ЧЕК-ЛИСТ ТВОЕЙ БЕЗОПАСНОСТИ

КЛАССИФИКАТОР УГРОЗ

Этот чек-лист поможет вам систематизировать знания о том, какие преступления существуют в цифровом мире, и распознавать их на дальних подступах

ШКОЛА КИБЕРБЕЗОПАСНОСТИ ДВИЖЕНИЯ ПЕРВЫХ

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

ФИНАНСОВОЕ МОШЕННИЧЕСТВО И ДИВЕРСИИ

Цель преступников: Хищение денег и дестабилизация общества через запуганных граждан

Звонок «из банка» 01

Сценарий

Лже-сотрудник сообщает о подозрительной операции, попытке оформления кредита или утечке данных. Цель — заставить жертву перевести личные накопления или оформить кредит.

Маркеры опасности

- ☐ *«Служба безопасности»*
- ☐ *«Ваш счёт заблокирован»*
- ☐ *«Сейчас я переключу вас на сотрудника ЦБ/МВД/ФСБ»*
- ☐ *«Произошла утечка данных»*
- ☐ *«Код из СМС»*

Звонок «от правоохранителей» 02

Сценарий

Звонящий представляется следователем, дознавателем, «ФСБ». Говорит, что вы стали жертвой мошенников, и для поимки преступников нужно участвовать в «спецоперации».

Маркеры опасности

- ☐ *«На ваше имя пытаются взять кредит»*
- ☐ *«Вы поможете следствию»*
- ☐ *«Не разглашайте гостайну, иначе будете привлечены к ответственности»*
- ☐ *«Оформите кредит и передайте курьеру/ переведите на "зеркальный счёт"»*

Склонение к диверсии 03

Сценарий

Самый опасный этап. Когда у жертвы больше нет денег, ей говорят, что она может вернуть их или «помочь стране», совершив поджог военкомата, автомобиля, административного здания или подрыв в людном месте.

Маркеры опасности

- ☐ *«Вы уже перевели деньги мошенникам, теперь вы соучастник»*
- ☐ *«У вас есть шанс все исправить»*
- ☐ *«Вам нужно взять коктейль Молотова»*
- ☐ *«Пришлите фото/видео поджога как доказательство»*

СОЗДАНИЕ ПРЕСТУПНОЙ ИНФРАСТРУКТУРЫ

Цель преступников: Обеспечить анонимность и техническую возможность для обзвонов и вывода денег

GSM-шлюзы 01

GSM-шлюз *(Global System for Mobile Communications шлюз) — это устройство, которое служит для подключения телефонных систем или устройств передачи данных к мобильным сетям через SIM-карты. Работает как промежуточное звено между телефонной системой (например, офисной АТС) и сотовыми операторами, обеспечивая возможность обмена данными или голосовыми вызовами через мобильные сети.*

Что делают преступники

Покупают и устанавливают оборудование, которое позволяет массово прозванивать жертв, подменяя номера. Оборудование часто ставят в квартирах ничего не подозревающих граждан.

Кого ищут в соучастники

Людей, готовых за небольшую плату установить у себя «оборудование для интернета/связи» (шлюз), администрировать его и менять сим-карты.

Сим-карты 02

Что делают преступники

Массово скупают сим-карты, оформленные на реальных людей, для использования в шлюзах и регистрации аккаунтов в мессенджерах.

Кого ищут в соучастники

Людей, готовых оформить на себя сим-карту и продать её за 100-300 рублей. Часто находят среди студентов и малообеспеченных слоёв населения.

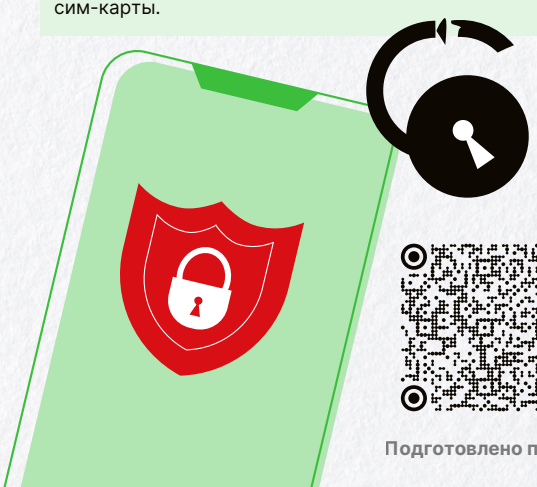
Банковские карты (дропы) 03

Что делают преступники

Скупают или арендуют банковские карты, оформленные на подставных лиц (дропов), для транзита и обналичивания похищенных средств.

Кого ищут в соучастники

Людей для привлечения в качестве курьеров (забрать, передать, перевести, положить на кошелёк, а также совершить любые другие действия с денежными средствами по указанию куратора)



Повышай свой личный уровень противодействия угрозам в сети и становись участником большой команды Школы КиберБезопасности Первых.

Больше киберзнаний, умений, навыков ты найдёшь на сайте

киберволонтеры.будьвдвижении.рф

Подготовлено при экспертизе МВД Россиии и Минпросвещения России

ЧЕК-ЛИСТ ТВОЕЙ БЕЗОПАСНОСТИ

КЛАССИФИКАТОР УГРОЗ

Этот чек-лист поможет вам систематизировать знания о том, какие преступления существуют в цифровом мире, и распознавать их на дальних подступах

ШКОЛА КИБЕРБЕЗОПАСНОСТИ ДВИЖЕНИЯ ПЕРВЫХ

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

ТЕХНИЧЕСКИЕ АТАКИ (ХАКИНГ)

Цель преступников: Нарушить работу критической инфраструктуры или частных компаний, уничтожить данные, парализовать управление

01 DDoS-атаки

На что направлена

На сайты госорганов, банков, аэропортов, больниц, «скорой помощи».

Последствия для обычных граждан

Невозможность записаться к врачу, оплатить услуги, заказать билет, зайти на портал госуслуг. Создание хаоса и паники.

02 Взлом и шифрование данных (вирусы-вымогатели)

На что направлена

На серверы больниц, школ, заводов, транспортных компаний. Данные шифруют и требуют выкуп за их расшифровку.

Последствия для обычных граждан

Отмена операций, сбои в расписании, утечка персональных данных (ваши паспортные данные, история болезней могут оказаться в сети).

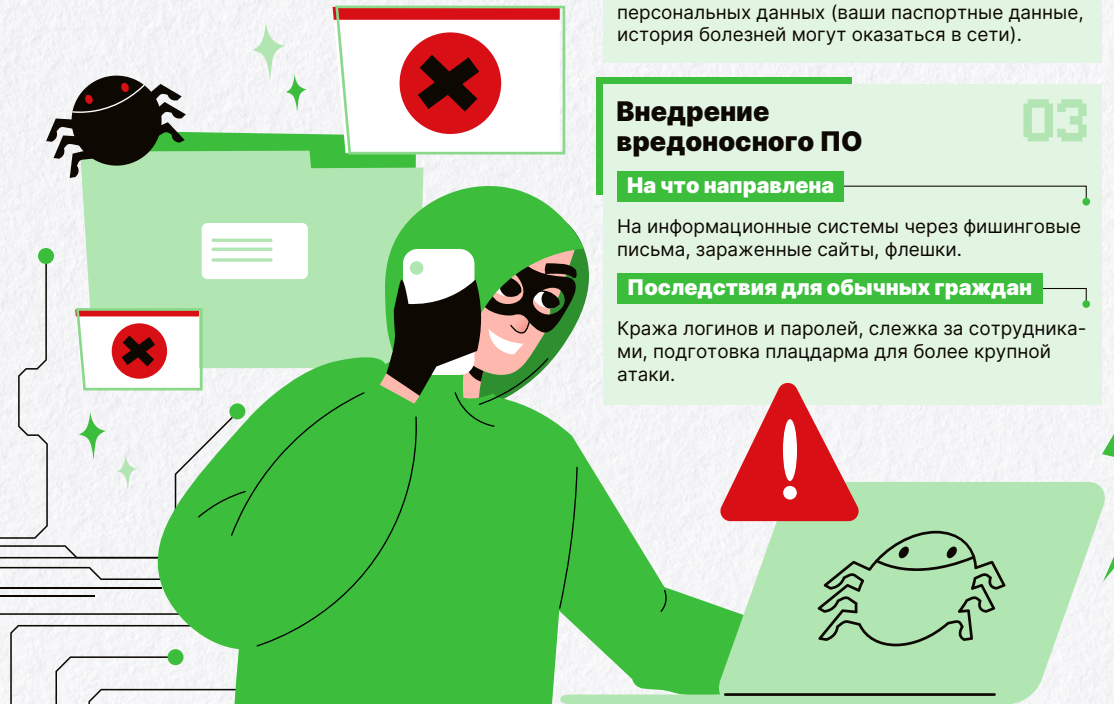
03 Внедрение вредоносного ПО

На что направлена

На информационные системы через фишинговые письма, зараженные сайты, флешки.

Последствия для обычных граждан

Кража логинов и паролей, слежка за сотрудниками, подготовка плацдарма для более крупной атаки.



ВОЗДЕЙСТВИЕ НА СОЗНАНИЕ (ПСИХОЛОГИЧЕСКИЕ ОПЕРАЦИИ)

Цель преступников: Посеять панику, расколоть общество, дискредитировать власть, вовлечь молодежь в деструктив

01 Сваттинг (Swatting)

Описание

Ложные сообщения о минировании школ, торговых центров, больниц, вокзалов.

Кто в зоне риска

Все общество. **Цель** — эвакуации, паника, отвлечение сил правопорядка, создание атмосферы нестабильности.

02 Деанон (Doxing)

Описание

Публикация в открытом доступе личных данных людей (адреса, паспорта, переписки, налоговая тайна) с целью травли, шантажа или физической расправы.

Кто в зоне риска

Публичные личности, госслужащие, военные, а также обычные граждане, вступившие в конфликт в сети.

03 Буллинг (Кибертравля)

Описание

Агрессивное преследование, оскорбления, унижения в соцсетях и мессенджерах, часто группой лиц.

Кто в зоне риска

Подростки, люди с активной гражданской позицией.

04 Пропаганда деструктивных ценностей

Описание

Вовлечение в опасные субкультуры, склонение к суициду, романтизация насилия и жёстокости (в т.ч. к животным), навязывание чуждых моральных норм.

Кто в зоне риска

Подростки и молодёжь. Вербовщики действуют через игры, анонимные форумы, создавая ложный авторитет.

Повышай свой личный уровень противодействия угрозам в сети и становись участником большой команды Школы КиберБезопасности Первых.

Больше киберзнаний, умений, навыков ты найдёшь на сайте

киберволонтеры.будьвдвижении.рф

Подготовлено при экспертизе МВД Россиии и Минпросвещения России

ЧЕК-ЛИСТ ТВОЕЙ БЕЗОПАСНОСТИ

ЗОЛОТЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

ШКОЛА КИБЕРБЕЗОПАСНОСТИ ДВИЖЕНИЯ ПЕРВЫХ

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

БЕЗОПАСНОСТЬ ЗВОНКОВ И ОБЩЕНИЯ

#1 Правило «Незнакомец = Опасность»

- **Никогда не отвечайте на звонки с неизвестных номеров.** Если звонок важный, перезвонят еще раз или напишут СМС. Если перезвонили — не берите трубку сразу, дайте себе время подумать.
- **Введите через поисковую строку в браузере номер телефона, с которого поступил звонок.** С вероятностью 80% вы найдёте отзывы: «Мошенники», «Телефонные спамеры».

#2 Правило «Мессенджер = Красная зона»

- **Запомните раз и навсегда: никакой официальный сотрудник** (банка, поликлиники, собеса, ФСБ, следователь) **не будет звонить вам через мессенджеры.** Используется только официальная телефонная связь или личный кабинет на официальном сайте.
- **В мессенджерах номер телефона — это просто картинка.** Звонок идет по ID. Если у вас высветился номер, это подделка.

#3 Правило «Тишина в эфире» (защита от дипфейков)

Искусственный интеллект может скопировать ваш голос по одной фразе. В разговоре с незнакомцем:

- **Не произносите:** *«Да», «Нет», «Подтверждаю», «Согласен», «Я, ФИО»*
- **Не называйте коды из СМС, паспортные данные, номера карт, PIN-коды, CVV**

#4 Правило «Проверка ссылки»

- **Никогда не переходите по ссылкам в сообщениях от незнакомцев.**
- Если ссылка пришла от друга (вдруг его взломали), **свяжитесь с ним по телефону и уточните,** что он прислал.
- Перед переходом **наведите мышку на ссылку** (на компьютере) **или зажмите палец** (на телефоне), **чтобы увидеть реальный адрес.** Он может оказаться мошенническим: g0s-uslugi.ru вместо gosuslugi.ru.

ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

#1 Двухфакторная аутентификация (2FA) — ваш главный щит

- **Включите 2FA везде, где это возможно:** Госуслуги, электронная почта, социальные сети, банковские приложения.
- Что это дает: даже если мошенники узнают ваш пароль, они не смогут войти в аккаунт без подтверждения по СМС или из приложения-аутентификатора.

#2 Настройки мессенджеров и антивирус

- Зайдите в настройки мессенджера и **отключите автоматическую загрузку медиафайлов** (фото, видео). Так вы не скачаете вирус случайно.
- **Установите антивирус** на телефон и компьютер. Да, на телефон тоже. Android — Kaspersky, Dr.Web и др. iPhone — могут быть уязвимы.

#3 Пароли

- **Не используйте один и тот же пароль** для всех сайтов.
- Самые популярные пароли (123456, qwerty, password) взламываются за секунду.
- Используйте менеджеры паролей, чтобы хранить сложные комбинации.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНЫВАЮТ

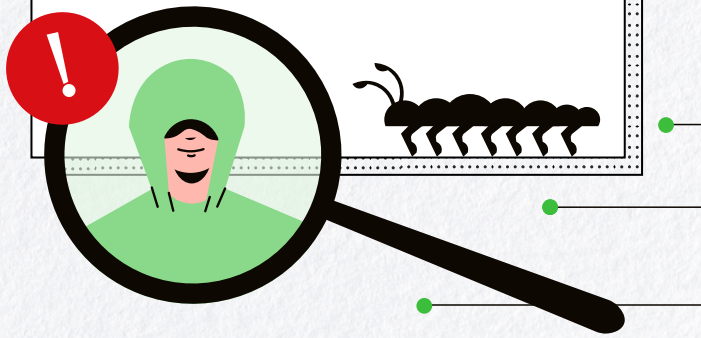
Алгоритм действий

01 **Сразу кладите трубку.** Не вступайте в диалог. Мошенники — «профессиональные психологи»

02 **Не поддавайтесь на угрозы.** Фразы *«вас посадят», «ваши деньги сгорят», «сейчас приедет наряд»* — это ложь. **Настоящий сотрудник полиции не решает вопросы по телефону**

03 **Перепроверяйте информацию.** Положите трубку и сами позвоните в банк по официальному номеру и в полицию по номеру **102** или **112**

04 **Сообщите близким.** Мошенники часто говорят: *«Никому не говорите, это тайна, иначе сорвётся спецоперация»*. Это 100% признак обмана. Обсудите это с родственником или другом — свежий взгляд сразу увидит подвох



Повышай свой личный уровень противодействия угрозам в сети и становись участником большой команды Школы КиберБезопасности Первых.

Больше киберзнаний, умений, навыков ты найдёшь на сайте

киберволонтеры.будьвдвижении.рф

Подготовлено при экспертизе МВД Россиии и Минпросвещения России

ЧЕК-ЛИСТ ТВОЕЙ БЕЗОПАСНОСТИ

НЕ СТАНЬ СООБЩНИКОМ

Внимательно прочитайте каждый пункт. Незнание закона не освобождает от ответственности, а наивность приведет в тюрьму

ШКОЛА КИБЕРБЕЗОПАСНОСТИ ДВИЖЕНИЯ ПЕРВЫХ

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

ЧЕРНЫЙ СПИСОК «ПОДРАБОТОК»

Если вам предлагают что-то из этого списка — вас вербуют для участия в преступной схеме. Даже если обещают «все чисто» и «просто курьером»

01 Продажа или аренда банковских карт

Вам говорят:

«Карта нам нужна для обнала криптовалюты/перевода зарубежных платежей/экономии налогов. Просто оформи на себя, мы платим 5000 рублей в месяц»

Реальность:

На вашу карту будут поступать деньги, украденные у бабушек и инвалидов. Вы — соучастник (дроп).

Статья УК РФ:

187 («Неправомерный оборот средств платежей»). Срок — **до 6 лет лишения свободы.**

02 Продажа сим-карт

Вам говорят:

«Сдай симки, которые никому не нужны. За каждую дадим 200 рублей. Или оформи новые и сдай нам»

Реальность:

С вашей сим-карты позвонят пенсионеру, скажут: «Ваш сын в беде, нужны деньги», и **украдут последнее. Все следы ведут на вас.**

Статья УК РФ:

274 («Нарушение правил эксплуатации средств хранения...»). Срок — **до 6 лет лишения свободы.**

03 Работа курьером по забору денег

Вам говорят:

«Вакансия — курьер. Нужно приехать по адресу, забрать конверт у клиента, перевести деньги на указанный счёт через терминал, процент оставишь себе»

Реальность:

Вы приезжаете к бабушке, которая только что оформила кредит и отдаёт вам все деньги, потому что ей сказали по телефону, что приедет «курьер из банка». **Вы — звено в цепи мошенников.**

Статья УК РФ:

159 («Мошенничество») или **158** («Кража»). Срок — **до 10 лет лишения свободы.** Если группа организованная (ст. 210) — **до пожизненного.**

04 Установка GSM-шлюзов / оборудования в квартире.

Вам говорят:

«Мы телекоммуникационная компания. Нужно поставить у тебя дома небольшой ящик с антеннами для усиления сигнала. Платим 10 000 в месяц, ничего делать не надо».

Реальность:

Через этот шлюз **мошенники делают тысячи звонков по всей стране. К вам придут с обыском и изымут оборудование.**

Статья УК РФ:

274 Срок — **до 6 лет лишения свободы.**

05 Продажа доступа к Госуслугам

Вам говорят:

«Дай зайти в твой аккаунт на Госуслугах на 5 минут, нам для проверки. Заплатим 1000 руб.»

Реальность:

Через ваш подтверждённый аккаунт оформят микрозаймы в МФО или украдут чью-то недвижимость, и к вам потом придут приставы за этими долгами.

Статья УК РФ:

159 («Мошенничество»), **272** («Неправомерный доступ к компьютерной информации»). Срок — **до 5-7 лет лишения свободы.**

Повышай свой личный уровень противодействия угрозам в сети и становись участником большой команды Школы КиберБезопасности Первых.

Больше киберзнаний, умений, навыков ты найдёшь на сайте

киберволонтеры.будьвдвижении.рф

ПОСЛЕДСТВИЯ

(О чем вам не скажут вербовщики)

- **Судимость навсегда останется в биографии.** Даже если дадут условный срок
- **Невозможность устроиться на хорошую работу**: госслужба, банки, крупные компании, учебные заведения, правоохранительные органы — путь закрыт
- **Ограничения:** нельзя выезжать в некоторые страны, получать опредёленные лицензии
- **Это клеймо на всю семью.** Судимость близкого родственника — всегда негативный фактор при любых проверках

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ВОВЛЕКАЮТ

Алгоритм действий

01 **Прекратить разговор.** Не соглашаться, не спорить, не пытаться переубедить. Просто сказать «нет» и заблокировать контакт

02 **Рассказать родителям или учителю.** Если предложение поступило в интернете от «нового друга» — это вербовка

03 **Сообщить в полицию.** Если вы уже втянулись и испугались, явка с повинной и содействие следствию могут смягчить наказание или освободить от него

Подготовлено при экспертизе МВД России и Минпросвещения России