



приоритет 

Сценарий мастер-класса «Ловушка сети: как остановить виртуальное преследование» или что такое киберсталкинг?»

Авторский коллектив:

Гуляев Д.Е. - директор центра по обеспечению прав молодежи в цифровом пространстве;

Камаева Е.А. - обучающаяся университета имени О.Е. Кутафина



СОЦИОПРАВО



приоритет 



«Ловушка сети: как остановить виртуальное преследование» или что такое киберсталкинг?: сценарий мастер-класса / Гуляев Д.Е., Камаева Е.А. Москва, 2025. 15 с.

*Камаева Екатерина Андреевна,
обучающаяся университета имени О.Е. Кутафина*

Сценарий мастер-класса

«Ловушка сети: как остановить виртуальное преследование» или что такое киберсталкинг?

Аудитория: 7-8 классы (14-16 лет)

Цель: приобретение нового знания

Время: 45 минут / 1.5 часа.

Инвентарь: стол для ведущего, презентация, ручки, листы бумаги, распечатанные заготовки, доска с мелом, проектор, доска для проектора, конверты с подсказками, папка для дела.

Приветственное слово, представление стикеров.

Спикер: практически вся наша жизнь сейчас оказалась перенесена в интернет-пространство. Это и онлайн-покупки, и общение в социальных сетях, и учеба на онлайн-платформах. С одной стороны, цифровизация сделала нашу жизнь проще и быстрее – сейчас не проблема общаться с человеком,

находящимся на другом конце Земли или купить новую кофточку в интернет-магазинах. Однако есть и обратная сторона: появилась новые возможности для совершения краж, интернет-травли, а также возникло и совершенно новое явление «киберсталкинг», о котором сегодня и пойдет речь.

Давайте перейдем к обсуждению. Поделитесь своими знаниями, кто знает что такое «киберсталкинг»?

Слушатели: *ответы.*

Спикер: интересная точка зрения. Хочу предложить вам две ситуации. Мне интересно узнать ваше мнение, можно ли назвать эти ситуации интернет-слежкой?

Два кейса выводятся на 1 слайд.

<i>Кейс 1</i>	<i>Кейс 2</i>
Пете очень нравится его одноклассница Маша. У девочки приближается день рождения. Петя очень хотел подарить Маше подарок, но не знал, что ей подарить. Он решил посмотреть ее сообщества и подписки в Социальных сетях, чтобы узнать, чем она интересуется.	Пете очень нравилась Маша. Но как очень часто бывает, Маше не нравился Петя. Но Петя решил, что она обязательно его полюбит, нужно только проявить настойчивость. Он каждый день посматривал ее аккаунт. Просмотрел всех ее друзей и каждый раз, когда какой-то новый мальчик добавлялся ей в «Друзья», он ревновал и писал ему угрозы или неприятные комментарии на страничке. С Машей стали неохотно общаться ребята из школы, поскольку знали, какие последствия это могло повлечь.

Итак, что думаете? Какие основные различия вы видите в этих двух ситуациях?

Слушатели: *ответы.*

Спикер: мне очень нравится ход ваших мыслей. Я предлагаю систематизировать ваши ответы и вывести конкретные признаки киберсталкинга. Как вы думаете, с какого признака стоит начать?

Спикер слушает ответы, которые ранее давали ребята и повторяет их. Ребята подбирают синоним. Спикер записывает слова на доску.

Предполагаемые варианты ответов (порядок может быть любой. Если слушатели упускают какой-то признак, спикер ссылается на ответы ребят, «кто-то из вас ранее обратил внимание на ...»):

- **Систематичность** («Действия по сбору информации должны повториться несколько раз и в отношении одного и того же человека. Важно, что действия могут быть не одинаковыми, но взаимодополняющими, например, сбор информации о человеке, отправка ему навязчивых сообщений. В таком случае действия скорее всего будут признаны систематичными»).

- **Продолжительность слежки** («слежка, как правило, имеет продолжительный характер, по статистике от 6 месяцев. Как думаете, как долго длилось самое продолжительное преследование в истории?»)

Слушатели: *ответы.*

Спикер: на самом деле, самое долгое преследование в Сети длилось 20 лет. Представляете? А ведь это только среди тех случаев, которые получили публичную огласку. Возможно, есть и более длинные периоды, но официально они не зарегистрированы, поскольку пострадавшие не стали обращаться за помощью к правоохранительным органам. Как вы думаете, почему люди, сталкиваясь с подобными правонарушениями, предпочитают не обращаться за помощью?

Слушатели: *ответы.*

Спикер: по вашему мнению, насколько эффективен этот способ решения проблемы?

Слушатели: *ответы.*

Спикер: а как бы вы повели себя, если бы столкнулись с киберсталкингом?

Слушатели: *ответы.*

Спикер:

- ***Причинение вреда.*** Мы подошли к очень сложному вопросу - вопросу соотношения мотивом и целей в праве. Очень часто люди ошибочно используют их как синонимы. Однако разница между ними есть. Мотив – это те эмоции, которые побуждают человека совершать те или иные действия. Это влюбленность, как в случае с нашим Петей. А вот цель, наоборот, подчинена именно силе логике и разума. Это тот результат, который мы видим в голове и которому стремимся. Поэтому, например, мы говорим, что целью ведения интернет-слежки может быть оказание давления. А вот мотивом может выступать влюбленность. Говоря о давлении, я в первую очередь имею в виду психологическое давление. Действия киберсталкера могут быть выражены в виде навязчивых сообщений, угроз, постоянных звонков, то есть оставаться в онлайн-пространстве. Но никогда не стоит забывать, что вред, который наносится жертве, может перенестись из формата «онлайн» в реальную жизнь.

- ***Преднамеренность.*** Какими мотивами руководствовался Петя?

Слушатели: *ответы.*

Спикер: Вы правы. Преследование лица, направленное на получение от него взаимных чувств, получило название «интимное преследование». Как вы считаете, что еще может сподвигнуть киберсталкера к сбору информации о другом человеке, написании ему навязчивых сообщений или угроз?)

- **Персонафицированность.** Действия киберсталкера могут быть направлены либо против конкретного человека, либо группы лиц, обладающих общим признаком. При том связь между «жертвой» и «киберсталкером» может быть как явная (например, если это бывшие возлюбленные), так и абсолютно неочевидная (если люди никогда не были знакомы). Более того, жертва иногда может даже не подозревать, что находится под чьим-то постоянным наблюдением, но даже в этом случае, действия будут являться киберсталкингом).

Ну что, друзья, мы проделали с вами серьезную аналитическую работу. Результат ее вы видите на доске. На основе всего того, что было сказано, как бы вы дали определение понятию киберсталкинг?

Слушатели: *ответы.*

Спикер: друзья, я вас поздравляю, ваше определение практически точь-точь совпадает с определением, которое содержится в словаре Касперского! Знаете, что по этому поводу там было написано?

Зачитывает с листка:

«Слово «киберсталкинг» состоит из двух слов – «cyber» («цифровой») и «stalking», что в переводе с английского переводится как преследование. Таким образом становится понятно, что киберсталкинг представляет систематическое преследование человека, группы или компании, их запугивание и домогательство с использованием Интернета и других электронных средств коммуникации. Это могут быть различные социальные сети, платформы для общения, мессенджеры».

Давайте подведем предварительный итог. Мы с вами определили, что из себя представляет киберсталкинг и выявили его критерии. Сейчас, с учетом этой информации, скажите, по вашему мнению, понесет ли Петя ответственность за проведение интернет-слежки в отношении Маши? Просто предположите

Слушатели: *ответы.*

Спикер: на самом деле, ответа на этот вопрос сейчас нет. Ни в уголовном кодексе, ни в кодексе об административных правонарушениях нет нормы, которая бы закрепляла ответственность за кибер-слежку. Но вот за отдельные проявления привлечь человека можно, и такая практика уже есть. Я предлагаю сейчас ознакомиться с несколькими. Пожалуйста, открывается на своих гаджетах Уголовный кодекс Российской Федерации.

Спикер называет статьи, ребята ищут размер санкций:

- Доведение до самоубийства (ст. 110 УК РФ);
- Склонение к совершению самоубийства или содействие в совершении самоубийства (ст. 110.1 УК РФ);
- Угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ);
- Клевета (ст. 128.1);
- Нарушение неприкосновенности частной жизни (ст. 137 УК РФ);
- Вымогательство (ст. 163 УК РФ);
- Некоторые исследователи также отмечают, что проявления киберсталкинга можно рассматривать и в свете административного права, например:
- Мелкое хулиганство (ст. 20.1 КоАП РФ);
- Оскорбление (ст. 5.61 КоАП РФ);
- Клевета (ст. 5.61.1 КоАП РФ).

Вот так. Но несмотря на нависшую над пользователями Интернета угрозу киберсталкинга, его распространение можно остановить. Сейчас мы предлагаем разработать нашу с вами собственную модель как противостоять киберсталкингу.

Возможные меры противодействия можно разделить на две группы: одни направлены на предотвращение киберсталкинга – таким образом невозможно будет против вас провести слежку, а вторые меры – это меры, направленные на его остановку, если интернет-слежка уже началась.

Друзья, поделитесь идеями, как обезопасить себя от действий киберсталкера?

Слушатели: *ответы.*

Возможные варианты. Если какой-то не назовут, стикер озвучивает их самостоятельно просит описать их эффективность:

Спикер (дополняет):

- ***Установить настройки приватности в социальных сетях.***

«Для этого можно ограничить круг лиц, которые могут писать вам личные сообщения или звонить».

- ***С особым вниманием относиться к Интернет-знакомствам.***

«Проверяйте тех, кого вы добавляете в «друзья» - для этого достаточно хотя бы посмотреть страничку человека. Если возникают подозрения о том, что аккаунт является «фейком» – об этом могут свидетельствовать, вымышленное имя пользователя, отсутствие какой-либо информации о нем, контент, который человек публикует у себя на странице - лучше не добавлять человека в друзья и тем более не начинать переписку».

- ***Обязательно обдумывайте, какую информацию стоит публиковать на своей страничке в социальной сети, а какую- нет.***

«Не стоит указывать или отмечать свой адрес проживания, свое расписание на день, информацию о своих доходах или доходах родителей».

- ***Тщательно подбирайте пароли для социальных сетей.***

«Часто именно через взломанные аккаунты киберсталкеры получают доступ к вашим данным, могут следить за вами, отправлять угрозы или распространять личную информацию без вашего согласия.

Вот тут на помощь приходят менеджеры паролей — это такие специальные программы, которые помогают создавать очень сложные пароли и надежно их

хранить. Благодаря им вам не нужно придумывать и запоминать сотни разных паролей — весь этот «тяжелый труд» берет на себя менеджер паролей.

Используя такой менеджер, вы значительно снижаете риск того, что кто-то взломает ваш аккаунт и начнет вас преследовать в интернете. Это как броня для вашей цифровой безопасности.

Так что, если хотите быть настоящими защитниками своей онлайн-жизни и бороться с киберсталкингом — выбирайте надежные менеджеры паролей. Это простой и эффективный способ защитить свою личную информацию и спокойствие!»

«Что вы бы могли посоветовать, если бы у вас спросили о правилах подбора пароля?»

- *Длина пароль минимум 10-12 символов;*
- *Избегайте последовательностей букв и цифр на клавиатуре (1234, asdf и других). Хакеры часто используют программы перебора по словарю, что делает такой пароль легко раскрываемым;*
- *Используйте разные пароли для разных социальных сетей;*
- *Используйте неочевидные замены. Например, 0 замените на O и тд.*

- ***Стараться не разрешать сбор данных cookie.***

«Нажимая «ОК», вы значительно облегчаете сайту задачу по сбору ваших данных, которые могут потом попасть не в те руки».

Благодарю вас, друзья, за ваши рекомендации. Я думаю, мы можем внести Ваши предложения в нашу памятку по Интернет-безопасности для учеников начальной школы.

Спикер: Современные технологии искусственного интеллекта кардинально изменили характер киберсталкинга, создав как новые угрозы, так и возможности для защиты. Давайте разберем, какую роль играет ИИ в этом явлении.

Риски использования ИИ киберсталкерами

Автоматизация преследования. Современные ИИ-системы позволяют киберсталкерам автоматизировать процесс слежки в масштабах, ранее недостижимых. С помощью алгоритмов машинного обучения злоумышленники могут систематически отслеживать активность жертвы в социальных сетях, анализировать ее поведенческие паттерны и предсказывать будущие действия.

Распознавание лиц и идентификация. Технологии распознавания лиц, основанные на ИИ, превратились в мощный инструмент для сталкеров. Как показал случай с приложением FindFace, любой пользователь может сфотографировать человека и найти его профили в социальных сетях, что привело к массовым случаям шантажа и травли.

Дипфейки и синтетические медиа. ИИ-технологии позволяют создавать крайне реалистичные поддельные видео и аудиозаписи. В 96% случаев дипфейки имеют порнографический характер и создаются без согласия изображенных людей. Это стало новым инструментом для киберсталкеров, позволяющим им шантажировать жертв и разрушать их репутацию.

Персонализированное преследование. ИИ анализирует цифровые следы пользователей, позволяя сталкерам создавать детальные профили своих жертв. Эта информация используется для более эффективного психологического воздействия и манипулирования.

Возможности ИИ для борьбы с киберсталкингом

Автоматическое обнаружение угроз. Системы на основе машинного обучения способны анализировать паттерны поведения в реальном времени и выявлять признаки киберсталкинга. Алгоритмы могут обнаруживать аномальную активность, подозрительные попытки доступа к личной информации и координированные атаки.

Анализ текстового контента. Технологии обработки естественного языка (NLP) позволяют автоматически анализировать сообщения, комментарии и посты на предмет угроз, оскорблений и признаков преследования. Системы могут выявлять скрытые угрозы даже в завуалированных сообщениях.

Защита приватности. ИИ-алгоритмы помогают пользователям лучше контролировать свои персональные данные, автоматически настраивая параметры конфиденциальности и предупреждая о потенциальных утечках информации.

Модерация контента. Платформы социальных сетей используют ИИ для автоматической модерации, блокируя нежелательный контент и предотвращая распространение материалов, используемых для киберсталкинга.

Вызовы и ограничения

Гонка технологий. Развитие ИИ создает ситуацию "щита и меча" - одновременно с появлением новых защитных механизмов злоумышленники находят способы их обхода.

Проблема ложных срабатываний. ИИ-системы могут ошибочно классифицировать безобидный контент как угрозу, что создает дополнительные проблемы в борьбе с киберсталкингом.

Адаптивность угроз. Киберсталкеры активно используют ИИ для адаптации своих методов к новым защитным мерам, создавая более сложные и изощренные формы преследования.

Спикер: важно понимать, что искусственный интеллект - это инструмент, который может использоваться как во благо, так и во вред. Наша задача - обеспечить развитие и применение ИИ-технологий таким образом, чтобы они служили защите пользователей от киберсталкинга, а не становились оружием в руках злоумышленников.

Какие меры предосторожности, по вашему мнению, должны предпринимать разработчики ИИ-систем, чтобы минимизировать риски их злонамеренного использования для киберсталкинга?

Слушатели: ответы.

А что делать, если уже оказался «под прицелом» киберсталкера? Наша команда Молодежного цифрового Омбудсмана провела анализ и выявила наиболее эффективные способы пресечения случаев киберсталкинга, если он уже начался:

1. Самое простое и очевидное – *не реагируйте на его выпады*. Заблокируйте, ограничьте доступ к своей странице. Не ведитесь на его уловки!

2. *Зафиксируйте факты киберсталкинга*. Для этого достаточно сделать скриншот. Так вам будет проще доказать факт преследования вас в Интернете.

3. При необходимости *обратитесь к взрослым или в полицию*. Не занимайтесь самостоятельным выслеживанием преступника – это задача полиции и других правоохранительных органов.

4. Вы также можете *обратиться за помощью к команде Молодёжного Цифрового омбудсмена. На экране qr-код.* Мы поддержим вас и поможем прекратить киберпреследование.

Предлагаем завершить наше обсуждение с помощью интерактива.

Групповая работа (два варианта) + Интерактив (в случае наличия времени).

1 вариант

Класс поделен на группы. Не более 4-5 групп.

Спикер: друзья, я уже говорила ранее, что мы создаем памятку для младших классов о безопасности в Интернете. Но с учениками младших классов у нас не получится устроить такой диалог на равных, как сегодня провели мы с вами. Поэтому нам нужна ваша помощь – нам необходимо записать для ребят небольшое видео о киберсталкинге. Важно, оно должно быть понятным для учеников начальной школы. Длительность у видео должна быть небольшая – не более 3 минут.

2 вариант

Спикер: сегодня мы с вами обсудили существующую на сегодня проблему киберсталкинга. Поделитесь, что вам показалось наиболее интересным?

Слушатели: *отвечают.*

Спикер: ну теперь вы точно можете самостоятельно урок проводить! И на самом деле, у вас есть такая возможность. Друзья, я уже говорила ранее, что мы создаем памятку для младших классов о безопасности в Интернете. Но с учениками младших классов у нас не получится устроить такой диалог на равных, как сегодня провели мы с вами. Поэтому нам нужна ваша помощь – нам необходимо записать для ребят небольшое видео о киберсталкинге. Оно должно быть понятным для учеников начальной школы. Поэтому предлагаю каждому из

поучаствовать в съемке видеоролика и поделиться самым интересным фактом, который вам сегодня запомнился (*спикер снимает самостоятельно*).

Интерактив (в длительности мастер-класса в два академических часа)

Формат «Своей игры», но с дополнениями под тематику урока.

Основная цель игры – повышение информированности .

Задача участников – выявить «киберсталкера»

Класс поделен на 4 команды (обязательное четное количество команд). 2 команды гражданами, две – правоохранительные органы.

На доске висит 4 изображения разных людей. Под каждым из них дана краткая информация (возраст, пол, имя, род занятий и тд). Фото цветные с людьми, внешне очень похожими. Изображения людей можно сгенерировать через нейросеть.

На проекторную доску выведен слайд, где изображен большой квадрат, поделенный на 12 ячеек. Задания будут разного плана – от решения кейсов до заданий на поиск какой-либо информации (например, познакомим их с некоторыми структурами МВД РФ или какими-то организациями, куда ребята могут обратиться в случае чего и тд; нормы УК РФ, а именно их санкции.

Игра начинается с того, что ведущий, представляется неким должностным лицом, например, сотрудником полиции, и сообщает о том, что поступило сложное дело, связанное с преследованием человека. Сообщается, что вся информация о жертве содержится в конверте. Ведущий открывает и зачитывает текст. Можно выдать по одной-две карточки дела на команду, чтобы все ознакомились. Можно также дать карточки подозреваемых.

Участники выбирают ячейку, при нажатии на нее появляется задание. За ответы ребята получают подсказки. Подсказки будут разные. У граждан они будут касаться каких-то личных данных о киберсталкере и о жертве (данные, которые позволят раскрыть его и жертву как личность, за которыми стоят свои

истории). У правоохранителей они более содержательные и больше указывают на признаки лица, по которым его можно будет опознать (ведь именно им в итоге нужно будет принять решение кто является киберсталкером).

На обсуждение вопроса – 5 минут.

Подсказки озвучиваются вслух, чтобы они были у каждого.

В конце на основе всех подсказок, «правоохранители» озвучивают ответ.

Ведущий озвучивает, что дело будет передано суд для возбуждения уголовного дела.

По окончании, ведущий обсудит с ребятами, что они чувствуют по отношению к жертве, киберсталкеру и мере ответственности, которая будет к нему применена.

Спикер: друзья, сегодня мы с вами провели огромную работу:

- Обсудили существующую проблему киберсталкинга;
- Выделили его характерные признаки;
- И даже разработали собственные модели противодействия киберсталкингу.

Завершая наш урок, хочу озвучить мысль, к которой я пришла сегодня во время нашего обсуждения: в мире нет ничего «черного» и «белого». Во всем можно найти как что-то положительное, так и отрицательное. Преступник – тоже человек. И мы никогда не знаем, какая история у этого человека. Поэтому в следующий раз, когда вы встретите злого, грубого человека, подумайте, а может он просто несчастен?

Спасибо за внимание!