

КТО МЫ?

Мы правопросветительский студенческий проект Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации.



С какой целью создано «КИБЕРЪОКО»?

Наша цель: снижение уровня киберпреступности в Приморском крае, правовое информирование населения о методах защиты от киберпреступлений и правилах безопасного поведения в сети Интернет, а также содействие развитию информационного общества.

Задачи «КИБЕРЪОКО»

1. Анализ и мониторинг киберпреступности как в Дальневосточном Федеральном округе, так и в Российской Федерации, а также выявление новых видов киберугроз и кибератак.
2. Сотрудничество с правоохранительными органами, экспертами в области информационной безопасности и другими организациями для противодействия киберпреступлениям.
3. Обучение и повышение осведомленности населения о методах защиты от киберпреступлений и правилах безопасного поведения в сети Интернет.
4. Создание и поддержка информационных ресурсов и образовательных программ по кибербезопасности.

Присоединяйтесь к нам, чтобы быть в курсе последних новостей, советов и рекомендаций по безопасности в интернете.



@CYBEROKO



Для слепых и
слабовидящих

УЧАСТНИКИ ПРОЕКТА



© Выполнено представителями «КиберЪОко» под научным руководством: Сыромля Ларисы Борисовны - заведующего кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, советника юстиции, кандидата юридических наук

ПАРТНЕРЫ ПРОЕКТА



КИБЕР
ОКО
ПОДКЛЮЧЕНИЕ
ЗАЩИЩЕНО

ДАЛЬНЕВОСТОЧНЫЙ
ЦЕНТР
ПРОФИЛАКТИКИ
КИБЕРПРЕСТУПНОСТИ

Ознакомьтесь с наиболее распространенными схемами вовлечения в террористическую деятельность!



ЗАДАНИЕ ЗА ВОЗНАГРАЖДЕНИЕ

Ищешь легкий заработок? Мы предлагаем несложные задания за очень щедрое вознаграждение! Подожди вертолет по следующим координатам и получи 5 000 000 рублей!



Отвечая на подобные сообщения, имейте в виду, что такое действие может быть квалифицировано как диверсия (ст. 281 УК РФ), за совершение которой предусмотрено наказание в виде лишения свободы на срок до 20 лет.

ПОМОГИ ПОЙМАТЬ ПРЕСТУПНИКА



Здравствуйте! Я сотрудник ФСБ. Мы узнали, что Ваши близкие в опасности. Для их спасения Вам необходимо создать дымовую завесу путем поджога здания по адресу...

Немедленно прекратите переписку! Сотрудники ФСБ никогда не будут связываться с вами в мессенджере и предлагать совершать противоправные действия.

РЕЛЕЙНЫЕ ШКАФЫ

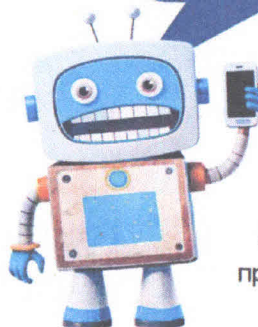
Привет! Сразу к делу! Видел «железные ящики» около железной дороги? Твоя задача - поджечь такой «ящик», а мы переведем за это 20 000 рублей.



Такие «ящики» называются релейными шкафами, которые предназначены для обеспечения безопасного движения поездов. Поджог релейного шкафа представляет угрозу для персонала и пассажиров поездов, идущих мимо.

СТРАННЫЕ СООБЩЕНИЯ

Здравствуй, Для тебя есть ЗаДание. Ты Должен Заминировать ЗДание. 100 000 рублей сразу, потом ещё 700 000. После минирования тебя Заберет наш человек и отвезет в безопасное место. Позже скинем тебе план Действий.



Если неизвестный номер заменяет некоторые буквы похожими на них символами, то он пытается скрыть свои сообщения от автоматических проверок системы безопасности. Это самый заметный признак мошенника!

ПОМОГИ ДОСТАВИТЬ ПОСЫЛКУ

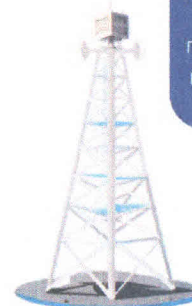
Привет! Нужна помощь! Ничего криминального. Просто перевезти рюкзак в указанное место. Чтобы мы могли убедиться в его доставке, ведй прямую трансляцию в телеграм-канале. Ты не представляешь, как поможешь нам!



Мошенники способны найти подход к любому человеку, поэтому никогда не отвечайте на подобные сообщения!

Задайте себе вопрос: «Что связывает меня с этим человеком?». Ни в коем случае не принимайте посылку! В ней может содержаться взрывное устройство, которое способно сдетонировать прямо у вас в машине или на указанном адресе.

У НАС ЕСТЬ СВЯЗИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ



Доброго дня. Вы подписаны на телеграм-канал города N. Совершите поджог в городе, а мы заплатим. У нас есть связи в правоохранительных органах – если Вас поймают, они помогут.

Прекратите переписку! Это прямой призыв к совершению теракта. Создатели таких сообщений никак не связаны с правоохранительными органами, поэтому они не повлияют на ваше освобождение. Вас просто используют в своих целях!

ВЫ ПОДОЗРЕВАЕТЕСЬ В СОВЕРШЕНИИ ПРЕСТУПЛЕНИЯ

С Вами разговаривает сотрудник Следственного комитета РФ. Вы подозреваетесь в помощи террористам. Если не будете сотрудничать с нами, Вас ожидает наказание в виде лишения свободы.



С вами разговаривает мошенник! Запомните, сотрудники правоохранительных органов не звонят своим подозреваемым и не угрожают им.

МЫ ЗНАЕМ О ТЕБЕ ВСЕ

Привет! Нужно заложить бомбу в торговом центре. Награда - 5000\$. Мы знаем, где живут твои близкие, поэтому, если откажешься, они могут пострадать.



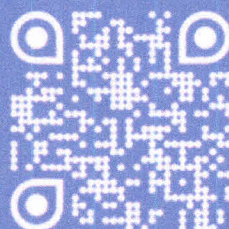
Подстрекатели, как правило, находятся за пределами нашей страны, поэтому их слова – просто угроза. Заблокируйте номер и сообщите об этом инциденте правоохранительным органам.

«Знание —
лучшая защита!»

ДАЛЬНЕВОСТОЧНЫЙ ЦЕНТР ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ КИБЕРЪОКО

КИБЕРМОШЕННИЧЕСТВО КАК ЗАЩИТИТЬ СЕБЯ И СВОИХ ДЕТЕЙ?

© Выполнено представителями
"КиберЪОко" под научным
руководством: Сыромля Ларисы
Борисовны - заведующего кафедрой
прокурорского надзора за
исполнением законов в оперативно-
розыскной деятельности и участия
прокурора в уголовном
судопроизводстве Дальневосточного
юридического института (филиала)
Университета прокуратуры
Российской Федерации, советника
юстиции, кандидата юридических наук



Подписывайся, ведь с нами ты
будешь в безопасности!

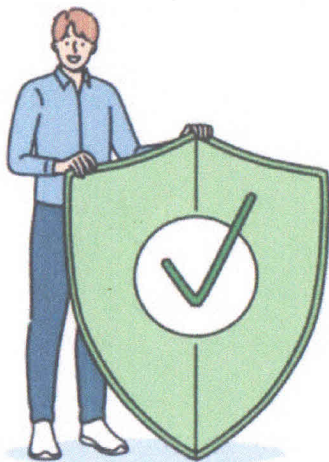
Версия для
слепых и
слабовидящих



КУДА ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ?

- Родители или учителя —
первые, кому можно рассказать
о проблеме;
- Полиция — 02 — если вы стали
жертвой мошенничества либо
единый номер экстренной
помощи — 102;
- Телефон доверия —
8 800 2000 122 — в случае,
если тебе нужно с кем-то
поделиться случившимся или
ты нуждаешься в поддержке.

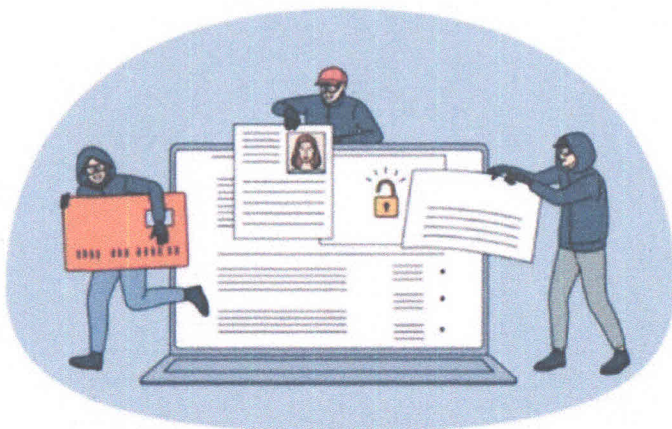
СОБЛЮДАЙТЕ ПРОСТЫЕ ПРАВИЛА ДЛЯ СОХРАНЕНИЯ СВОЕЙ БЕЗОПАСНОСТИ В СЕТИ!



© Выполнено представителями
"КиберЪОко" под научным
руководством: Сыромля Ларисы
Борисовны - заведующего кафедрой
прокурорского надзора за
исполнением законов в оперативно-
розыскной деятельности и участия
прокурора в уголовном
судопроизводстве Дальневосточного
юридического института (филиала)
Университета прокуратуры Российской
Федерации, советника юстиции,
кандидата юридических наук

НЕ ПРЕНЕБРЕГАЙТЕ
ПРОГРАМНО-ТЕХНИЧЕСКИМИ
СПОСОБАМИ ЗАЩИТЫ ИНФОРМАЦИИ:

- ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ;
- ИСПОЛЬЗУЙТЕ АНТИВИРУСНЫЕ ПРОГРАММЫ;
- ИСПОЛЬЗУЙТЕ БРЕНДМАУЭРЫ ПРИ ВЫХОДЕ В ИНТЕРНЕТ.



ПРИСОЕДИНЯЙТЕСЬ К НАМ И
УЗНАВАЙТЕ ПЕРВЫМИ О НОВЫХ
СПОСОБАХ ЗАЩИТЫ В СЕТИ!



ПРАВООСВЕТИТЕЛЬСКИЙ БУКЛЕТ ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

КИБЕР
ОКО
ПОДКЛЮЧЕНИЕ
ЗАЩИЩЕНО



Для слепых и
слабовидящих

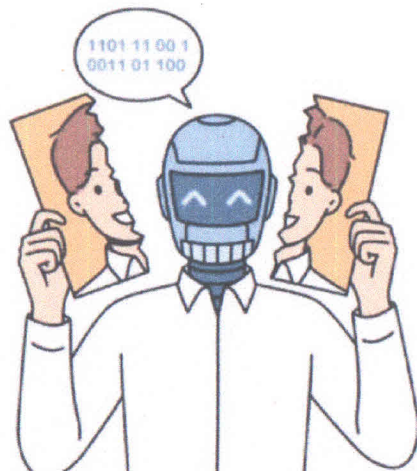
КИБЕРЭКСТРЕМИЗМ



ПРЕСТУПНИКИ ИСПОЛЬЗУЮТ ИНТЕРНЕТ ДЛЯ ПРОДВИЖЕНИЯ КИБЕРЭКСТРЕМИЗМА.

ИЗБЕГАЙТЕ УЧАСТИЯ В ГРУППАХ, ГДЕ:

- ДЕМОНИСТРИРУЕТСЯ ЗАПРЕЩЕННАЯ СИМВОЛИКА;
- ПУБЛИКУЮТСЯ И ОПРАВДЫВАЮТСЯ АКТЫ НАСИЛИЯ;
- НЕГАТИВНО ОЦЕНИВАЕТСЯ КАКАЯ-ЛИБО СОЦИАЛЬНАЯ ГРУППА.



КИБЕР-ТОРГОВЛЯ НАРКОТИКАМИ

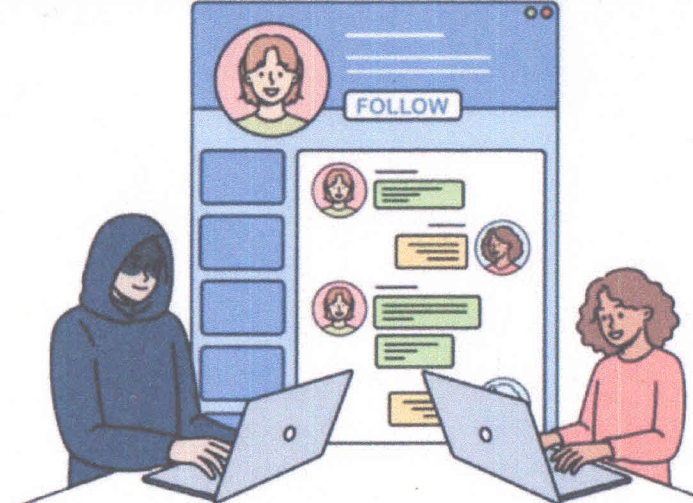
ПРЕСТУПНИКИ ИСПОЛЬЗУЮТ СОЦИАЛЬНЫЕ СЕТИ ДЛЯ ПРОДАЖИ НАРКОТИКОВ И ВЕРБОВКИ “ЗАКЛАДЧИКОВ”. НЕ СОГЛАШАЙТЕСЬ НА ПОДОЗРИТЕЛЬНУЮ “РАБОТУ”.

**ОНИ ЖЕЛАЮТ ИСПОЛЬЗОВАТЬ ВАС
КАК ИНСТРУМЕНТ, САМИ ПРИ ЭТОМ
ОСТАЮТСЯ В ТЕНИ!**



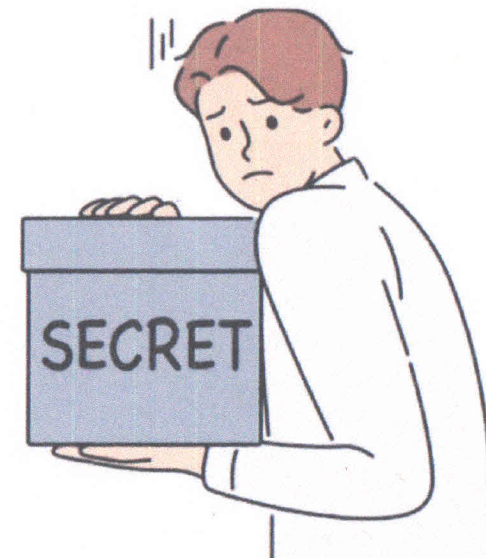
ЗА РАСПРОСТРАНЕНИЕ НАРКОТИКОВ ПРЕДУСМОТРЕНО НАКАЗАНИЕ ВПЛОТЬ ДО ПОЖИЗНЕННОГО ЛИШЕНИЯ СВОБОДЫ.

**ЛЕГКИЕ ДЕНЬГИ - ТЯЖЕЛЫЕ
ПОСЛЕДСТВИЯ!**



НЕ ВЫКЛАДЫВАЙТЕ В ОТКРЫТЫЕ СЕТИ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ О СЕБЕ И СВОЕЙ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ!

**МОШЕННИКИ МОГУТ
ИСПОЛЬЗОВАТЬ ЭТИ СВЕДЕНИЯ В
СВОИХ ЦЕЛЯХ!**



СТ "СКЛОНЕН ЛИ ТЫ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИЧЕСТВА"?

• Как часто ты используешь одинаковые пароли для разных аккаунтов?

- а) Никогда
- б) Иногда
- в) Часто

• Делишься ли ты личной информацией (например, адресом, номером телефона) в социальных сетях?

- а) Никогда
- б) Иногда
- в) Часто

• Проверяешь ли ты ссылки, прежде чем на них кликнуть?

- а) Всегда
- б) Иногда
- в) Никогда

• Используешь ли ты двухфакторную аутентификацию для своих аккаунтов?

- а) Да, всегда
- б) Иногда
- в) Нет, никогда

• Насколько сильно ты беспокоишься о безопасности своих данных в интернете?

- а) Очень беспокоюсь
- б) Иногда беспокоюсь
- в) Совсем не беспокоюсь

РЕЗУЛЬТАТЫ

Больше ответов «а»: Ты достаточно осторожен в интернете и принимаешь меры для защиты своих данных.

Больше ответов «б»: У тебя есть некоторые привычки, которые могут подвергнуть тебя риску. обрати внимание на безопасность своих аккаунтов.

Больше ответов «в»: Тебе стоит серьезно задуматься о своей безопасности в интернете и изменить некоторые привычки.

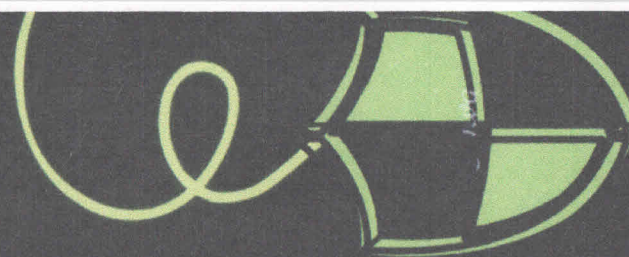
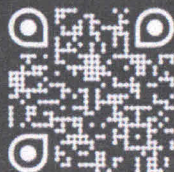
БУДЬ В ТЕМЕ, ЧТОБ НЕ ПОПАСТЬ В РУКИ КИБЕРМОШЕННИКОВ!

© Выполнено представителями "КиберЪОко" под научным руководством: Сыромля Ларисы Борисовны - заведующего кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, советника юстиции, кандидата юридических наук

5 минут в день и ты узнаешь:

- как не стать жертвой кибермошенничества;
- что делать, если ты или твои знакомые попались «в руки» злодея;
- какие еще опасности ожидают нас в цифровом пространстве и многое другое.

Для слепых и слабовидящих



**СТОП
КИБЕРМОШЕННИЧЕСТВУ**

Безопасность детей
в цифровом мире

ЧТО ТАКОЕ КИБЕРМОШЕННИЧЕСТВО?

«Это не игра. Это реальная угроза»



Фейковые «бесплатные» игры или подарки.

Поддельные конкурсы и опросы.

Мошенничество через стримы и стримеров.

Угрозы с требованиями денег или действий.

ПРИМЕР

Пишет одноклассница: «Привет, это Маша! Мой аккаунт в ВКонтакте взломали, можешь, пожалуйста, помочь мне и сообщить код, который придет на твой телефон».

5 ПРАВИЛ ЗАЩИТЫ



ПАРОЛЬ-МОНСТР

Используй буквы, цифры и символы.
Пример: «БЕЗопасно24!»



НЕ КЛИКАЙ НА СТРАННОЕ

Ссылки от незнакомцев
= вирусы.



АНОНИМНОСТЬ

Не указывай школу, адрес, график занятий.

БЛОКИРУЙ АГРЕССОРОВ

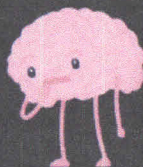
Не бойся жаловаться в поддержку соцсети.



«Защищён тот, кто осведомлён!»

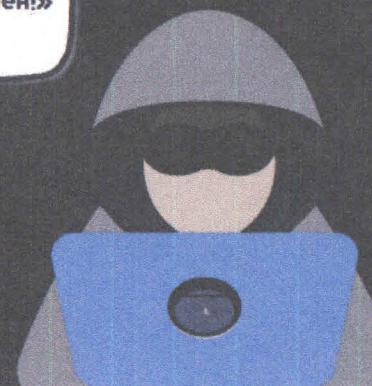
ДУМАЙ

Если что-то кажется подозрительным – так и есть!



ЧТО ДЕЛАТЬ, ЕСЛИ ПОПАЛ В БЕДУ?

1. Не паникуй и не удаляй переписку.
2. Сделай скриншот – это доказательство.
3. Расскажи взрослым: Родители, учитель, психолог.
4. Позвони:
 - В полицию по номеру 02 (сам или через родителей);
 - В горячую линию «Дети России» по номеру 8-800-2000-122 (круглосуточно анонимно).



Кибермошенничество – обман с использованием компьютерных и интернет-технологий.

Цель кибермошенничества: хищение чужого имущества и конфиденциальных (секретных) данных, обман и злоупотребление доверием пользователей.

Правила безопасного поведения в сети «Интернет»:

1. Не разглашай личную информацию. Не стоит сообщать в интернете своё настоящее имя, адрес проживания, контактные данные, рассказывать о своих знакомых, друзьях и одноклассниках.
2. Периодически меняй пароли. Это позволит обезопасить себя от кражи личной информации и иных проблем в сфере кибербезопасности.
3. Не открывай файлы, присланные от неизвестных людей. Такие файлы могут содержать вирусы или фото/видео с нежелательным содержанием.
4. Игнорируй подозрительные письма и сообщения от незнакомцев, не переходи по ссылкам, обещающим бесплатные подарки.
5. Сообщай о проблемах. Если кто-то ведет себя неправильно или угрожает, расскажи об этом родителям или учителям.

Авторы: Пендюр Марина Сергеевна,
Пяткин Никита Сергеевич

АКТУАЛЬНЫЕ СХЕМЫ МОШЕННИЧЕСТВА, НАПРАВЛЕННЫЕ НА НЕСОВЕРШЕННОЛЕТНИХ:

«Здравствуй! Это твоя учительница, Мария Ивановна. Твоя мама должна была сообщить мне код, который пришёл ей в SMS-сообщении. Сообщи мне его срочно. Без него я не могу поставить тебе оценки в электронный журнал».



Ни в коем случае не
говори код!
Отключись и расскажи
о звонке родителям.

«Ищем молодых ребят для лёгкой работы. Оплата 2000 руб./час. Если ты молодой, умеешь пользоваться компьютером и тебе нужно подзаработать, то переходи по ссылке и сразу же получай аванс вместе с первым заданием».

Никогда не переходи по
неизвестным ссылкам!

Мошенники могут
использовать их для кражи
твоих конфиденциальных
данных, денежных средств
или для заражения твоего
устройства вирусом.

Для слепых и
слабовидящих



© Выполнено представителями «КиберЪОко»
под научным руководством: Сыромля Ларисы
Борисовны - заведующего кафедрой
прокурорского надзора за исполнением
законов в оперативно-розыскной
деятельности и участия прокурора в
уголовном судопроизводстве
Дальневосточного юридического института
(филиала) Университета прокуратуры
Российской Федерации, советника юстиции,
кандидата юридических наук



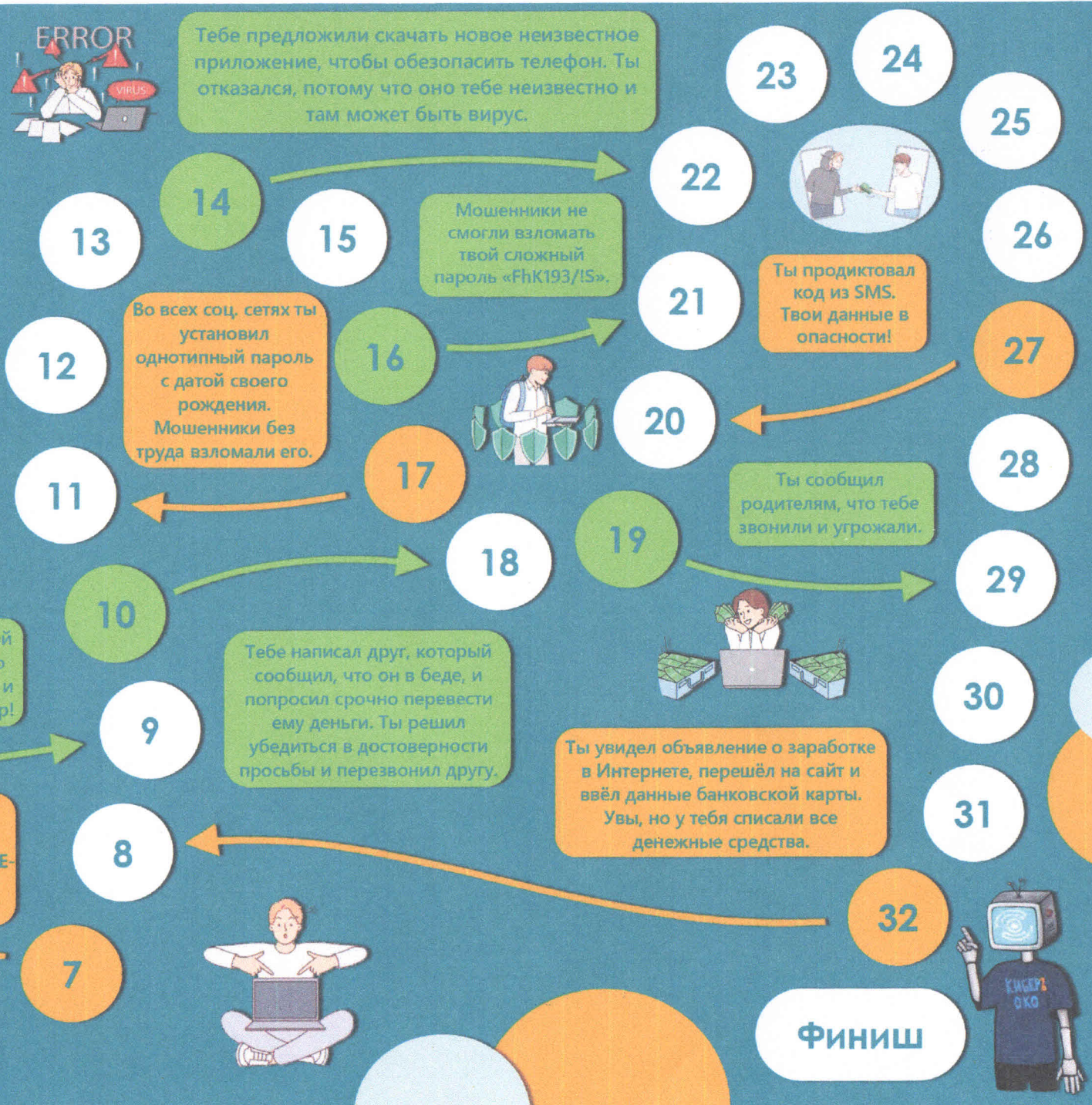
ЗАЩИТА
НЕСОВЕРШЕННОЛЕТНИХ ОТ
КИБЕРМОШЕННИЧЕСТВА:
КРЕАТИВНЫЙ ПОДХОД

Дорогие друзья, мы предлагаем вам сыграть в увлекательную игру! Вам необходимо помочь Диме как можно скорее прийти до дома.

ПРАВИЛА ИГРЫ:

Вам понадобятся 1 игровой кубик и фишки по количеству игроков.

Игроки ходят по очереди. В свой ход игрок бросает кубик и переставляет свою фишку вперёд ровно на столько шагов, сколько выпало очков на кубике. Если игрок попал на цветное поле, то ему необходимо перейти по стрелке.

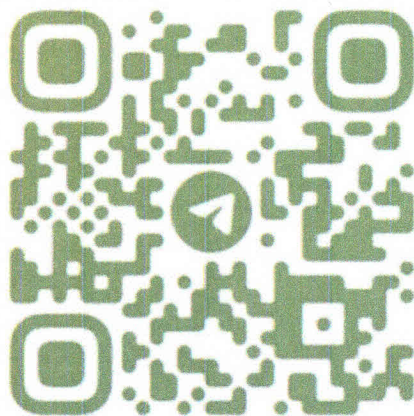


Что такое нелегальный оборот оружия?

Это любая деятельность, связанная с незаконной покупкой, продажей, передачей, хранением или изготовлением оружия. В интернете это может проявляться в виде объявлений на форумах, в даркнете, мессенджерах и социальных сетях.



Для слепых и
слабовидящих



Интернет – это мощный инструмент, предоставляющий доступ к огромному количеству информации и возможностей. Однако, как и любой инструмент, он может быть использован во вред, в том числе для нелегального оборота оружия.

Для несовершеннолетних это представляет особую опасность, поскольку они более уязвимы и могут легче стать жертвами мошенников или преступников.



© Выполнено представителями "КиберОко" под научным руководством: Сыромля Ларисы Борисовны - заведующего кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, советника юстиции, кандидата юридических наук

Противодействие
**Нелегальному
обороту оружия**



Как защитить себя?

Никогда не интересуйтесь оружием в интернете: Не посещайте сайты и форумы, посвященные оружию. Не ищите информацию о его приобретении или изготовлении.

Не общайтесь с людьми, предлагающими оружие: Если вам предлагают купить или получить оружие, немедленно прекратите общение и сообщите об этом взрослым или в правоохранительные органы.

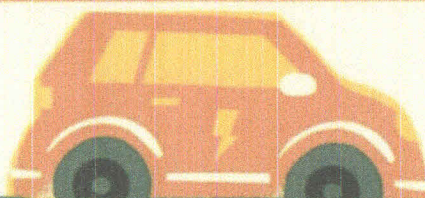
Будьте критичны к информации в интернете: Не верьте всему, что видите и читаете. Проверяйте информацию из разных источников.

Поговорите с родителями или другими доверенными взрослыми: Если у вас возникли вопросы или сомнения, связанные с оружием, обратитесь за помощью к взрослым.



Запомните: Владение оружием – это большая ответственность. Не подвергайте себя и окружающих опасности.

Почему это опасно?



*** Уголовная ответственность:** Даже простое хранение незаконно приобретенного оружия влечет за собой серьезные последствия, вплоть до лишения свободы. Не думайте, что закон вас не коснется, потому что вы несовершеннолетний.

*** Риск для жизни и здоровья:** Оружие в руках неопытного человека – это огромная опасность. Неосторожное обращение может привести к трагическим последствиям.

*** Участие в преступной деятельности:** Вас могут вовлечь в незаконные группировки или использовать для совершения преступлений.

*** Мошенничество:** Вы можете стать жертвой мошенников, которые возьмут деньги за оружие, но ничего не пришлют или пришлют не то, что обещали.

*** Психологическая травма:** Столкновение с миром насилия и преступности может оставить глубокий психологический след.

Куда обратиться за помощью?

Родители или другие доверенные взрослые

Полиция

102 (с мобильного) или 02 (со стационарного)

Телефон доверия для детей и подростков

8-800-2000-122



Кто мы?

Мы - правопросветительский студенческий проект Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, направленный на информирование граждан о методах защиты от киберпреступлений и правилах безопасного поведения в интернете!



С какой целью создано «КИБЕРЪОКО»?

Наша цель - снижение уровня киберпреступности в регионе, правовое информирование населения, защита прав и интересов граждан и организаций от киберпреступлений, а также содействие развитию информационного общества.

Задачи «КиберЪОко»:

1. Анализ и мониторинг киберпреступности как в Дальневосточном федеральном округе, так и в Российской Федерации, а также выявление новых видов киберугроз и кибератак.
2. Сотрудничество с правоохранительными органами, экспертами в области информационной безопасности и другими организациями для противодействия киберпреступлениям.
3. Обучение и повышение осведомлённости населения о методах защиты от киберпреступлений и правилах безопасного поведения в сети Интернет.
4. Создание и поддержка информационных ресурсов и образовательных программ по кибербезопасности.

Присоединяйтесь к нам, чтобы быть в курсе последних новостей, советов и рекомендаций по безопасности в интернете.



@CYBEROKO



Для слепых и слабовидящих

УЧАСТНИКИ ПРОЕКТА



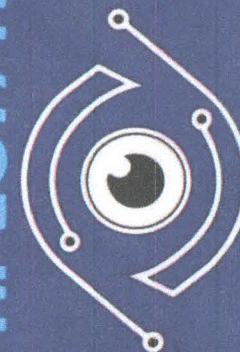
© Выполнено представителями "КиберЪОко" под научным руководством: Сыромля Ларисы Борисовны - заведующего кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, советника юстиции, кандидата юридических наук

ПАРТНЕРЫ ПРОЕКТА



КИБЕР
ОКО
ПОДКЛЮЧЕНИЕ
ЗАЩИЩЕНО

ДАЛЬНЕВОСТОЧНЫЙ
ЦЕНТР
ПРОФИЛАКТИКИ
КИБЕРПРЕСТУПНОСТИ



Ознакомьтесь с наиболее распространенными схемами мошенничества!



ЗВОНОК ИЗ ТЕХПОДДЕРЖКИ

Алло, это техподдержка, действие вашего номера телефона заканчивается, продиктуйте код из СМС, чтобы продлить договор, иначе вы не сможете пользоваться мобильной связью!



! Немедленно положите трубку, ведь это мошенники !
Чтобы обезопасить себя, установите "Анти-спам" или скачайте антивирус.

ВЫ СТАЛИ ПОБЕДИТЕЛЕМ КОНКУРСА!



Поздравляем! Вы стали победителем нашего розыгрыша одного миллиона рублей! Перейдите по ссылке и получите свой заветный приз!

! Задумайтесь, принимали ли вы участие в каком-либо конкурсе? Если нет - прекратите переписку и не переходите по неизвестным ссылкам !

ПРОСРОЧКА ПО ИПОТЕЧНОМУ КРЕДИТУ

Вы просрочили платеж по ипотеке! Срочно переведите денежные средства по новым реквизитам оплаты чтобы избежать штрафа!



! Проверьте информацию о просрочке платежа в приложении банка или по официальному номеру банка. Не спешите переводить средства по новым реквизитам, обо всех изменениях уточняйте информацию в банке !

ЕСЛИ ВЫ ОКАЗАЛИСЬ В ТАКОЙ ИЛИ ПОДОБНОЙ ЖИЗНЕННОЙ СИТУАЦИИ И СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, ВАМ НЕОБХОДИМО ОБРАТИТЬСЯ В ОРГАНЫ ВНУТРЕННИХ ДЕЛ ИЛИ ПРОКУРАТУРУ

ВАШ РОДСТВЕННИК ПОПАЛ В БЕДУ!

Добрый день! С вами говорит майор Свирепов. Ваш внук стал виновником ДТП и разбил машину важных людей. Мы готовы помочь ему избежать наказания за содеянное. Это обойдется вам в кругленькую сумму...



! Не поддавайтесь панике. Свяжитесь с «пострадавшим» родственником !

Мошенники мастерски используют множество психологических приёмов, чтобы вывести жертву на эмоции.

ЗВОНКИ И СООБЩЕНИЯ ОТ РУКОВОДСТВА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Здравствуйте! Это ректор университета, пишу по такому делу. Я проводил встречу с куратором нашего учреждения, Пузыркиным В.В. Мне предоставили список сотрудников, с кем он будет связываться лично. Попросили предупредить. Поэтому не пропустите звонок, это важно.



! "Вдох-выдох", следует задуматься и не поддаваться эмоциям !
Свяжитесь с руководством учебной организации по официальным каналам связи.

! Обратите внимание на оформление полученных документов и формулировку требования !
Помните, что в последнее время особую актуальность обретает технология deep fake, позволяющая подделывать голос кого угодно.
Официальные обращения от представителей государственных учреждений не поступают посредством социальных сетей, в мессенджерах.

ЗВОНОК ОТ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА

Здравствуйте! Вас беспокоит служба безопасности. На данный момент кто-то пытается вывести денежные средства с вашего счета. Не могли бы вы назвать номер вашей карты, CVV-код и код из СМС?



! Будьте бдительны! Не поддавайтесь уловке!

Главное отличие настоящей службы безопасности от мошенников - банку достаточно услышать, что вы не подтверждаете операцию; никаких кодов для блокировки никогда не запрашивают.

ЗВОНОК ОТ «НАЧАЛЬНИКА»

Здравствуйте! Произошла утечка данных, в результате чего средства с банковских счетов и вкладов могут быть похищены. В ближайшее время с вами свяжется представитель компетентных органов, который проинструктирует о дальнейших действиях. Только никому не говорите о вашем разговоре, чтобы избежать излишней огласки.



! Убедитесь, что разговариваете именно с вашим руководителем !
Чтобы это проверить - позвоните ему, но при этом наберите номер самостоятельно, а не перезванивайте на знакомый номер, с которого поступил звонок.

СФОТОГРАФИРУЙ МАМИНУ КАРТОЧКУ

Привет, Малыш! Я подруга твоей мамы, тетя Света. Мне срочно нужна твоя помощь! Я потеряла кошелек и не могу вернуться домой! Сфотографируй, пожалуйста, мамину банковскую карту с двух сторон и отправь мне по этому номеру, а я потом занесу ей денежку, а тебе шоколадку!



! Обезопасьте своего ребенка от влияния мошенников. Проведите с ним беседу о финансовой грамотности !
Постарайтесь объяснить своим детям, что они также могут стать жертвой мошенников, и им нужно быть осторожными и не разглашать никакие данные чужим людям.

Кто мы?

Мы правопросветительский
студенческий проект
Дальневосточного юридического
института (филиала) Университета
прокуратуры Российской Федерации.



С какой целью создано «КИБЕРЪОКО»?

Наша цель: снижение уровня киберпреступности в
Приморском крае, правовое информирование
населения о методах защиты от
киберпреступлений и правилах безопасного
поведения в сети Интернет, а также содействие
развитию информационного общества.

Задачи «КИБЕРЪОКО»

1. Анализ и мониторинг киберпреступности как в
Дальневосточном Федеральном округе, так и в
Российской Федерации, а также выявление новых
видов киберугроз и кибератак.
2. Сотрудничество с правоохранительными
органами, экспертами в области
информационной безопасности и другими
организациями для противодействия
киберпреступлениям.
3. Обучение и повышение осведомленности
населения о методах защиты от
киберпреступлений и правилах безопасного
поведения в сети Интернет.
4. Создание и поддержка информационных
ресурсов и образовательных программ по
кибербезопасности.

Присоединяйтесь к нам, чтобы быть в курсе последних
новостей, советов и рекомендаций по безопасности в
интернете.



@CYBEROKO



Для слепых и
слабовидящих

УЧАСТНИКИ ПРОЕКТА



© Выполнено представителями «КиберЪОко»
под научным руководством: Сыромля
Ларисы Борисовны - заведующего кафедрой
прокурорского надзора за исполнением
законов в оперативно-розыскной
деятельности и участия прокурора в
уголовном судопроизводстве
Дальневосточного юридического института
(филиала) Университета прокуратуры
Российской Федерации, советника юстиции,
кандидата юридических наук

ПАРТНЕРЫ ПРОЕКТА



КИБЕР
ОКО
ПОДКЛЮЧЕНИЕ
ЗАЩИЩЕНО

ДАЛЬНЕВОСТОЧНЫЙ
ЦЕНТР
ПРОФИЛАКТИКИ
КИБЕРПРЕСТУПНОСТИ

Ознакомьтесь с наиболее распространенными схемами мошенничества!



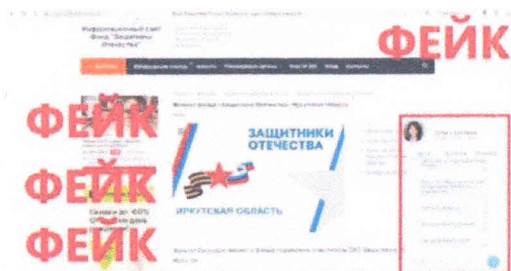
ФИШИНГОВЫЙ САЙТ ФОНДА «ЗАЩИТНИКИ ОТЕЧЕСТВА»

Вы переходите по первой ссылке на сайт «fzo.gov.prim.ru», где видите яркие рекламные баннеры и всплывающий чат с консультантом:
– Здравствуйте, мы поможем Вам получить выплаты за символическое вознаграждение!

Немедленно прекратите общение с консультантом и закройте сайт!

Обратите внимание на то, что:

- 1) на официальном сайте фонда не размещается реклама;
- 2) ссылка официального сайта фонда не содержит никаких иных символов, кроме «fzo.gov.ru»;
- 3) фонд работает на безвозмездной основе и не требует вознаграждение за свои действия;
- 4) разговоры с сотрудниками фонда не проходят во «всплывающих чатах».



ОБНОВЛЕНИЕ БАЗЫ ДАННЫХ

Вас беспокоит сотрудник фонда «Защитники Отечества». Мы вынуждены обновить нашу базу данных. Пожалуйста, отправьте ответным сообщением данные своего паспорта. Это необходимо для получения выплат.



Ни в коем случае не отправляйте свои данные! Правильным решением будет позвонить по официальному номеру фонда и уточнить, действительно ли происходит обновление данных.

КАДРОВЫЕ ПЕРЕСТАНОВКИ

Здравствуйте, это председатель фонда «Защитники Отечества». Недавно мы уволили недобросовестного сотрудника, который отправлял данные о наших воинах мошенникам. Для того, чтобы защитить Ваши выплаты от хакерских атак, отправьте нам сведения о себе.

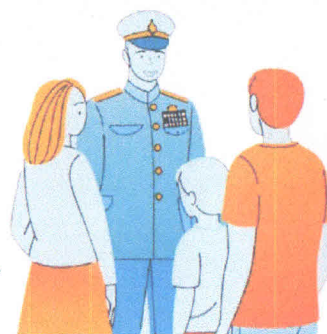


Не стоит верить таким «кадровым перестановкам». Защита от хакерских атак является направлением деятельности специально обученных для этого сотрудников, которые не будут запрашивать ваши персональные данные через СМС-рассылку.

ВАШИ ВЫПЛАТЫ В ОПАСНОСТИ

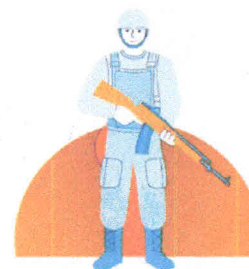
Это фонд «Защитники Отечества»! С нами связались сотрудники ФСБ и сообщили, что на Ваш счёт будет совершена хакерская атака. Срочно переведите свои социальные выплаты на следующий безопасный счёт...

С вами разговаривает мошенник! Никаких «безопасных счетов» не существует. Если вы сомневаетесь в правильности своих действий, обратитесь к представителям фонда через официальный сайт. Только так вы гарантированно будете общаться с настоящими сотрудниками фонда.



ОПЛАТИТЕ УСЛУГИ В ОФИСЕ

Добрый день. Вы посещали сайт фонда «Защитники Отечества» и общались с нашим онлайн-консультантом. Вам была оказана посильная помощь. Теперь Вам необходимо прийти в наш офис и оплатить оказанные услуги.



Немедленно положите трубку, ведь с вами общается мошенник!

Не забывайте, что на официальном сайте фонда нет «консультантов», а помощь, оказываемая сотрудниками, является бесплатной.

Киберсуицид — это самоубийство или попытка самоубийства, в котором цифровые технологии (интернет, социальные сети, мессенджеры, онлайн-сообщества и т. д.) играют ключевую роль в мотивации, планировании, организации или непосредственном совершении акта.

УСЛОВИЯ И ПРИЧИНЫ, СПОСОБСТВУЮЩИЕ ПОБУЖДЕНИЮ НЕСОВЕРШЕННОЛЕТНЕГО К КИБЕРСУИЦИДУ

1) **«онлайн-травля» (кибербуллинг):** непрекращающиеся оскорбления, унижения, угрозы в сети могут довести человека до неблагоприятного психоэмоционального состояния с выраженным уровнем постоянного эмоционального напряжения, психического истощения, состояния беспомощности, безнадежности и бессилия, что обуславливает развитие суицидальных тенденций;



2) **депрессия и другие психические расстройства:** интернет может усиливать существующие проблемы с психическим здоровьем;



3) **изоляция и одиночество:** социальные сети могут приводить к ощущению изоляции и неприятия;

4) **участие в онлайн-играх:** под видом «квестов», «испытаний» или «секретных клубов» пользователям предлагают выполнять задания



5) **влияние медиа и негативного контента:** романтизация самоубийств в медиа, пропаганда видео и аудио материалов суицидального характера на видео каналах, форумах и в социальных сетях»;

6) **неспособность справиться с онлайн-проблемами:** потеря репутации, взлом аккаунтов, сексуальная эксплуатация и шантаж и др.

МАРКЕРЫ СУИЦИДАЛЬНОГО ПОВЕДЕНИЯ ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

Маркеры суицидального поведения – это сигналы, знаки, которые прямо или косвенно дают понять окружающим о намерении человека совершить самоубийство.



На стадии антивитаальных переживаний:

- высказывания о том, что надоело жить, не хочу жить, и т.п.;
- поиск информации (интернет-серфинг) о способах суицида, а также участие в группах, пропагандирующих суицид;
- увеличение времени, проводимого в Интернете, особенно, ночью;
- скрытность – резко меняет пароли на мобильных устройствах, скрывает экран, становится подозрительным и закрытым в отношении своей онлайн-деятельности и др.

На стадии суицидальных замыслов:

- высказывания о своих намерениях покончить жизнь самоубийством, в том числе, в виде шуток, а также постах в социальных сетях;
- заявления о том, какие способы, время и место совершения самоубийства наиболее подходящие, безболезненные, доступные;
- завершение своих дел, возвращение долгов, раздача своих вещей, прощание с близкими, написание прощальных записок; резкое, без явной причины изменение настроения от сниженного к повышенному.

На стадии суицидальных намерений:

- собственно суицидальные попытки;
- появление или усиление самоповреждающего поведения (порезы, ожоги, царапины и др.);
- употребление алкоголя, наркотиков – способ медленного самоуничтожения (латентный суицид);
- демонстрация рискованного поведения – действия, несущие угрозу для жизни, но при этом осознанной цели именно сейчас покончить жизнь самоубийством нет и др.