайн-редакторы документов и файлов

03

не использовать облачные хранилища

04

не использовать персональные данные при регистрации (если это строго не требуется сервисом)

05

не использовать общедоступные VPN

# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Чат-боты и ИИ:

01

Не вводите конфиденциальные данные

02

Читайте политику конфиденциальности

03

Используйте корпоративные версии (по возможности)

04

Минимизируйте интеграции с базами данных на ПК

05

Проверяйте сгенерированные ответы

06

Внедрите политику использования и внутренний регламент по работе с ИИ

# ПОЛЕЗНЫЕ РЕСУРСЫ И ССЫЛКИ

## Официальные ресурсы

Федеральная служба по техническому и экспортному контролю (ФСТЭК России):

fstec.ru

Национальный координационный центр по компьютерным инцидентам (НКЦКИ):

safe-surf.ru

## Международные ресурсы по информационной безопасности:

Агентство Европейского союза по кибербезопасности (ENISA):

enisa.europa.eu

Национальный институт стандартов и технологий США (NIST):

nist.gov