Приложение 2

Памятка «Щит в онлайн-мире»

Нижний Новгород, 2025 год

Твой цифровой щит: как защититься в онлайн-мире

ишинг: осторожно, мошенники!

Что это? - Попытка выманить твои личные данные (пароли, данные карт) под видом надежного источника (банка, известной компании, госучреждения).

Как защититься?

- **Проверяй отправителя:** внимательно смотри на адрес электронной почты или имя отправителя. Часто мошенники используют похожие, но не идентичные названия;
- **Не переходи по подозрительным ссылкам:** Наведи курсор на ссылку (не нажимая!), чтобы увидеть полный адрес. Если он выглядит странно, не переходи;
- **Не вводи данные на незнакомых сайтах:** никогда не вводи логины, пароли или данные банковских карт, если не уверен в подлинности сайта. Лучше зайди на официальный сайт напрямую;
- **Будь бдителен:** если сообщение вызывает сильные эмоции (страх, жадность, срочность), это повод задуматься.

Основные статьи ответственности: Статья 272 УК РФ (неправомерный доступ к компьютерной информации), статья 159.6 УК РФ (мошенничество в сфере компьютерной информации).

Дипфэйк) и искусственный интеллект: не верь глазам своим!

Что это? Использование нейросетей для создания поддельных видео, аудио или изображений, которые выглядят очень реалистично.

Как защититься?

- **Проверяй признаки подделки:** Неестественная мимика, движения губ, размытые контуры, странные тени;
- **Не вступай в переписку с вымогателями:** если тебе прислали deepfake-видео с угрозами, не паникуй и не переводи деньги;
- **Зафиксируй факт:** Сделай скриншоты сообщений и видео;
- **Обратись за помощью:** Расскажи родителям, учителям или обратись в правоохранительные органы (МВД, Генеральная прокуратура РФ).

Основные статьи ответственности: Статья 137 УК РФ (нарушение неприкосновенности частной жизни), статья 128.1 УК РФ (клевета).

течки данных: Береги свою информацию!

Что это? - Твои личные данные (имя, фамилия, телефон, почта, иногда пароли) попадают в открытый доступ из-за взлома сайтов или сервисов, которыми ты пользуешься.

Как защититься?

- **Используй сложные и уникальные пароли:** для каждого сервиса должен быть свой сложный пароль. Используй комбинации букв, цифр и символов;
- **Включи двухфакторную аутентификацию (2FA):** это дополнительный уровень защиты, когда для входа, помимо пароля, нужен код из СМС или специального приложения;

- **Ограничь объем личной информации:** не делись в интернете лишними данными о себе, своей семье, адресе или планах;
- **Регулярно обновляй ПО:** Обновления часто содержат исправления уязвимостей, которые могут использовать злоумышленники.

Основные статьи ответственности: Статья 5, 6, 7 ФЗ № 152-ФЗ (принципы обработки персональных данных, согласие, конфиденциальность).

ража биометрических данных: Береги своё лицо и голос!

Что это? Незаконный сбор и использование твоих биометрических данных (отпечатки пальцев, изображение лица, голос) для мошенничества или подмены личности.

Как защититься?
- **Не участвуй в подозрительных челленджах:** не записывай видео или аудио для неизвестных приложений, которые просят произнести определённые фразы или показать лицо;
- **Проверяй политику конфиденциальности:** прежде чем дать приложению доступ к камере или микрофону, узнай, как оно будет использовать твои данные;
- **Используй биометрию только в официальных приложениях:** Банковские приложения, «Госуслуги» — это безопасно. Сомнительные приложения — нет.

Основные статьи ответственности: Статья 10 ФЗ № 152-ФЗ (обработка специальных категорий персональных данных), статья 6 и 9 ФЗ № 152-ФЗ (согласие на обработку биометрических данных).

ибербуллинг: не молчи!

Что это? - Травля, оскорбления, угрозы или распространение ложной информации о тебе в интернете.

Как защититься?
- **Не отвечай агрессией:** это только подстегнет обидчика;
- **Сохраняй доказательства:** Делай скриншоты сообщений, комментариев, страниц;
- **Блокируй обидчика:** Ограничь его доступ к своим страницам и информации;
- **Расскажи взрослым:** Обратись за помощью к родителям, учителям или другим доверенным взрослым. Ты не один!
- **Используй настройки приватности:** Ограничь круг лиц, которые могут видеть твои публикации и личную информацию.

Основные статьи ответственности: Статья 5.61 КоАП РФ (оскорбление), статья 137 УК РФ (нарушение неприкосновенности частной жизни), статья 128.1 УК РФ (клевета).

анипуляция информацией: Думай критически!

Что это? Распространение фейковых новостей, искажение фактов, пропаганда с целью повлиять на твое мнение или заставить тебя действовать определенным образом.

Как защититься?

- **Проверяй источники:** Кто опубликовал информацию? Это авторитетное СМИ, эксперт или анонимный пользователь?
- **Ищи подтверждения:** Проверь информацию в нескольких независимых источниках. Если новость важная, о ней напишут многие;
- **Анализируй содержание:** Обращай внимание на заголовки, эмоциональную окраску текста, отсутствие фактов и ссылок на источники;
- **Развивай критическое мышление:** Задавай вопросы: «Кому это выгодно?», «Какова цель этой информации?», «Есть ли другие точки зрения?»;
- **Не делись непроверенной информацией:** прежде чем репостить или отправлять новость, убедись в ее достоверности.

Основные статьи ответственности: Статья 15.3 ФЗ № 149-ФЗ (блокировка недостоверной информации), статья 13.26 КоАП РФ (нарушение порядка распространения информации в сети Интернет).

ифровая зависимость: Контролируй своё время!

Что это? Чрезмерное использование социальных сетей, видеохостингов и игр, которое мешает учёбе, общению с друзьями и здоровью.

Как защититься?

- **Устанавливай лимиты времени:** Используй встроенные функции телефона или приложения для контроля экранного времени.
- **Отключай уведомления:** они постоянно отвлекают и заставляют возвращаться в приложения.
- **Планируй «цифровой детокс»:** Выделяй время, когда ты полностью отключаешься от гаджетов.
- **Занимайся спортом и хобби:** Реальная жизнь гораздо интереснее виртуальной!

Основные статьи ответственности: Статья 16 ФЗ № 149-ФЗ (защита прав пользователей на достоверную информацию).

уда обращаться за помощью?

- **Роскомнадзор:** https://rkn.gov.ru
  о
- **Генеральная прокуратура РФ:** https://epp.genproc.gov.ru
  м
- **МВД России (Киберполиция):** https://мвд.рф, телефон: 102
- **Портал «Госуслуги»:** https://gosuslugi.ru
- **Единый телефон доверия:** 8-800-2000-122 (бесплатно)
  б
  р
  б
  ц

тобы получить «Сертификат Молодого амбассадора

безопасности», используйте QR-код бота, либо получите дополнительную информацию в образовательных каналах:

Чат-бот @pushkin_help_bot	Подписка на канал в MAX	Подписка на канал в Telegram
@pushkin_help_bot	@pushkin_help	
Сообщество в ВК https://vk.com/pushkinhelpai @pushkinhelpai		

ридическая памятка:

Федеральный закон «О персональных данных»/

Этот закон был принят в 2006 году и с тех пор неоднократно обновлялся.

Что такое персональные данные? Это любая информация, которая относится к конкретному человеку: ваше имя, фамилия, дата рождения, адрес, номер телефона, адрес электронной почты, фотографии, даже IP-адрес вашего компьютера. Всё это — ваши персональные данные.

Что регулирует этот закон?

Во-первых, он устанавливает ваши права:

- Право знать, кто и какие ваши данные обрабатывает;
- Право требовать удаления или исправления неверных данных;
- Право отозвать согласие на обработку данных.

Во-вторых, он устанавливает обязанности компаний и организаций:

- Они обязаны получить ваше согласие перед сбором данных
- Они обязаны обеспечить безопасность хранения ваших данных
- Они не могут передавать ваши данные третьим лицам без вашего согласия

Если оператор (компания, организация, госорган):

- Обрабатывает ваши персональные данные без вашего согласия, когда оно требуется по закону;
- Использует ваши данные не для тех целей, о которых заявил изначально;
- Не обеспечивает безопасность ваших данных, что привело к их утечке;
- Не выполняет ваши законные требования: не удаляет, не исправляет или не блокирует ваши данные;
- Не предоставляет вам информацию о том, какие данные он обрабатывает и зачем,

то ему грозит по Федеральному закону № 152-ФЗ «О персональных данных»:

- Административная ответственность по ст. 13.11 КоАП РФ:
- Гражданско-правовая ответственность: вы можете взыскать компенсацию морального вреда и убытков через суд.
- Уголовная ответственность по статьям 137, 272 УК РФ (если нарушение содержит состав преступления).
- Запрет на обработку данных по решению уполномоченного органа (Роскомнадзора).

Важный момент для вас, как для несовершеннолетних: до 14 лет согласие на обработку персональных данных дают ваши родители или законные представители. С 14 до 18 лет вы можете давать согласие сами, но с письменного согласия родителей.

Федеральный закон № ФЗ-149 "Об информации, информационных технологиях и о защите информации".

Это более широкий закон, который регулирует всё, что связано с информацией в цифровом пространстве.

Ключевые положения этого закона:

- Право на достоверную информацию — закон гарантирует, что вы имеете право получать правдивую информацию. Если кто-то распространяет заведомо ложные сведения (фейки), это может быть наказуемо;
- Защита от вредоносной информации — закон запрещает распространение информации, которая:

ризывает к насилию или экстремизму;

одержит детскую порнографию;
ропагандирует наркотики;
одержит инструкции по созданию оружия или взрывчатых веществ

- Ответственность за распространение информации — если вы что-то публикуете в интернете, вы несёте за это ответственность. "Я просто репостнул" или "Я не знал, что это запрещено" — не освобождает от ответственности.

Если кто-то (или организация):

- Распространяет о вас заведомо ложную информацию, которая создает угрозу общественной безопасности или причиняет вред вашим правам;
- Незаконно ограничивает доступ к вашей информации или нарушает установленный порядок ее распространения;
- Н

то ему грозит по Федеральному закону № 149-ФЗ:

- Блокировка сайта/ресурса, распространяющего запрещенную информацию;
- Удаление незаконного контента;
- Административная ответственность по соответствующим статьям КоАП РФ (например, за нарушение порядка распространения информации);
- Гражданско-правовая ответственность — вы можете взыскать компенсацию морального вреда и убытков через суд;
- Уголовная ответственность — если нарушение попадает под действие Уголовного кодекса (например, клевета в интернете).

Важно понимать: этот закон также регулирует работу интернет-сервисов, социальных сетей, мессенджеров. Например, именно на основании этого закона в России блокируются сайты с запрещённым контентом.

<u>Кодекс об административных правонарушениях РФ (КоАП РФ)</u>.

Это более "мягкий" вид ответственности по сравнению с уголовной, но всё равно серьёзный.

Статья 5.61 КоАП РФ — "Оскорбление"

Что это значит? Если кто-то:

- Публично унижает ваши честь и достоинство в грубой, неприличной форме;
- Оскорбляет вас в интернете, социальных сетях или мессенджерах;
- Допускает оскорбительные высказывания в СМИ или публичных произведениях,

то этому человеку или компании грозит штраф:

- Для граждан — от 3 000 до 10 000 рублей;
- Для должностных лиц — от 30 000 до 100 000 рублей;
- Для организаций — от 100 000 до 700 000 рублей и выше.

Важно: это административная, а не уголовная ответственность. Наказание серьезнее, если оскорбление было публичным, особенно в интернете. Отдельно наказываются должностные лица за оскорбления, совершенные в связи с исполнением обязанностей (штраф до 150 000 ₽ или дисквалификация). Соцсети и СМИ обязаны удалять оскорбительный контент, иначе им также грозит штраф.

Статья 13.11 КоАП РФ — "Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)"

Что это значит? Если кто-то:

- Собирает ваши данные без согласия;
- Передаёт их третьим лицам без разрешения;
- Не обеспечивает их безопасность,

то этому человеку или компании грозит штраф:

- Для граждан — от 1 500 до 800 000 рублей;
- Для должностных лиц — от 6 000 до 2 000 000 рублей;
- Для организаций — от 30 000 до 20 000 000 рублей и выше.

Повторные нарушения штрафуются строже!

Статья 13.15 КоАП РФ — "Злоупотребление свободой массовой информации"
Эта статья касается распространения запрещённой информации через интернет. Штрафы здесь уже серьёзнее — от 2 000 до 400 000 рублей для граждан.

Важно для вас: С 16 лет вы уже можете быть привлечены к административной ответственности. До 16 лет ответственность несут ваши родители.

Статья 13.26 ***КоАП РФ*** — "Нарушение сроков и (или) порядка доставки (вручения) адресату судебных извещений", влечет наложение административного штрафа на должностных лиц в размере от 500 до 1000 рублей; на юридических лиц – 5000 до 10000 рублей.

Уголовный кодекс РФ (УК РФ)

Это самое серьёзное — уголовная ответственность. Это уже не штрафы, а реальные последствия, вплоть до лишения свободы. Основные статьи, которые касаются цифровой безопасности:

Статья 128.1 УК РФ — "Клевета"
Распространение заведомо ложных сведений, порочащих честь, достоинство или репутацию другого лица.

Если кто-то:

- Распространяет о вас заведомо ложные сведения, которые порочат вашу честь, достоинство или подрывают репутацию;
- Делает это публично — в речи, в СМИ или в интернете (в соцсетях, мессенджерах);
- Обвиняет вас в совершении тяжкого преступления или преступления против половой неприкосновенности,

то ему грозит:

- Штраф до 5 000 000 рублей;
- Обязательные работы до 480 часов;
- Принудительные работы до 5лет;
- Арест до 6 месяцев;
- Лишение свободы до 5 лет.

Важно: это одна из основных статей для защиты репутации. Наказание напрямую зависит от способа и масштаба распространения лжи, а также от тяжести ложных обвинений. Публикация клеветы в интернете считается отягчающим обстоятельством.

Статья 137 УК РФ — "Нарушение неприкосновенности частной жизни"

Если кто-то:

- Незаконно собирает или распространяет сведения о вашей частной жизни;
- Публикует вашу личную переписку без согласия;
- Распространяет ваши интимные фотографии или видео,

то ему грозит:

- Штраф до 350 000 рублей;
- Обязательные работы до 360 часов;
- Исправительные работы до 1 года;
- Принудительные работы до 4 лет;
- Арест до 6 месяцев;
- Лишение свободы до 5 лет.

Важно: это одна из самых частых статей, по которым привлекают за кибербуллинг и "слив" личной информации.

Статья 159.6 УК РФ — "Мошенничество в сфере компьютерной информации"
Это про кибермошенничество.

Если кто-то:

- Взламывает ваш аккаунт для кражи денег или личных данных;
- Обманным путем получает доступ к вашим электронным кошелькам или банковским счетам;
- Путем фишинга или использования вредоносных программ похищает ваши цифровые активы,

то ему грозит:

- Штраф до 1 000 000 рублей;
- Обязательные работы до 480 часов;
- Исправительные работы до 2 лет;
- Принудительные работы до 5лет;
- Лишение свободы до 10 лет.

Важно: это основная статья для борьбы с кибермошенничеством. Наказание резко ужесточается, если преступление совершено группой лиц, с использованием служебного положения, или если ущерб признан крупным (свыше 1 млн руб.) или особо крупным (свыше 6 млн руб.)

Статья 163 УК РФ — "«Вымогательство» "
Требование передачи чужого имущества (денег) под угрозой распространения сведений, позорящих потерпевшего

Если кто-то:

- Требует у вас деньги, имущество или право на него под угрозой расправы;
- Шантажирует вас, угрожая повредить ваше имущество;
- Угрожает распространить компрометирующие сведения (фото, видео, любую другую информацию), которые могут навредить вашей репутации или интересам,

то ему грозит по статье 163 УК РФ («Вымогательство»):

- Ограничение свободы до 4 лет;
- Принудительные работы до 4 лет;
- Арест до 6 месяцев;
- Лишение свободы до 4 лет.

Важно: Наказание резко ужесточается, если вымогательство совершено:

- Группой лиц по предварительному сговору;
- С применением насилия;
- В крупном размере (свыше 250 тыс. руб.) — лишение свободы до 7 лет.
- Организованной группой, в особо крупном размере (свыше 1 млн руб.) или с причинением тяжкого вреда здоровью — лишение свободы от 7 до 15 лет.

Эта статья часто применяется при борьбе с кибершантажом и требованиями денег под угрозой "слива" личной переписки или фотографий.

Статья 272 УК РФ — "Неправомерный доступ к компьютерной информации"

Если кто-то:
- Взломал ваш аккаунт в социальной сети;
- Получил доступ к вашему компьютеру или телефону без разрешения;
- Украл ваши пароли.

то ему грозит:
- Штраф до 500 000 рублей;
- Исправительные работы до 2 лет;
- Ограничение свободы до 4 лет;
- Принудительные работы до 5 лет;
- Лишение свободы до 7 лет.

Статья 273 УК РФ — "Создание, использование и распространение вредоносных компьютерных программ"

Это про вирусы, трояны, программы-шпионы. Если кто-то создаёт или распространяет такие программы, ему грозит:
- Ограничение свободы до 4 лет;
- Принудительные работы до 5 лет;
- Лишение свободы до 6 лет;
- Дополнительный штраф до 200 000 рублей.

Статья 274.1 УК РФ — "Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации"

Это про серьёзные кибератаки на государственные системы, банки, больницы. Наказание
- Принудительные работы до 5 лет;
- Лишение свободы до 10 лет;
- Дополнительный штраф до 1 000 000 рублей;

Важно для вас: С 14 лет наступает уголовная ответственность за тяжкие преступления (например, по статье 137 УК РФ при отягчающих обстоятельствах). С 16 лет — полная уголовная ответственность по всем статьям.