**Конспект к презентации**

**Информационная памятка для несовершеннолетних по вопросам кибербезопасности в сети «Интернет»**

|  |  |
| --- | --- |
| **№ слайда** | **Описание слайда** |
| **Слайд 1** | Практика манипулирования общественным мнением имеет долгую историю, а «fake news», как метод воздействия на умы и поведение людей, как средство ведения информационных войн, давно и широко используется в политической сфере.  Сегодня мы наблюдаем военизацию информации в беспрецедентных масштабах. В большинстве стран мира снижается доверие к СМИ, а социальные медиаплатформы заменяют роль журналистики, предлагая простые, доступные и свободные инструменты для обмена информацией, практически не подающиеся контролю и фактчекингу (проверке фактов), что представляет существенную угрозу для информационной безопасности государства.  Термин «fake news» всё больше становится политизированным, на государственном уровне с помощью фейков решаются разнообразные задачи – от дестабилизации внутриполитической и социальной ситуации, влияния на политические процессы (в том числе на предвыборные кампании), снижения репутации политика до провоцирования массовых беспорядков, цветных революций, радикальных действий и войн. В различных регионах мира ложные новости приводят к подрыву суверенитета и нарушению территориальной целостности государств. |
| **Слайд 2** | **Fake news: что это?**  Фальши́вые (подде́льные, «фе́йковые», ло́жные) но́вости — это информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных СМИ с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду. Простыми словами **Fake** – подделка.  Главный принцип генерирования фальшивых новостей — максимально негативная или абсурдная информация, которая регулярно тиражируется в онлайн-пространстве.  И если одни фейки условно безвредны, то большая их часть представляет угрозу здоровью людей или является инструментом для манипулирования сознанием.  Фейк вызывает максимально сильные, негативные эмоции — гнев, беспокойство, страх, тревогу, ненависть, которые возникают у человека из-за попадания в его точку боли. Например, проблемы в бизнесе, низкие зарплаты, отсутствие социальных гарантий, рост цен на продукты.  Например, весной 2020 года в Британии пытались [поджечь](https://www.bbc.com/russian/news-52284859) 20 сотовых вышек из-за появления слуха о том, что 5G распространяет коронавирус. А ещё раньше поджог, который совершили поверившие в этот фейк, уничтожил оборудование для передачи связи, которой пользовались аварийно-спасательные службы и несколько мобильных операторов, лишив кого-то тем самым, возможно, надежды на спасение.  Также в СМИ активно гулял [фейк](https://aibolit66.ru/patient/articles/COVID-19/" \t "_blank) на тему того, что домашние животные могут заразиться COVID-19, вакцинация населения опасна, а защититься от заразы можно с помощью обильного горячего питья, пребывания на солнце и даже водки.  Но дело тут не только в каронавирусе, главная цель - это введение в заблуждение, для того чтобы получить финансовую или политическую выгоду. |
| **Слайд 3** | **Есть три составляющих фейковых новостей:** *соцсети, телекоммуникационные технологии и специфическая мотивация.*  Фейковые новости практически всегда либо про политику, либо про деньги. Политических манипуляторов привлекает в соцсетях их «народный» характер, а коммерческих злоумышленников — ещё и монетизация.  **Политика.** Чаще всего fake news генерируются для влияния на выборы или какую-либо политическую фигуру. Традиционные источники информации для этого не совсем подходят, ведь обычный человек всё более склонен верить «таким же простым людям, как и он» в соцсетях, а не «аффилированным с государством или корпорациями» СМИ. Именно поэтому фейковые новости создаются с прицелом на соцсети — здесь у каждого участника есть определённый «соседский» круг доверия.  **Деньги.** Создавая фейковые новости, можно усиливать активность определённых групп потенциальных клиентов. «Только три знака зодиака переживут 2020 год…» — кликбейт-заголовок, который в итоге может привести на посадочную страницу сервиса платной рассылки гороскопов. Соцсеть в этом случае играет роль хирургически точного инструмента вовлечения нужных групп потенциальных клиентов в орбиту влияния бренда. А пережив 2020 год, представители «неудачливых» знаков уже и не вспомнят о короткой новости, репост которой они увидели в тематической группе.  **В будущем появится ещё и третий мотив — конкуренция**, то есть фейковые новости всё чаще будут создавать для подрыва репутации бизнеса. |
| **Слайд 4** | **Далее разберём, как, собственно, работает механизм создания и распространения фейковых новостей.**  Фейковые новостные кампании обычно проходят в несколько этапов, хотя это процесс творческий, и в зависимости от целей или особенностей аудитории некоторые стадии могут быть опущены. |
| **Слайд 5** | 1. **Разведка**  На первом этапе организатор кампании изучает целевую аудиторию. Он отвечает на три основных вопроса: «Кому врать?», «О чём врать?» и «Зачем врать?». Анализ проводится самый широкий — от образовательного уровня и информационной грамотности будущих читателей до их взглядов на жизнь. Собственно, на этом этапе и были пойманы специалисты Cambridge Analytica, которые собирали персональные данные пользователей Facebook для политических целей. |
| **Слайд 6** | 1. **Вооружение**  На втором этапе создаётся, собственно, фейковая новость. Её главная особенность в том, что почти всегда «декорации» фальсифицированной истории, то есть участники события, место и время действий, — реальные, а фейком является, собственно, само событие. В зависимости от масштабов компании, фейковых новостей может быть несколько. К примеру, первая история сообщает о событии, а последующие — развивают тему. Иногда к ним примешиваются даже настоящие новости, которые дополняют картину выдуманной истории. Они направлены на скептическую часть потенциальной аудитории.  *Помимо новостей, на втором этапе создаются агенты распространения:* фейковые пользователи соцсетей, фейковые новостные сайты, фейковые группы и сообщества. Для этого в ход идут чёрные и белые технологии SMM, позволяющие за деньги плодить и продвигать поддельных пользователей соцсетей. К примеру, в соцсети Weibo (китайский аналог Twitter) селебрити с 300 тыс. подписчиков можно создать примерно за 2,5 тыс. долларов всего за месяц. |
| **Слайд 7** | 1. **Распространение**  Обычно фейковая новость сперва появляется на таком же фейковом сайте новостей или на любой другой площадке, где публикации никак не контролируются. Далее в дело вступает «гуру» — прокачанный и авторитетный у целевой аудитории блогер, который публикует новость у себя. Сообщение подхватывают боты — реальные пользователи соцсетей или роботы, созданные/привлечённые специально для фейковой новостной кампании. Помимо распространения, они выполняют очень важную функцию — изолируют скептиков, которые остаются в меньшинстве и предпочитают сохранять молчание вместо противостояния фейкам. |
| **Слайд 8** | 1. **Эксплуатация**  На следующем этапе новость доходит до целевой аудитории и начинает жить своей жизнью. Наиболее вдохновлённые читатели лайкают и репостят фейковое сообщение, делятся им в мессенджерах. Возникает вирусный эффект, который привлекает внимание ещё более широкой аудитории — журналистов и других профессиональных участников медиаполя. Фейковая новость попадает в мейнстрим-медиа. |
| **Слайд 9** | 1. **Промывка**  Этот этап используется в долгосрочных кампаниях, призванных коренным образом изменить отношение целевой аудитории к каким-либо явлениям, причём иногда диаметрально противоположным образом. Для этого запускается не одна, а несколько последовательных фейковых новостных кампаний. Одна и та же история раскрывается через различные аспекты, появляются все новые герои событий, а вирусный эффект генерируется многократными волнами |
| **Слайд 10** | 1. **«Домашняя работа»**   После достижении заданной цели могут потребоваться дополнительные, закрепляющие действия. К примеру, если речь идёт о кампании, подрывающей репутацию какого-либо политика, в информационное поле могут быть запущены позитивные новости о нём, которые не имеют прямого отношения к фейковой истории, но несколько корректируют образ жертвы в глазах общественности. Такие действия призваны устранить у общественности ощущение травли или спланированной акции в отношении политика. |
| **Слайд 11** | 1. **Заметание следов**   Последний этап — сокрытие следов активности. Наиболее распространённая технология, позволяющая это сделать, — отвлекающая новость. Используя уже созданную инфраструктуру из ботов можно вбросить новое «информационное» сообщение. По своей тематике оно должно совершенно отличаться от прежней фейковой истории, быть ещё более громким и резонансным. Такая фейковая новость переключает внимание общественности на новую проблему и «глушит» голоса тех, кто, возможно, к этому моменту сумел идентифицировать прежний фейк. |
| **Слайд 12** | **Теперь, разобравшись в алгоритмах, давайте посмотрим на фейковую новость не глазами создателей, а со стороны аудитории. И выясним параллельно, как противостоять fake news?**  *Вырабатываем «иммунитет» к фейкам.*  Поскольку fake news бьют прямой наводкой по пользователям, первый рубеж обороны могут составить только сами читатели. Прежде всего, они должны определять фейковые новости по следующим признакам: |
| **Слайд 13** | 1. **Гиперболизированные и кликбейтные заголовки.**   Заголовки новостей коротко описывают суть произошедшего. Особенностью этой техники является обращение к пользователю на равных, использование разговорной лексики, фейковое задействование известных имен для придания авторитетности материалу. Так, читатели в возрасте верят кликбейт-«новостям», что актер или телеведущий излечился от серьезного заболевания, и переходят по ссылке, которая ведет на сайт, продающий какой-нибудь препарат.  Кликбейтный заголовок интригует читателя, призывая ознакомиться с продолжением начатой истории или обещая рассказать подробности сенсационного известия. По факту пользователь находит информацию, далекую от ожидаемой. Его любопытство не удовлетворено, но для владельца ресурса это не имеет никакого значения.  ***Распознать кликбейт по тексту или изображению несложно. Его явными признаками являются:***   * Стиль изложения, имитирующий желание как можно быстрее рассказать о важном событии, включая намеренные опечатки. * Упоминание неординарных и даже шокирующих происшествий. * Использование популярных мемов. * Знаки выделения– стрелка, кружок, обводка. * Обращение к актуальным и хайповым темам. * Задействование в тексте заголовка устойчивых оборотов речи и всем знакомых цитат.   ***Создателям кликбейтного контента хорошо знакомы те категории информации, которые вызывают безусловный интерес пользователей:***   * Опасные природные явления, стихийные бедствия, катастрофы, случаи чудесного спасения, смерть, болезни. * Заболевания, внезапное излечение от тяжелых недугов, улучшение внешнего вида без особых усилий, особенно похудение. * Истории успеха известных личностей и компаний. * Лайфхаки, простые способы обогащения и существенной экономии. * Острые социальные проблемы. * Предсказания будущего от знаменитых провидцев.   Авторы кликбейтных заголовков успешно играют на эмоциях и вводят в заблуждение даже критически настроенных пользователей.  **Эта техника по-прежнему действенна по двум причинам:**  **1. Люди ненавидят незнание**  Недостаток информации и желание получить ее любыми путями, особенно когда дело касается жизни, благополучия, угрозы здоровью, – сильнейший мотиватор, заставляющий людей нажимать на баннеры и ссылки. Они хотят убедиться, что находятся в безопасности, что им ничто не навредит, или стремятся найти способы избавления от существующей угрозы. Мало кто устоит перед заголовком типа «Проснувшийся вулкан может стать причиной гибели тысяч россиян»: появляется желание прочитать материал и убедиться, что твой населенный пункт расположен на безопасном расстоянии от места катастрофы.  **2. Страх упустить важное**  Синдром упущенной выгоды – весьма распространенное явление современной жизни. Его характерным признаком считается боязнь лишиться информации, которая уже известна остальным, или не принять участия в каком-то событии. Кликбейт использует эту особенность человеческой психики, заставляя нажимать на ссылку, чтобы не отстать от окружающих. Например: «Миллионы пользователей уже знают об этих фишках социальной сети. А вы?». Естественно, человек хочет убедиться, что ничего не пропустил и тоже владеет этими полезными сведениями.  ***Распространенные виды кликбейта:***  **1. Преувеличение**  Как добиться устойчивого интереса к описываемому явлению при помощи заголовка? Преувеличить его значение, используя размытые формулировки. Прочитав фразу типа «Страна готовится попрощаться с известным телеведущим» наталкивают на мысль о неизлечимой болезни и скорой кончине, однако на самом деле речь идет о его поездке на отдых.  Обычный заголовок должен выглядеть в этом случае как «Телеведущий проведет отпуск в Таиланде», но никакой интриги в таких заголовках нет, значит, и переходов по ним будет на порядок меньше.   1. **Искажение фактов**   Самый опасный вид кликбейта связан с формированием у читателя неверного представления об описываемых событиях или явлениях. Оно может проявиться в результате намеренного обобщения или замалчивания части информации.  Примером, когда автор утаил важные сведения, чтобы повысить интерес к материалу, может служить следующий заголовок: «Правительство готовит меры по запрещению iPhone». Российский пользователь, исходя из прочитанного, делает вывод о том, что любимым смартфоном нельзя будет пользоваться на его родине, и срочно кликает по ссылке, чтобы узнать, что речь на самом деле шла об Индии.  **3. Манипуляция эмоциями**  Чтобы усилить воздействие на читателей, авторы кликбейта придают заголовку такой вид, будто его писали второпях, стремясь как можно быстрее донести до аудитории важные новости: ставят лишние знаки препинания (особенно часто злоупотребляют восклицательными знаками), допускают пропуск букв, используют капслок и разговорные выражения. Все это должно подтолкнуть пользователя к срочному переходу на страницу статьи.  Примеров масса: «Смотреть ВСЕМ!!! Школьница на выпускном, ужасные нравы современной молодежи!!!», «ШОК!!! Страшная утрата, которую никто не мог предвидеть!». |
| **Слайд 14** | 1. **Подозрительные домены или искажённые названия сайтов популярных медиа, похожие на настоящие**. Забейте в поисковик название интересующего вас СМИ — на первых позициях в выдаче будут оригиналы. Сравните их интернет-адресом подозрительного источника.   **Важно знать!!!**  Фейковые сайты – один из самых опасных видов подделок. Если большинство фейковых фотографий не несут в себе прямой угрозы, то фальшивые сайты, полностью копирующие оригинал, созданы исключительно для фишинга. Понятие «фишинг» означает мошенническую схему для кражи пользовательских данных: логины и пароли соцсетей, реквизиты банковских карт и электронных кошельков и т.д.  Фишинговые сайты работают следующим образом: мошенники создают ресурс, который выглядит точно так же, как другой популярный портал (ВКонтакте, Одноклассники, Авито и прочие). Затем ссылки на него распространяются по соцсетям и мессенджерам, чаще всего под видом раздачи халявных денег или чего-то похожего. Наивные пользователи переходят по ним и видят, что для получения их якобы миллионных выигрышей нужно авторизоваться, например, через ВКонтакте. Они вводят свой логин и пароль, а злоумышленники успешно умыкают их себе, сразу же меняют данные для входа, и свою страницу назад человек уже не получит. Дальше этот профиль можно продать или использовать для обмана друзей этого пользователя якобы от его имени.  **Как защититься от фишинга?** Очень легко – быть внимательным. Во-первых, вам нужно осознать, что никто и никогда не даст вам денег в интернете просто так. Никто и никогда без исключений. Если какие-то подозрительные ссылки пророчат вам быстрый заработок за несколько кликов мышки, это стопроцентное мошенничество. Во-вторых, всегда обращайте внимание на адрес сайта. Мошенники очень часто добавляют всего одну букву в адрес или как-то иначе меняют его, чтобы он казался настоящим, а невнимательные пользователи этого не поняли. |
| **Слайд 15** | 1. **Большое количество ошибок или опечаток в тексте новости**. Попробуйте найти на сайтах известных вам СМИ эту же историю, но в более развёрнутом виде. Если поиски не увенчаются успехом, то, скорее всего, перед вами автоматически сгенерированный контент.   Так, например, в российских Telegram-каналах начали появляться украинские вбросы, связанные с объявленной в стране частичной мобилизацией. Представители Центра информационно-психологических операций пытались устроить панику в городах России, но выдали себя глупыми ошибками.  Так, например, в 2022 году на подобные ошибки обратил внимание телеграмм-канал "Война с фейками".  **Фейк отражен на слайде:** С 22 сентября в России представители военкоматов будут дежурить на стационарных постах ГИБДД. Дорожные полицейские будут останавливать автомобили под управлением мужчин, после чего их будут направлять к представителям военкоматов. На внутригородских дорогах будут дежурить мобильные группы. Информацию распространяют украинские и российские телеграм-каналы.  **Правда:** Документ фейковый, хотя и выполнен очень искусно. Тем не менее, сотрудники ЦИПсО ВСУ прокололись на мелочах. Например, «мероприятия» нельзя «выполнить», их можно «провести» или «обеспечить». Не выделены запятыми деепричастные обороты.  Представители ГУОБДД вряд ли могут входить в мобильные группы: их нет в регионах, это офисные сотрудники управления по безопасности дорожного движения. Патрульные полицейские, отвечающие за дорожное движение, называются инспекторами ГИБДД.  На документе размещена личная подпись Владимира Кузина. Однако, сейчас в органах МВД используются индивидуальные цифровые электронные подписи. Кроме того, руководители подразделений Госавтоинспекции на региональном уровне не входят в главное управление.  Наконец, в регионах нет подразделений ГУОБДД. Дорожной полицией руководят начальники УГИБДД ГУ МВД России по определенной области, краю или республике.  Есть ошибки и в оформлении — между текстом и подписью должен быть двойной отступ. В фейковом документе его нет.  Наконец, МВД России официально [заявило](https://vk.com/wall-26323016_47908), что данная информация не соответствует действительности. Опубликованный скан указания ГУОБДД МВД России является фейковым, а содержащиеся в этом «документе» сведения – ложными. |
| **Слайд 16** | 1. **Поддельные фото или коллажи.**   Попробуйте сохранить подозрительное фото и поискать его копии через фотопоисковики (Google, TinEyE и т.п.). Если копий нет в авторитетных источниках, то скорее всего перед вами фотошоп или дипфейк (deepfake) — это методика синтеза изображения, которая позволяет заменять одни элементы на другие.  К примеру, с помощью замены лиц эта технология может заставить говорить знаменитого человека то, что он не произносил, и делать то, что он никогда не делал.  Обычно называемые формой «синтетических медиа», дипфейки имитируют лица, движения и голоса людей с такой точностью, что их часто невозможно отличить от оригинала в реальной жизни без специальных инструментов.  Например, у одного из пользователейя **TikTok** в аккаунте всего было 3 ролика! Однако он уже собрал более **250 тысяч подписчиков**, почти миллион лайков и несколько миллионов просмотров.  И это всё благодаря **впечатляющему дипфейку с Томом Крузом где он** создал свои ролики со звездой франшизы «Миссия: невыполнима».  Другой пример: У генерального директора британской энергетической компании [мошенники смогли выманить 220 000 евро](https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#2e1ea5ee2241) с помощью дипфейковой имитации голоса руководителя головной компании, якобы запросившего срочно перевести указанную сумму. Подмена была настолько натуралистичной, что обманутый директор не стал перепроверять информацию, хотя средства переводились не в головной офис, а на сторонний счет. Только когда «босс» запросил еще один трансфер, его собеседник заподозрил неладное, но переведенные деньги уже бесследно исчезли.  К сожалению, дипфейки эволюционируют угрожающими темпами. Еще два года назад подделки легко было отличить по низкому качеству передачи движения; кроме того, люди в таких видео практически никогда не моргали. Однако технологии не стоят на месте, и дипфейки последнего поколения выполнены заметно более качественно.  По приблизительным оценкам, сейчас по Сети гуляет более 15 000 дипфейк-видео. Некоторые из них шуточные, но есть и такие, которые создавались для манипуляций общественным сознанием. Сейчас изготовление нового дипфейка занимает от силы пару дней, так что вскоре их может стать намного больше. |
| **Слайд 17** | 1. **Отсутствие отметок о времени публикации новости**. Даты публикации скрывается для того, чтобы максимально продлить «жизнь» фейковой новости. Такое сообщение будет казаться актуальным сколь угодно долго, пока не будет явно противоречить действительности. Забейте заголовок подозрительной новости и попробуйте поискать его, используя фильтры времени. Скажем, укажите прошлый год или прошлый месяц. Если вы найдёте аналогичную новость в архивах, то скорее всего это фейк. |
| **Слайд 18** | 1. **Отсутствие указания автора и источника**.   Многие фейки генерируются автоматизировано, поэтому никаких упоминаний ни автора, ни источника не остаётся. Тем не менее в последнее время фейковые новости выходят за авторством никому не известных журналистов — скорее всего их имена также случайны, и за ними не стоят реальные люди.  Попытайтесь найти новость или её авторов в мейнстрим-media. Прежде всего — в информационных агентствах.  Если же источники указаны, то попробуйте изучить их. Зачастую под видом копий, действующих официальных информационных ресурсов, совершают попытки скрыть реальные источники информации или их отсутствие. |
| **Слайд 19** | **Уголовная ответственность за распространение фейков о действиях ВС РФ**  5 марта 2022 года вступили в действия поправки в закон, в частности, введена статья 207.3 Уголовного кодекса РФ, которой усиливается ответственность за распространение фейков о действиях Вооруженных Сил РФ, а также за публичные призывы к введению санкций против России.  В соответствии с поправками публичное распространение под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных Сил РФ в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, будет наказываться штрафом от 700 тыс. до 1,5 млн рублей. Также возможно лишение свободы на срок до трех лет.  Если нарушение закона было совершено с использованием служебного положения, по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой‑либо социальной группы, то срок лишения свободы может составить до 10 лет.  Указанные выше деяния, если они повлекли тяжкие последствия, будут наказываться лишением свободы на срок от 10 до 15 лет.  Тем, кто был подвергнут административному наказанию за публичную дискредитацию ВС РФ, грозит штраф в размере от 100 тыс. до 300 тыс. рублей либо лишение свободы на срок до трех лет с отсутствием права занимать определенные должности или заниматься определенной деятельностью на тот же срок.  Также в соответствии с законом за призывы к введению санкций против РФ будет грозить штраф до 500 тыс. рублей либо лишение свободы на срок до трех лет со штрафом до 200 тыс. рублей.  **Внесены поправки были и в КоАП**. В соответствии с ними ответственность за публичные действия, направленные на дискредитацию использования Вооруженных Сил РФ в целях защиты интересов РФ и ее граждан, поддержания международного мира и безопасности, в том числе за публичные призывы к воспрепятствованию использования ВС РФ, составит: от 30 тыс. до 50 тыс. рублей — для граждан, от 100 тыс. до 200 тыс. рублей — для должностных лиц, от 300 тыс. до 500 тыс. рублей — для юридических лиц.  За аналогичные действия, если они сопровождались призывами к проведению несанкционированных публичных акций, грозит максимальный штраф до 100 тыс. рублей для граждан и до 1 млн рублей — для юрлиц.  За призывы к введению санкций против России штрафы составят до 50 тыс. рублей для граждан и до полумиллиона рублей — для юридических лиц. |