ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО ВОЛГОГРАДСКОЙ ОБЛАСТИ

СЛУЖИМ РОССИИ, СЛУЖИМ ЗАКОНУ!

«Профилактика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»

2025

План
занятия

1. Статистические сведения и материальный ущерб
2. Основные способы и схемы IT-преступлений
3. Законодательные инициативы против IT-преступлений
4. Профилактический материал

1 Статистические сведения

Регистрация IT-преступлений

Наибольшая

регистрация IT-преступлений отмечается в выделенных на карте районах

динамика регистрации за январь				
всего ИТТ	пр.г.	тек.г.	динамика	процент
ОП-6(СОВЕТСКИЙ)	378	754	376	99.5
КОТЕЛЬНИКОВО	121	158	37	30,6
ОКТЯБРЬСКИЙ	28	36	8	28,6
КИКВИДЗЕНСКИЙ	22	27	5	22,7
ОП-2 (КРАСНООКТЯБРЬСКИЙ)	481	579	98	20,4
КАМЫШИНСКИЙ	557	638	81	14,5
ОП-5(ВОРОШИЛОВСКИЙ)	394	431	37	9,4

Материальный ущерб

по итогам

9 МЕС 2025 года

составил

1.4 млрд руб

по итогам

9 мес 2024 года

составил

1.5 млрд руб

Количество IT-преступлений

по итогам

9 мес 2025 года

составило

9485

по итогам

9 мес 2024 года

составило

10211,

- **на 7.1% меньше**,

чем в прошлом году

Основной массив IT-преступлений

составляют

имущественные преступления,

большинство из них

IT-мошенничества

2
Основные способы и схемы IT-преступлений

Основные способы и схемы IT-преступлений

01

Телефонные мошенничества
под предлогом звонка

сотрудника банка

Основные способы и схемы IT-преступлений

02

Телефонные мошенничества
с использованием

аккаунтов руководителей

в мессенджерах

Основные способы и схемы IT-преступлений

03

Телефонные мошенничества

с продажей движимого/ недвижимого имущества

и перевода денег мошенникам

Основные способы и схемы IT-преступлений

04

Телефонный звонок якобы

оператора сотовой связи

о замене сим-карты

Основные способы и схемы IT-преступлений

05

Телефонный звонок якобы

медицинского работника

для записи на диспансеризацию или флюорографию

Основные способы и схемы IT-преступлений

06

Телефонный звонок якобы

представителя энергосбыта

для записи на замену счетчиков

Основные способы и схемы IT-преступлений

07

Телефонный звонок якобы

представителя соцуслуг

о выплате по спец программе,
под которую вы подпадаете

Основные способы и схемы IT-преступлений

08

Телефонный звонок якобы

представителя госструктур

под предлогом
«родственник попал в беду»

Основные способы и схемы IT-преступлений

09

Биржевое мошенничество,

инвестирование денег,
быстрый доход

Основные способы и схемы IT-преступлений

10

Мошенничества

с использованием торговых интернет-площадок

(авито, юла, вайлберис, озон)

Основные способы и схемы IT-преступлений

11

Быстрый заработок

под видом
«курьер на наличные»

Основные способы и схемы IT-преступлений

12

Повторный обман

под предлогом возврата ранее похищенных мошенниками денег и понуждение к деструктиву, диверсиям

Основные способы и схемы IT-преступлений

13

Сообщения в мессенджерах

с вредоносными файлами формата .apk с вопросами типа «это ты на фото?»

Если у вас **Android, то любое приложение, установленное на вашем устройстве, использует **.apk** **Android Package Kit** – это специальный установочный файл, содержащий код, ресурсы и параметры программы.*

Основные способы и схемы IT-преступлений

Какие бывают вредоносные APK?

Фишинговые APK

– замаскированные под легальные приложения (например, «Google Play Update»), крадут пароли и платёжные данные

Троянские APK

– получают доступ к SMS и банковским приложениям, подписывают жертву на платные услуги

Шпионские APK

– скрыто записывают звонки, отслеживают местоположение и копируют переписки

Бэкдоры

– позволяют хакерам удалённо управлять устройством

Основные способы и схемы IT-преступлений

Как защититься от опасных APK?

01

Скачивайте приложения только из проверенных источников

💬**RuStore** – официальный российский магазин приложений, созданный при поддержке VK и Минцифры России. В RuStore каждое приложение проходит проверку безопасности на соответствие требованиям перед публикацией. Также проверку проводят Google Play, Galaxy Store, Huawei AppGallery, F-Droid.

02

Используйте надежные антивирусные приложения

03

Используйте сервисы анализа APK

💬VirusTotal, HashDroid, Checksum Calculator позволяют проверить файлы перед установкой.

04

Следите за разрешениями

💬Если фонарик требует доступ к контактам или камере – это тревожный сигнал.

3 Законодательные инициативы против IT-преступлений

Поправки в Федеральный закон "О связи"

1 Введены **строгие меры** по **верификации абонентов** мобильной связи

2 **SIM-карты** активируются только после подтверждения данных через портал **«Госуслуги»** или **Единую биометрическую систему**

3 **Иностранным гражданам** для получения SIM-карты необходимо оформить СНИЛС, зарегистрироваться на **«Госуслугах»** и сдать **биометрические данные**

4 **Ограничено количество номеров**, которые могут быть зарегистрированы на одного человека: не более **20** для граждан России и не более **10** для иностранцев

Банки станут быстрее включать реквизиты мошенников в свои системы

Банк России
установил время, в течение которого
кредитные организации будут вносить реквизиты злоумышленников,
поступившие из базы данных регулятора,
в собственные системы противодействия подозрительным операциям

с 22 октября 2024 года
для крупных банков, а также кредитных организаций, значимых на рынке платежных услуг, этот срок составит **два часа**, а

с 1 января 2025 года
– **один час**

В отношении остальных банков установлен срок в **три часа**

Изменения в УК РФ

В Уголовный кодекс
Российской Федерации внесены изменения, согласно
которым за

вовлечение несовершеннолетних в преступную деятельность

через Интернет грозит

лишение свободы до 6 лет

Изменения в УК РФ

Новая статья
272.1 УК РФ

«Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения»

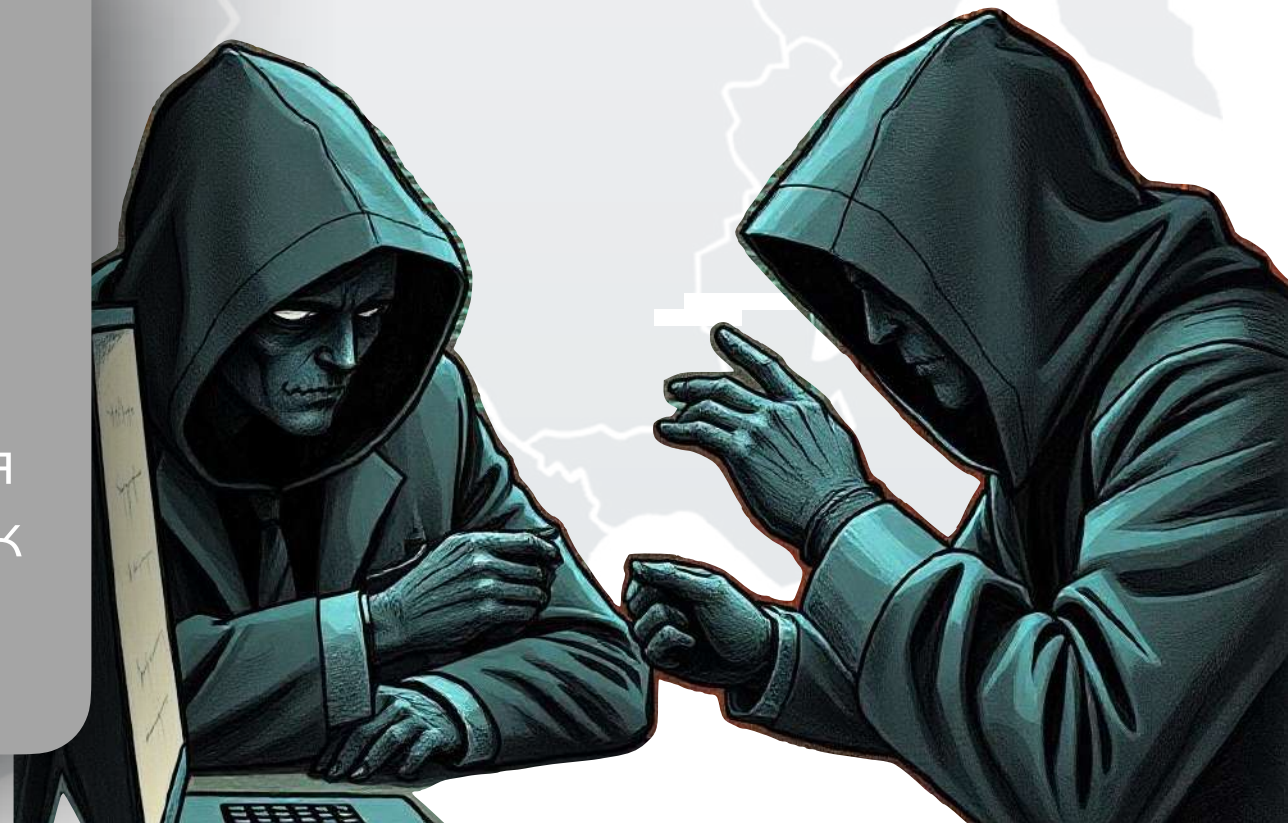
Наказание может достигать

до 10 лет

лишения свободы

Концепция государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий

Одной из важных частей государственной системы должна стать **специализированная цифровая платформа**, обеспечивающая оперативный обмен информацией между **правоохранительными органами**, **Центральным банком**, **кредитными организациями** и **операторами связи** для установления всех обстоятельств и лиц, причастных к мошенническим действиям



Кроме того, документ предполагает принятие мер, направленных на:

Мониторинг информационных ресурсов и блокировку противоправного контента в сети Интернет

Уточнение порядка предоставления цифровых услуг.

Оперативное приостановление операций с денежными средствами, используемыми в преступных схемах

Развитие криминалистических методов и цифровых инструментов для расследования преступлений.

Участие в международных инициативах по борьбе с киберпреступностью.

Обучение специалистов и повышение их технической подготовки.

Информирование населения о рисках и методах защиты от цифровых преступлений.

Минцфиры России разработали проект поправок в уголовный кодекс

Вводится законодательное определение ИИ. Использование ИИ-технологий становится квалифицирующим признаком преступлений

Вводятся отдельные нормы об ответственности за кибератаки различных сценариев

Устанавливаются смягчающие обстоятельства для сотрудников, допустивших нарушения правил эксплуатации объектов КИИ

Фактически: *в* Уголовный кодекс вводится **понятие технологий искусственного интеллекта**. В понимании законопроекта, **ИИ – это комплекс технологий,** которые позволяют имитировать мыслительные (когнитивные) функции и получать при выполнении задач результаты, сопоставимые с результатами интеллектуальной деятельности человека

Мошенники сначала создают ложную, но правдоподобную угрозу, чтобы выбить человека из равновесия

Новый приём: убеждают «подтвердить номер паспорта голосом» – такого способа не существует

Схема:

звонок от «ЕМИАС» → затем «Госуслуги» про «взлом» → сообщения от «Военной прокуратуры» с требованием срочных действий

Цель – вызвать панику и вынудить передать данные/доступ

Что нельзя хранить в смартфон

01 **Документы:** фото/сканы паспорта, СНИЛС, ИНН, прав, карт – используют для фейков и доступа. Храните в защищённом облаке с 2FA.

02 **Пароли и коды:** заметки, мессенджеры, автосохранение в браузере – риск. Используйте менеджер паролей или офлайн-хранение.

03 **Банковские уведомления:** раскрывают привычки и доход – регулярно очищайте историю.

04 **Конфиденциальная переписка:** в чатах часто есть карты, PIN, ответы на вопросы – удаляйте чувствительное или храните в защищённом резерве.

05 **Фотографии в галерее:** рабочие документы и интимные фото – переносите в закрытые папки или удаляйте.

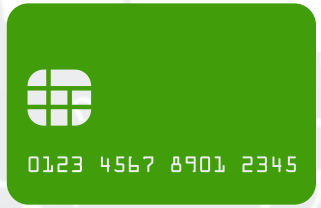
06 **Контакты:** номера родственников/коллег – удаляйте лишние, резервируйте защищённо, не храните личные примечания

4
Профилактический материал

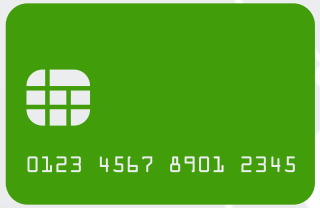
- Будьте **избирательны при покупке в интернет-магазинах**. Изучайте отзывы, информацию о продавце, внимательно сверяйте адрес сайта
- **Не сообщайте коды** из сообщений незнакомым, а также другую важную информацию: номер карты, CVC-код и т.д.
- **Не вводите данные банковской карты** на сомнительных сайтах и используйте отдельную карту для онлайн-шоппинга
- **Не авторизуйтесь на незнакомых сайтах** через аккаунты в соцсетях и мессенджерах.
- Подключите **двухфакторную аутентификацию** для входа в свои учетные записи. Используйте разные сложные пароли для каждого аккаунта и регулярно их обновляйте
- Не открывайте **подозрительные письма** и не скачиваете файлы из ненадежных источников
- Не отвечайте на **звонки с незнакомых номеров**. Установите защиту от спама и определитель номера
- Всегда проверяйте информацию и **не принимайте поспешных решений**

«Золотой час» после компрометации

В медицине есть понятие **«Золотой час»**, которое используется в реаниматологии для отсчета времени после получения травмы, когда наиболее высок шанс, что первая помощь и лечение наиболее эффективны



Когда человек скомпрометировал свои учетные записи, устройства, аккаунты в онлайн-сервисах, у него тоже есть «Золотой час», чтобы минимизировать последствия



Если вы только что разгласили данные, которые мошенники могут использовать для взлома учетной записи, например, код двухфакторной идентификации, CVV и т.д., то стоит предпринять следующие шаги:

«Золотой час» Банковская карта после компрометации

Риск: взлом учетной записи в банковском сервисе, кража денег со счетов, оформление кредита на жертву

01

Необходимо оперативно сменить пароль, код доступа в банковский сервис

02

Заморозить банковские карты и счета

03

Оперативно свяжитесь с банком по номеру, указанному на банковской карте или официальном сайте, сообщите о звонке или сообщении - продиктуйте им номер телефона злоумышленников

04

Предупредите родных, близких, работодателя, что пока ваши банковские карты могут быть скомпрометированы и лучше не переводить на них деньги

«Золотой час» Популярный государственный сервис после компрометации

Риск: компрометация личной информации, подтверждение личности в кредитной организации, сервисе мобильного оператора, оформление кредита.

01

Необходимо оперативно сменить пароль, код доступа в банковский сервис

02

Позвоните на горячую линию сервиса и сообщите о возможной компрометации

03

Если есть доступ к личному кабинету, проверьте заявки, разрешения, в том числе в сторонних сервисах

04

Обратитесь в МВД и передайте всю возможную информацию об инциденте

«Золотой час» Мобильный номер после компрометации

Риск: злоумышленники смогут сбросить пароли и получать коды двухфакторной идентификации во всех сервисах, в которых указан украденный номер

01

Свяжитесь с вашим мобильным оператором (по официальному номеру телефона, в приложении или в салоне связи) и сообщите, о том, что ваш номер, может быть, скомпрометирован

02

По возможности, привяжите сервисы, соцсети, мессенджеры к нескомпрометированному номеру телефону

03

Внимательно следите за приходящими смс о блокировке, перевыпуске или переносе SIM-карты

04

Предупредите родных, друзей, коллег, что с вашего номера могут звонить, писать злоумышленники с просьбой одолжить денег, поделиться чувствительной информацией и т.д.

«Золотой час» Мессенджеры и соцсети после компрометации

Риски: компрометация переписок, доступ злоумышленников к чувствительной информации, мошенничество с просьбой одолжить деньги, шантаж. Использование аккаунта в дальнейших сложных киберпреступных схемах

01

Попробуйте сменить пароль на совершенно новый и достаточно сложный, включить двухфакторную идентификацию

02

В списке привязанных к аккаунту устройств нужно срочно отключить все незнакомые и недоступные вам девайсы

03

Смените пароли, защитите ссылки, которые могли быть в переписках

04

Если подозреваете, что учетная запись скомпрометирована, например, не приходят одноразовые коды безопасности, то следуют сразу обратиться в службу поддержки

05

Предупредите ваш круг контактов, что вашим аккаунтом в мессенджере могут завладеть злоумышленники с целью, например, рассылать сообщения с просьбой одолжить денег

06

Попросите родственников и близких: если мошенники будут писать с украденного контакта, то следует массово жаловаться в службу поддержки мессенджера.

Распространите среди знакомых и родственников!

Онлайн-занятия по финансовой грамотности для старшего поколения

ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ ПО ВОЛГОГРАДСКОЙ ОБЛАСТИ

СЛУЖИМ РОССИИ, СЛУЖИМ ЗАКОНУ!

Спасибо за внимание!

24 июля 2024

Скачай презентацию