БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ НАЧИНАЕТСЯ С ТЕБЯ, А ПРОДОЛЖАЕТСЯ С НАМИ!

КИБЕР ВОЛОНТЕРЫ

ДОМ МОЛОДЕЖИ

ГОСУДАРСТВЕННЫЙ КОМИТЕТ МОЛОДЕЖНОЙ ПОЛИТИКИ РЕСПУБЛИКИ КРЫМ

КИБЕР ВОЛОНТЕРЫ

“БЕЗОПАСНОСТЬ ОНЛАЙН – ЭТО КОМАНДНАЯ РАБОТА, ГДЕ КАЖДЫЙ ВАЖЕН!”

ДОМ МОЛОДЕЖИ

вместе с росмолодёжь

КИБЕР ВОЛОНТЕРЫ

ИНТЕРНЕТ СОЗДАН, ЧТОБЫ СОЕДИНЯТЬ, А НЕ РАЗРУШАТЬ

МЫ ЗАЩИЩАЕМ СЕТЬ, КОГДА ЗАЩИЩАЕМ ДРУГ ДРУГА.

БУДЬ ТЕМ, КТО ЧИНИТ, А НЕ ЛОМАЕТ

БЕЗОПАСНОСТЬ МОЛОДЁЖИ В ЦИФРОВОМ ПРОСТРАНСТВЕ

15 июля 2022 г. по поручению Главы Республики Крым С.В. Аксёнова на базе АНО «ДОМ МОЛОДЕЖИ» был открыт отдел Центра мониторинга сети Интернет.

АНО «ДОМ МОЛОДЕЖИ» создана в целях формирования условий для всестороннего развития молодёжи, реализации ее потенциала, вовлечения молодёжи в активную социальную практику, решение актуальных вопросов и проблем молодежи и формирование позитивной гражданской позиции подрастающего поколения.

Центр мониторинга сети Интернет занимается обеспечением безопасности в Интернете и помогает предотвращать опасные и деструктивные явления среди молодёжи. Главная задача — поиск в Интернете деструктивного и противоправного контента, который содержит призывы к насилию, пропаганду наркотиков, суицидальные настроения и другие опасные вещи.

Кроме мониторинга, Центр проводит профилактическую работу: организует психологические консультации, тренинги и образовательные мероприятия для школьников и студентов. Командой специалистов «Дома Молодежи» большое внимание уделяется тому, чтобы молодёжь умела безопасно пользоваться Интернетом и получала полезную и позитивную информацию.

Чтобы связаться с Центром мониторинга сети Интернет и сообщить о деструктивном контенте, необходимо написать на официальную почту: dommolodcrimea@mail.ru

- **Антивирус** – ПО для обнаружения и удаления вредоносных программ.
- **Анонимность** – Возможность скрывать свою личность в сети.
- **Авторизация** – Предоставление прав доступа.
- **Аутентификация** – Проверка подлинности пользователя (пароли, 2FA, биометрия).
- **Блокировка** (в чате или соцсети) – Инструмент, позволяющий ограничить доступ нежелательным пользователям к своему аккаунту или сообщениям.
- **Ботнет** – Сеть зараженных устройств под контролем злоумышленника.
- **Вложения (аттачменты)** – Файлы, прикреплённые к письму или сообщению. Это могут быть документы, картинки, архивы и т.п.
- **Вирус** – Программа, заражающая файлы и распространяющаяся между компьютерами через сеть.
- **DoS/DDoS-атака** – Перегрузка системы запросами.
- **Двухфакторная аутентификация** (2FA) – Способ входа в аккаунт, при котором помимо пароля нужно ввести дополнительный код (например, из SMS или специального приложения).
- **Zero-Day** – Уязвимость, неизвестная разработчикам до начала эксплуатации.
- **HTTPS (защищённый протокол)** – Протокол безопасного соединения между сайтом и пользователем, защищающий данные от перехвата.
- **Информационная безопасность** – Сохранение конфиденциальности, целостности и доступности информации.
- **Инсайдерская угроза** – Риски, исходящие от сотрудников организации.
- **Кибератака** – Целенаправленное вредоносное воздействие на ИТ-системы.
- **Кибербезопасность** – Защита систем, сетей и данных от цифровых атак.

- **Кибербуллинг** – Форма травли, которая происходит онлайн: через комментарии, мессенджеры, соцсети, онлайн-игры.
- **Кибергигиена** – Базовые практики безопасного поведения в сети.
- **MITM-атака** – Перехват данных между отправителем и получателем.
- **Парольная защита** – Использование уникальных и сложных паролей для защиты ваших аккаунтов.
- **Патч** – Обновление для устранения уязвимостей.
- **Penetration Testing** – Тестирование на проникновение для выявления уязвимостей.
- **Рансомвер** – Шифрование данных с требованием выкупа.
- **Руткит** – Вредоносная программа, позволяющая злоумышленнику скрытно управлять устройством.

- **SQL-инъекция** – Внедрение вредоносного кода в базы данных.
- **Скриншот** – Снимок экрана.
- **Социальная инженерия** – Манипуляции с целью получения доступа к конфиденциальной информации.
- **Троян** – Вредоносная программа, маскирующаяся под безопасную.
- **Троллинг** – Поведение в интернете, направленное на провоцирование других пользователей.
- **Утечка данных** – Ситуация, когда личная информация пользователя попадает в руки третьих лиц.
- **Фишинг** – Мошеннические письма или сообщения с целью кражи личных данных.
- **Эксплойт** – Программа или метод, использующий уязвимость.
- **Шифрование** – Преобразование данных в нечитаемый формат без специального ключа.
- **Шпионское ПО** – Программа, которая собирает информацию о пользователе без его ведома.

ЦИФРОВЫЕ ОШИБКИ
с реальными последствиями

1. Кибербуллинг в чате класса

Ситуация: В школьном чате один ученик оскорбляет и травит другого, создаёт оскорбительные мемы и публикует в соцсетях.

Ответственность:

- Статья 5.61 КоАП РФ — оскорбление (административный штраф).
- Если травля систематическая и сопровождается угрозами — уголовная ответственность по статье 119 УК РФ (угроза жизни и здоровью), ст. 128.1 УК РФ (клевета), ст. 137 (нарушение неприкосновенности частной жизни).

2. Создание фейкового профиля учителя

Ситуация: Студент создаёт аккаунт учителя в TikTok и публикует от его имени шутливые или провокационные видео.

Ответственность:

- Статья 137 УК РФ — нарушение неприкосновенности частной жизни.
- Статья 128.1 УК РФ — клевета, если от имени вымышленного профиля публикуются ложные сведения.

3. Переход по фишинговой ссылке на «скидку»

Ситуация: Студент получает ссылку от друга в мессенджере «только сегодня скидка на технику 90%», переходит и вводит данные карты.

Ответственность (для мошенников):

- Статья 159.3 УК РФ — мошенничество с использованием электронных средств платежа. Если сам студент переслал ссылку другим — может быть признан соучастником.

4. Участие в Telegram-боте по «сливам»

Ситуация: Школьник подписан на канал, где анонимно выкладывают интимные фото/видео одноклассников.

Ответственность:

- Статья 242.1 УК РФ — изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних
- Статья 137 УК РФ — нарушение неприкосновенности частной жизни.
- Уголовная ответственность с 16 лет, а в ряде случаев — с 14 лет.

5. Рассылка спама или ссылок на пиратские сайты

Ситуация: Студент публикует ссылки на скачивание взломанных игр, фильмов, ПО.

Ответственность:

- Статья 146 УК РФ — нарушение авторских и смежных прав.
- Статья 13.41 КоАП РФ — распространение запрещённой информации.

6. Создание бота, атакующего школьный сайт (DDoS)

Ситуация: Группа школьников запускает бот-атаку на сайт школы «ради прикола» перед экзаменами.

Ответственность:

- УК РФ Статья 274.1 — неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
- Статья 274.1 УК РФ — создание средств для DDoS-атак.
- Статья 272 УК РФ — вмешательство в работу информационных систем.
- Возможна уголовная ответственность с 16 лет.

7. Использование найденной банковской карты

Ситуация:

Студент находит на улице банковскую карту и решает «попробовать»: покупает еду, переводит деньги себе на счёт.

Ответственность:

- Статья 158 УК РФ — кража (использование чужих средств — это хищение).
- Статья 159.3 УК РФ — мошенничество при безналичных расчетах с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.
- Уголовная ответственность наступает с 14 лет.
- Даже если сумма небольшая, действия квалифицируются как умышленное преступление.

8. «Дай карту – переведу тебе деньги»

Ситуация:

Школьник даёт свою банковскую карту однокласснику, чтобы тот «перевёл деньги за игру». Позже оказывается, что карта использовалась для получения денег от мошеннической схемы. Банк блокирует счёт, а владелец карты вызывается в полицию как участник.

Что нарушено:

- Даже если подросток не знал о преступлении, передача карты третьим лицам противоречит условиям банка.
- В случае выявления схемы — возможна уголовная ответственность за соучастие в мошенничестве (ст. 159 УК РФ) или отмывание доходов, полученных преступным путём (ст. 174 УК РФ).
- Ответственность может наступить с 14 лет.

9. Продажа реквизитов карты «для заработка»

Ситуация:

Студент размещает объявление в Telegram: «Продам реквизиты карты для переводов». Незнакомец покупает данные и использует их в мошеннических операциях. Студента вызывают на допрос.

Что нарушено:

- Продажа или передача реквизитов банковской карты может быть квалифицирована как:
- Ст. 187 УК РФ — незаконный оборот платёжных средств и данных (до 6 лет лишения свободы);
- Ст. 159.3 УК РФ — участие в мошеннических схемах;
- Также может быть наложен штраф до 1 млн рублей.
- Даже если студент «ничего не делал сам», участие в схеме считается осознанным содействием преступлению.

10. «Ты же просто репостишь – ничего страшного?»

Ситуация:

Старшеклассник подписан на анонимный Telegram-канал, где регулярно публикуют «острую правду» о власти и «справедливое сопротивление». Он делает репост записи, в которой содержатся призывы к насильственным действиям, а также видео с инструкциями по изготовлению запрещенных веществ и предметов для участия в несанкционированных акциях.

Через некоторое время на его аккаунт выходит полиция — пост зафиксирован системой мониторинга экстремистского контента.

Даже если ты не создавал материал, а просто репостнул, лайкнул или переслал другу — это уже может быть квалифицировано как распространение запрещённой информации.

Российское законодательство признаёт интернет-активность (в том числе в соцсетях) юридически значимой.

Что нарушено:

- Статья 205.2 УК РФ — публичные призывы к осуществлению террористической деятельности, а также оправдание терроризма:
  - ответственность с 14 лет;
  - до 7 лет лишения свободы.
- Статья 280 УК РФ — публичные призывы к экстремистской деятельности:
  - ответственность с 16 лет;
  - штраф, арест или лишение свободы (до 5 лет).
- Статья 282 УК РФ — возбуждение ненависти по политическим, национальным, религиозным признакам:
  - за репост, мем, комментарий — уже были реальные уголовные дела.

11. « «Юмористический контент о взрывах – это же шутка?»

Ситуация:

Студент выкладывает в социальные сети юмористическое изображение здания с подписью «Было бы красиво, если бы оно взлетело...», сопровождая это шуточным комментарием. Шутка быстро разлетается, на него жалуются пользователи. Публикацией интересуется полиция.

Что нарушено:

- Статья 207.3 УК РФ — публичное распространение заведомо ложной информации об актах терроризма:
  - даже «шутки» могут быть квалифицированы как создание паники или оправдание насилия.
  - до 5 лет лишения свободы.
- Статья 205.2 УК РФ — оправдание терроризма (если шутка восхваляет или одобряет насилие):
  - ответственность с 14 лет;
  - штраф до 1 млн рублей или тюремное заключение.

Комментарий: Формат шутки не освобождает от ответственности. Шутка может быть воспринята как реальный призыв или угроза, особенно в контексте тревожной обстановки.

12. «Вступил в "тайную группу" в чате»

Ситуация:

Студент случайно попал в закрытую группу в Discord, где участники обсуждают подготовку «акций возмездия». Он не участвует активно, но читает обсуждения, иногда ставит лайки, не сообщая об увиденном.

Что нарушено:

- Статья 205.3 УК РФ — незамедлительное неуведомление о готовящемся террористическом акте.
- Статья 282 УК РФ — если группа распространяет экстремистскую идеологию, а участник её поддерживает (даже молча).
- Статья 205.3 УК РФ — прохождение обучения в целях осуществления террористической деятельности
- Наказание: от 100.000 р. штрафа до 1 года лишения свободы.

13. Собирал донаты «на борьбу с системой»

Ситуация:

Подросток создаёт анонимный кошелёк и размещает QR-код в соцсетях со словами «на сопротивление» и «на движение за правду». На деле средства переводятся в запрещённую экстремистскую организацию.

Что нарушено:

- Статья 205.1 УК РФ — содействие террористической деятельности, финансирование.
- Статья 282.3 УК РФ — финансирование экстремисткой деятельности.
- Наказание: от 5 до 15 лет лишения свободы.

14. «Решил поспорить в комментариях»

Ситуация:

Школьник активно пишет под политическими постами в соцсетях, призывая к «жесткому действию«, «отправить чиновников на нары», «снести систему» и т.п. Своё поведение считает «высказыванием мнения» и «игрой на публику».

Что нарушено:

- Статья 280 УК РФ — публичные призывы к экстремизму.
- Статья 282 УК РФ — если есть признаки возбуждения социальной/политической вражды.
- Статья 20.29 КоАП РФ — производство и распространение экстремистских материалов (если делится ссылками на запрещённые ресурсы).
- Наказание: от административного штрафа до 5 лет лишения свободы — в зависимости от тяжести и повторности.

15. «Нарисовал граффити по просьбе “старшего”»

Ситуация:

Студент-художник по просьбе «куратора» из интернета рисует на стене здания странный символ и QR-код, ведущий на Telegram-канал. Он не проверял, что это за ресурс. Позже выясняется — это закрытое сообщество с террористической идеологией.

Что нарушено:

- Статья 205.2 УК РФ — участие в распространении террористической пропаганды.
- Статья 214 УК РФ — вандализм — повреждение или осквернение зданий, памятников и пр.
- Статья 282 УК РФ — возбуждение ненависти или вражды, если рисунок содержит экстремистские символы.
- Наказание: штраф, обязательные работы, лишение свободы до 7 лет.

16. «Сделал TikTok с оружием и странной музыкой»

Ситуация:

Школьник публикует видео, на котором он держит предмет, похожий на оружие (например, страйкбольный автомат), на фоне песни с текстом про «отмщение». В описании фраза: «Ждите, скоро всё изменится».

Что нарушено:

- Статья 207.3 УК РФ — распространение ложной информации о теракте, если это расценено как угроза.
- Статья 205.2 УК РФ — оправдание терроризма (если в тексте видео/музыке есть явные отсылки).
- Статья 20.3 КоАП РФ — пропаганда экстремизма — за использование символики или намёков.

1. Осторожно с сообщениями и письмами

Никогда не открывай подозрительные письма, ссылки и вложения от незнакомцев. Если письмо выглядит странно, лучше его удалить. Обращай внимание на адрес отправителя — иногда мошенники маскируются под знакомые организации.

2. Придумывай сложные и разные пароли

Используй длинные и уникальные пароли для каждого сайта. Не используй одинаковые пароли для соцсетей, почты и интернет-магазинов. Лучше всего, если пароль будет состоять из букв, цифр и символов.

3. Включи двухфакторную аутентификацию (2FA)

Это дополнительная защита аккаунтов. Даже если кто-то узнает твой пароль, он не сможет войти без второго кода, который приходит по SMS или в специальное приложение. Это сильно снижает риск взлома.

4. Обновляй приложения и антивирус

Регулярно устанавливай обновления для телефона, компьютера и приложений. Обновления часто закрывают уязвимости, которыми могут воспользоваться злоумышленники. Антивирус помогает заранее обнаружить вредоносные программы.

5. Осторожно с общественным Wi-Fi.

Не заходи в личные аккаунты (например, банк или соцсети) через бесплатные Wi-Fi в кафе, транспорте или торговых центрах.Твоя безопасность в интернете — в твоих руках.

6. Проверяй любую «выгодную» информацию

Если тебе обещают лёгкие деньги, подарки, подработку с большой оплатой — не верь на слово. Всегда проверяй, кто это предлагает. Настоящие работодатели не просят переводить деньги или сразу присылать паспорт.

7. Рассказывай другим, как защититься

Поделись этими советами с друзьями, родными и одноклассниками. Чем больше людей знают об интернет-угрозах, тем труднее обмануть. Это особенно важно для младших школьников и пожилых родственников.

8. Следи за операциями по банковской карте

Иногда проверяй выписку по карте. Если заметил незнакомую операцию — сразу сообщи в банк и родителям. Чем быстрее среагируешь, тем легче вернуть деньги и заблокировать мошенников.

9. Устанавливай антивирус, проводи проверки

Даже бесплатный антивирус может предотвратить заражение вирусами. Периодически запускай полную проверку устройства, особенно если оно стало тормозить или вести себя странно.

10. Не делись личной информацией в сети

Не публикуй в открытом доступе свои личные данные: адрес, номер телефона, паспорт, фото документов и банковской карты. Эти данные могут использовать мошенники, даже если ты просто хотел показать друзьям, как получил водительские права или карту банка.

11. Не показывай экран посторонним

Старайся не демонстрировать экран своего телефона или компьютера незнакомым людям. Особенно если у тебя открыты личные переписки, банковские приложения или важные документы. Будь осторожен даже при видеозвонках или онлайн-уроках — убедись, что на экране нет лишней информации.

Чтобы связаться

с Центром мониторинга и сообщить о деструктивном контенте, необходимо написать на официальную почту: dommolodcrimea@mail.ru