КАК БЕЗОПАСНО ВЕСТИ СЕБЯ В МЕДИАПРОСТРАНСТВЕ

Цель:

Рассмотреть основные аспекты безопасного поведения в цифровом пространстве.

Описание:

Данная лекция содержит в себе три раздела, посвященных кибератакам, фейкам и дипфейкам, популярным схемам интернет-мошенничества и безопасной работе с нейросетями. В ходе занятия разъясняются аспекты медиабезопасности и критического мышления.

Ключевые слова

Фейки, дипфейки, фишинг, вишинг, медиаугрозы, критическое мышление, правила медиабезопасности, мошеннические угрозы, кибератаки, методы социальной инженерии, нейросети

Презентация к лекции

2

Роль цифровой среды в жизни каждого человека возрастает. Для многих работа и учеба завязаны на активном использовании интернет-ресурсов. По последним данным технологической компании Mediascope, в среднем россиянин проводит в сети более 4,5 часов в день. Зачастую даже в качестве отдыха человек выбирает не отказ от телефона или компьютера, а просмотр контента, чтение статей, постов, новостей, общение с другими интернет-пользователями. По этим причинам отказаться от пребывания в информационном пространстве чрезмерно трудно, а для некоторых — просто невозможно.

3

Вопросы к аудитории

Вы когда-нибудь проверяли, сколько часов ежедневно проводите в цифровой среде?

Какому приложению или занятию в интернете вы посвящаете больше всего времени?

4

В этой лекции мы разберем, можно ли защитить себя от таких угроз, как киберпреступления, распространение деструктивного контента, фейки, мошенничество.

5

Сегодня в интернете появляется все больше информационных каналов, а, следовательно, и различных мнений и новостей. Количество цифровых каналов, блогов, сообществ растет — становится все труднее воспринимать публикуемый контент критически и перепроверять его на достоверность. Это логично, ведь чем больше людей принимает участие в общении, публикации контента, тем сложнее становится контролировать эту коммуникацию. Каждый из нас это остро ощутил в 2020 году во время пандемии COVID-19. Именно в это время распространялось большое количество непроверенной, зачастую ошибочной и наполненной эмоциями информации. В обществе нарастала напряженность, паника, отрицание действительности. Так произошло из-за большого количества фейков, публикуемых о вакцинации, причинах появления болезни, личных недовольствах и ошибочных умозаключениях со стороны людей, не имеющих медицинского образования.

6

Фейки — это недостоверная или искаженная информация, которая подается под видом правды и нуждается в перепроверке. Фейки опасны не только потому, что вводят людей в заблуждение. Распространение фейков

имеет непредсказуемые последствия, так как они могут выводить людей из состояния равновесия, подталкивать к беспорядкам и необдуманным поступкам, что впоследствии формирует социальную напряженность, конфликтность и способствует росту преступности. Также распространение фейков формирует недоверие общества по отношению к СМИ и чувство безысходности, так как зачастую каналы копируют друг у друга новости, следовательно, выявить правду становится все сложнее.

Начиная с 2022 года можно заметить большое количество фейков вокруг специальной военной операции на Украине, экономической ситуации в России, политики, госбезопасности, социально-значимых происшествий. Например, фейки о мобилизации, дефиците товаров, кризисе отдельных отраслей производства, снижении пенсий и социальных выплат. Все это направлено на дискредитацию образа России и Вооруженных сил Российской Федерации.

7

Сегодня каждому из нас **важно уметь отличать фейковую информацию от правдивой.** Для этого важно придерживаться нескольких правил:

1. Обращайте внимание на эмоциональный контекст публикации. Зачастую фейковые новости содержат излишнюю эмоциональность, «кричащие» заголовки, призывы к действию, отсутствие конкретики.
2. Ищите источник информации. Также проверьте, есть ли эта новость на сайтах официальных информационных издательств: РИА Новости, Lenta.ru, ТАСС, Интерфакс, Газета.ru и т. д.
3. Если к новости прикреплен снимок, попробуйте найти источники фотографии. Проверить источник можно через поиск по фото в сервисах «Яндекс», Google, а также на сайте TinEye, который показывает первоисточник фотографии и другие ресурсы, где она уже использовалась.
4. Обратитесь к сайтам проверки фактов. Возможно, эту новость уже опровергли. Если нет, вы можете направить новость на проверку. Например, существуют Международная ассоциация по проверке фактов (GFCN), разработанная информационным агентством ТАСС и АНО «Диалог Регионы», сайт «Лапша Медиа» от АНО «Диалог Регионы».
5. Проверяйте наличие ошибок. Если в новости приводятся статистические данные, ссылки на исследования, цитаты, следует перепроверить их подлинность. Наличие цифр и авторитетных фамилий делают иллюзию достоверности приводимой информации.
6. Оценивайте массовость новости. У фейков есть такая характеристика, как массовость, то есть максимально широкое распространение информации. Например, фейковую новость могут распространять с помощью ботов. Под такими постами будет большое количество комментариев и репостов.
7. Придавайте значение каналу распространения информации. Фейки чаще распространяются в социальных сетях и мессенджерах, чем в информационных агентствах. Официальные издания, такие как ТАСС, РИА Новости, Интерфакс и т. д., обязаны проверять новости и проводить фактчекинг.

8

Вопросы к аудитории

Вам часто приходится проверять новости на достоверность?

Каким информационным источникам вы доверяете?

9

Важно отметить, что за распространение фейков, согласно законодательству Российской Федерации, предусмотрена как административная, так и уголовная ответственность: части 9 и 10.1 статьи 13.15 КоАП РФ «Злоупотребление свободой массовой информации», статьи 207.1 и 207.2 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» и «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия» соответственно.

10

К фейкам относятся и **дипфейки** — сгенерированные картинки или видео, которые созданы при помощи наложения реального изображения, видео или голоса человека на какой-то другой материал. С помощью искусственного интеллекта и машинного обучения подменяется лицо, мимика, жесты, голос. Сегодня стало возможным генерировать дипфейки не только с политическими деятелями, знаменитостями, лидерами общественного мнения, но и с непубличными людьми.

11

Вопросы к аудитории

Как вы думаете, для чего могут использоваться дипфейки?

Случалось ли такое, что дипфейк был насколько реалистичен, что вы не смогли сразу это определить?

12

Технологии не стоят на месте, поэтому отличить дипфейк от реального фото или видео без специального анализа бывает трудно. Дипфейки могут использоваться в том числе мошенниками, чтобы убедить жертву в «реальности» ситуации. Например, происходили случаи, когда сотрудников организаций обманывали фальшивыми сгенерированными голосовыми сообщениями или видеозвонками от их руководителей. Несмотря на реалистичность дипфейков, их можно отличить по следующим признакам: резкие изменения интонации, неестественные движения и мимика, нерегулярное моргание, странное или темное освещение, нечеткие границы наложенного элемента,

нестабильность фона. Также распознать дипфейки помогут специальные приложения и онлайн-сервисы, которые легко найти в интернете. Среди них Forensically, Image Edited, Deepware, Microsoft Video Authenticator и т. д.

13

Вопрос к аудитории

Сегодня каждый из нас может попасться в эту ловушку. Представьте, что вам написал близкий человек с просьбой срочно занять определенную сумму денег. Как бы вы поступили?

14

Чтобы проверить, реальный ли человек обратился с просьбой, следует сделать несколько шагов. Во-первых, можно позвонить ему по телефону или написать через альтернативный канал связи, чтобы убедиться в реальности ситуации. Во-вторых, задайте человеку такой вопрос, ответ на который знаете только вы вдвоем. В-третьих, если вам звонят по видеосвязи, то можно попросить совершить какое-то действие (снять очки, поправить волосы, провести рукой перед лицом и др.).
Тогда сгенерированное изображение даст сбой.

15

Мы разобрали негативный пример использования искусственного интеллекта. Но есть и обратная сторона. Появилось множество нейросетей, которые могут мгновенно собирать и обрабатывать большое количество источников информации по определенному алгоритму и выдавать ответ на заданный вопрос. Большинство интернет-пользователей хотя бы раз в жизни использовали нейросети для решения задач. Нейросети и правда могут быть мощным инструментом для творчества и работы, но их использование требует внимательности. Ошибки в обращении с персональными или корпоративными данными могут обернуться утечками, продажами третьим лицам и их незаконным использованием, поскольку удаленные сервера искусственного интеллекта не всегда гарантируют конфиденциальность. Неправильное пользование нейросетью может привести и к получению недостоверной информации на запрос.

Обезопасить свои данные при работе с нейросетью можно следующими способами:
— Изучите политику конфиденциальности сервиса. Обратите внимание, есть ли в ней пункт об использовании данных и можно ли отменить эту опцию. В настройках Яндекса, например, можно ограничить передачу запросов для обучения искусственного интеллекта.
— При введении запроса обезличивайте данные. Формулируйте задачу так, чтобы не указывать персональную или корпоративную информацию.
— Перепроверяйте информацию, сгенерированную нейросетью и не доверяйте ей на 100% в вопросах, связанных с государственной историей (информация может искажаться), медициной (вы рискуете навредить себе, не проконсультировавшись с врачом) и по другим критически важным темам.
— Пользуйтесь только проверенными известными российскими сервисами вместо новых или неизвестных (YandexGPT, GigaChat, Шедеврум и пр.).

— Проверяйте ссылки сервисов искусственного интеллекта. Под видом известной платформы может скрываться фейковый сайт, ворующий пароли и платежные данные.

16

Вопросы к аудитории

Как вы думаете, развитие искусственного интеллекта скорее помогает или вредит образовательному процессу?

Как грамотно и без вреда использовать нейросети в своей жизни, учебе и работе?

17

Сегодня практически каждому из нас звонили или писали мошенники. За 2024 год по данным Сбера было выявлено, что мошенники осуществляют более шести миллионов звонков в сутки. Только в 2024 году у граждан России было похищено 27,5 миллиардов рублей. Это не один или два человека, которые звонят и похищают деньги, опустошают банковские счета. Речь идет о целых организациях — колл-центрах — с немалым количеством подготовленных людей, где каждый выполняет свою роль в преступной схеме.

Большинство таких колл-центров располагается на территории Украины: в Днепропетровске, Киеве, Львове, Одессе. Такие центры выявляют и в России, а их участников — задерживают, однако именно на Украине создана благоприятная среда для деятельности таких мошеннических организаций по ряду причин. Сотрудники мошеннических колл-центров сейчас пытаются скупать телефонные номера разных стран, первоочередно стран СНГ (Казахстана, Таджикистана и др.), в которых номера начинаются с привычных для россиян комбинаций «+79...».

Мошеннические атаки со стороны Украины происходят в рамках информационной войны для дестабилизации российского общества и поиска новых источников финансирования Вооруженных сил Украины, а также они могут стать началом вовлечения в террористическую деятельность.

18

Колл-центры используют такой метод социальной инженерии, как **вишинг.** Они звонят по телефону и давят на человеческие слабости (страх, наивность, доверчивость, незнание чего-либо и т. д.) для доступа к личным данным, аккаунтам или банковским счетам. У мошенников составлены целые сценарии по различным ситуациям для общения с жертвой атаки. Чем больше личных данных жертвы есть у мошенника, тем быстрее он может войти в доверие, как бы подтверждая подлинность своего звонка. Чаще всего мошенники представляются сотрудниками банков, в том числе Центрального банка, госслужб, операторов связи, техподдержки Госуслуг. Популярные легенды: *«с вашего счета пытаются снять или перевести деньги, обнаружена попытка взять на вас кредит», «срок действия вашей сим-карты заканчивается, необходимо*

ее продлить или актуализировать информацию, переподписать договор», «обнаружена попытка сменить номер телефона, привязанный к вашему аккаунту на Госуслугах». Главное в любой схеме, что человека вынуждают называть личные данные (ФИО, дату рождения, данные паспорта), данные банковских счетов (номер карты, срок действия, Код CVV/CVC), код из СМС (для входа в личный кабинет Госуслуг, оператора мобильной связи и т. д.).

19

Еще один метод, который используют мошенники — **фишинг.** В этом случае на номер телефона, адрес электронной почты, в сообщения аккаунта в социальных сетях или мессенджерах отправляют ссылку на фишинговый сайт. Легенды могут быть разные: выигрыш в конкурсе, реклама об уникальных скидках, уведомление об обнаружении попытки взлома ваших аккаунтов, подозрительной активности, о том, что ваши личные данные на сервисе необходимо актуализировать, предложения получить отсрочку от мобилизации, любые «официальные уведомления» (повестки в военкомат, обвинения в совершении преступления), ссылка на созданную нейросеть или бота, которые «помогут» написать диплом и домашние задания и так далее. Помните, что переходить по ссылкам с незнакомых адресов нельзя! Регулярно проверяйте свое устройство через антивирусное ПО на наличие угроз.

20

Мошенники постоянно актуализируют свои схемы обмана. Помимо уже рассмотренных вишинга и фишинга, которые основываются на человеческих слабостях, существует еще множество махинаций. Например, случаи мошенничества, которые реализуются через разные сервисы для обмена сообщениями (WhatsApp, Telegram), зафиксированы и в национальном мессенджере MAX. Злоумышленники представляются сотрудниками платформы и склоняют жертву к регистрации аккаунта, просят назвать код из СМС (который на самом деле является кодом для входа в Госуслуги) и получают доступ к личным данным и банковским счетам жертвы. После, жертве звонят второй раз и сообщают, что аккаунт на Госуслугах взломан, запугивая возможными кредитами или финансированием экстремизма или терроризма. Обезопасить свои финансы предлагают переводом денег на «безопасный счет» или самостоятельным снятием наличных со счета и передачи их «курьеру».

21

Еще один способ обмана — бесконтактная кража денег через NFC–технологию беспроводной передачи данных малого радиуса действия. NFC есть в большинстве смартфонов, но не во всех. С помощью технологии NFC мы можем бесконтактно проводить оплату в магазинах, передавать небольшие файлы с одного устройства на другое, если они находятся близко друг к другу, быстро подключать к телефону беспроводные устройства, такие как наушники или колонки. Мошенники звонят, представляясь работниками банка или правоохранительных органов, говорят о взломе аккаунта на Госуслугах и подозрительной финансовой активности. Чтобы обезопасить счета, предлагают скачать на телефон специальное приложение. После скачивания, просят взять свою банковскую карту, приложить к телефону и ввести PIN-код. Данные карты считываются с помощью технологии NFC и передаются мошенникам. В этот момент на устройстве мошенника открыто такое же приложение, он находится возле банкомата, прикладывает устройство к терминалу, вводит PIN-код и получает доступ к счету. Такой способ обмана имеет разные схемы, но суть всегда одинаковая:

программа, которую вынуждают скачать на смартфон, на самом деле перенаправляет NFC-сигнал на устройство мошенника. Этот сигнал банкомат считывает, как карту, после чего злоумышленник забирает себе денежные средства. Помните: нельзя устанавливать приложения из файлов, вложений, ссылок от непроверенных источников!

Контролировать устройство жертвы мошенники научились и другим способом. Они могут представляться работниками медицинских организаций или государственных служб и склонять к установке приложения для оплаты коммунальных услуг, записи к врачу, оформления льгот, социальных выплат. Предлогом для скачивания могут выступать любые бытовые потребности человека.

22

По понятным причинам пожилые люди являются легкой мишенью для мошеннических атак. Злоумышленники, которые звонят пенсионерам, представляются работниками Министерства здравоохранения, социальных служб и фондов и предлагают бесплатную путевку в санаторий. Под этим предлогом мошенники запрашивают личные данные и код из СМС. Затем жертве поступает второй звонок от «правоохранительных органов» со срочным предложением «обезопасить деньги», так как были зафиксированы подозрительные или незаконные финансовые махинации. Как вы можете обезопасить своих родных? Поговорите с ними, расскажите про возможные схемы мошенничества, про то, что нельзя никому сообщать свои личные данные, код из СМС, пароли, нельзя верить бесплатным предложениям, выигрышам, персональным скидкам и тем более переводить деньги незнакомцам под любыми предлогами.

Сегодня очень популярны маркетплейсы (Ozon, Wildberries, Яндекс.Маркет и т. д.). С ними мошенники также связали свои схемы. Например, звонки от «работников маркетплейсов» с уведомлением о посылке, которую вы не заказывали. Сообщается, что заказ уже оплачен, нужно лишь согласовать время доставки. Уговаривают, что посылка ценная и жалко будет ее потерять. Чтобы подтвердить получение, просят сообщить код из СМС, который на самом деле является кодом для авторизации в Госуслугах. Далее действуют по уже описанной ранее схеме. Помните, что коды из СМС запрашивают только мошенники!

23

Вопрос к аудитории

Что необходимо сделать, если человек все-таки попался на мошеннические уловки?

24

Алгоритм действий, если человек стал жертвой мошеннической атаки, зависит от конкретного случая. **Есть несколько универсальных советов:**
— заблокируйте карту и позвоните на горячую линию банка. Удостоверьтесь, что ваши сбережения в сохранности. Проверьте, оформлены ли на ваше имя кредиты. На Госуслугах есть возможность проверить свою кредитную историю («узнать свое БКИ через Цифрового ассистента»);

— измените пароль от аккаунта, на который производилась атака, поставьте двухфакторную аутентификацию, обратитесь в службу поддержки платформы.
Если взломали приложение оператора связи, проверьте, не установлена ли переадресация на чужой номер телефона;
— звоните в банк, которым пользуетесь, в полицию или посетите их ближайшие отделения. Через портал Госуслуги можно обезопасить себя от дистанционного кредитования («установление запрета на получение кредита»). Эта услуга запрещает оформлять на ваше имя кредиты без вашего очного присутствия.

25

С помощью методов социальной инженерии, программных или аппаратных уязвимостей происходят кибератаки не только на отдельных людей, но и на целые компании.
Об этом особенно важно помнить сотрудникам крупных компаний. Например, летом 2025 года хакеры взломали систему «Аэрофлота». Десятки рейсов были отменены или перенесены, а терабайты личных данных клиентов смогли попасть в руки мошенников. Хакеры заявили, что находились в системах «Аэрофлота» с 2024 года.
Так, цели кибератак, в отличие от мошенничества, могут заключаться не только в краже денежных средств или личных данных. **Кибератака** — это попытка получить несанкционированный доступ к информационной системе или оборудованию компании для того, чтобы нарушить их работоспособность, похитить, изменить или уничтожить данные, шпионить за организациями на протяжении долгого времени.

Большинство способов кибератак мы с вами рассмотрели (заражение системы вредоносным ПО, методы фишинга и вишинга, дипфейки). Помимо этого, киберпреступники постоянно испытывают системы и оборудование, которые хотят атаковать, на уязвимости, ведь чтобы взломать целую систему нужно найти всего лишь одно слабое место. Кроме того, преступники могут использовать сразу несколько методов, чтобы повысить свои шансы на успех.

Крупные компании уделяют особое внимание своей информационной системе и постоянно инвестируют ресурсы в обеспечение кибербезопасности.
Для этого создаются специальные центры или отделы, которые регулярно проверяют оборудование, ищут проблемные места системы. Несмотря на это, ни одна компания не может быть на 100% застрахована от возможных рисков.

26

Как защититься от мошеннических угроз?
— В некоторые браузеры встроены антифишинговые фильтры, которые созданы, чтобы проверять сайты или входящие адреса электронной почты и предупреждать пользователя о потенциальной опасности.
— Если вам пишет незнакомый человек или сообщение приходит с незнакомого адреса, то никогда не переходите по указанным ссылкам и не скачивайте прикрепленные файлы.
— Запомните, что только мошенники запрашивают по телефону ваши личные данные. Ни один сотрудник госслужбы, отделов безопасности, технической поддержки никогда не будет запрашивать конфиденциальную информацию или пытаться решить с вами важные вопросы по телефону или через мессенджеры, электронную почту.
Чтобы перестраховаться, позвоните по официальному номеру организации или посетите ее ближайшее отделение для уточнения информации.

— В используемых приложениях, где есть такая функция, установите двухфакторную аутентификацию. Например, ее можно установить в сервисах «Яндекс», «ВКонтакте», «Госуслуги», Telegram. Так, мошенники не смогут войти в ваши аккаунты, даже если уже узнали логин и пароль.
— Установите на ваше устройство антивирусное ПО. Обновляйте его, когда появляются новые дополнения.
— Не отвечайте на незнакомые номера. Если вы ответили, то не называйте никаких личных данных, не верьте предоставляемым документам или названных должностям, перепроверяйте информацию в официальных источниках. Лучше всего сразу завершить разговор.
— В приложениях некоторых операторов связи есть функция распознавания телефонных номеров. Активируйте ее. Тогда во время входящего звонка оператор связи уведомит вас, что этот звонок является подозрительным.

27

Вопросы к аудитории

Как вы думаете, какие категории людей наиболее подвержены мошенническим уловкам?

Как еще вы можете помочь своими родным не попасться на «крючки» мошенников?

28

Сегодня действительно важно развивать критическое мышление, потому что оно помогает нам выявлять фейки, не поддаваться на уловки мошенников и в целом сохранять спокойствие в непростые времена. Главный принцип критики — ставить под сомнение получаемую информацию и проверять ее. Относиться к информации критически не значит категорически. Дело не в том, чтобы отрицать любую входящую новость, а в том, чтобы не позволить новости или произошедшему событию вывести вас или окружающих из состояния эмоционального равновесия.

29

Вопросы к аудитории

Как лично вы понимаете, что такое критическое мышление?

Как его можно развивать?

30

Мы уже обсудили, как реагировать на фейковую информацию, киберугрозы и мошенничество. Это все можно назвать частью негатива в медиапространстве. **Как правильно реагировать на негатив, который может встретиться в информационном поле?**

— Не отвечайте на угрозы или неконструктивную критику. Тот, кто распространяет негатив, ждет любой реакции. Если игнорировать такие проявления, то человек поймет, что это ни к чему не приводит и с большой вероятностью прекратит подобное поведение.

— Сохраняйте спокойствие. Если какое-то неоднозначное или печальное событие уже произошло, то раздраженность, паника и страх не сделают лучше вам или окружающим. Когда человек излишне эмоционален, то его способность критически оценивать ситуацию снижается.

— Не распространяйте информацию среди знакомых и друзей, пока не удостоверитесь, что это не фейк. Так вы не будете повышать уровень напряженности и паники среди людей.

— Ограничьте свое присутствие в медиапространстве хотя бы во время отдыха, чтобы минимизировать деструктивное воздействие онлайн-среды.

— Подавайте жалобы, если считаете увиденный материал вредным для окружающих. Если заметили оскорбительную или фейковую информацию, то пожалуйтесь на нее с помощью специальной кнопки или через администрацию онлайн-площадки.

— Обратитесь в Роскомнадзор, если заметили, что чьи-то личные данные разместили публично.

— Если вам угрожают в интернете или оскорбляют вас, то соберите доказательства в виде скриншотов и незамедлительно обратитесь в местное отделение полиции.

31

Критическое мышление является одной из составляющих **медиабезопасности** — комплекса знаний и мер, которые стоит применять для защиты от вредного информационного воздействия и для комфортного пребывания в интернет-пространстве. Медиабезопасность стала неотъемлемой частью современности, ведь цифровые технологии активно внедряются во все сферы нашей жизни. **Рассмотрим ключевые правила медиабезопасности:**

32

— Перепроверяйте информацию. Распространение искаженных, намеренно ложных данных происходит по разным причинам и от различных источников: в современный век информационных противоборств необходимо всегда помнить об этом. Не действуйте, пока не убедитесь в достоверности полученной информации.

— Игнорируйте подозрительные рассылки и звонки. Это помогает защититься от мошенников и предотвращает утечку личной информации.

— Учитесь распознавать психологическое давление на себя и тренируйте критическое мышление. Если кто-то торопит вас, пугает или вызывает чувство вины, это может быть попыткой манипуляции. В таких ситуациях лучше брать паузу и задавать себе вопрос: не пытаются ли вас побудить совершить действия против вашей воли? Злоумышленники нередко используют эмоциональное воздействие для управления поведением человека.

— Устанавливайте везде разные, но надежные пароли. Надежный пароль состоит минимум из 12 знаков как строчных, так и прописных латинских символов, а также цифр. Лучше всего периодически менять пароли примерно раз в 3 месяца. В пароле избегайте дату рождения, имя, копирование логина, примитивные комбинации по типу «1234qwerty»

или «password1» и не записывайте пароль в заметки телефона.
— Проверьте конфиденциальность в социальных сетях. Разрешите видеть ваши личные данные только друзьям и не указывайте в личных профилях избыточную информацию о себе.
— Не отправляйте фото своих документов через социальные сети и мессенджеры.
— Не сохраняйте свои пароли в браузере, которым пользуетесь.
— Старайтесь не подключаться к открытым точкам Wi-Fi, например, в аэропортах, ресторанах, отелях, на вокзалах.
— Выключайте Bluetooth и Wi-Fi, когда не пользуетесь ими.
— В настройках телефона контролируйте разрешения приложений (например, отслеживание вашего местоположения, доступ к камере, микрофону).
— Не сканируйте неизвестные QR-коды, особенно те, которые расположены в общественных местах. Они могут содержать вирусные ПО и фишинговые ссылки.
— Регулярно обновляйте приложения и антивирусные ПО. Удаляйте приложения, которыми уже не пользуетесь.

33

Вопросы к аудитории

Как бы вы в целом определили свой уровень медиабезопасности?

По вашему мнению, человек может самостоятельно повышать этот уровень?

В рамках этой лекции мы рассмотрели основные аспекты безопасного поведения в цифровом пространстве. Информационные технологии будут только развиваться и открывать новые возможности как для доброжелательных интернет-пользователей, так и для злоумышленников. Государство в свою очередь вносит огромный вклад в противодействие киберугрозам и развитие медиабезопасности граждан, но, несмотря на это, каждый человек сам несет ответственность за свою жизнь. Чтобы защититься от деструктивного влияния, следуйте правилам медиабезопасности, которые были рассмотрены в лекции. Эти правила достаточно простые, поэтому внедрить их в повседневность и обезопасить свое будущее сможет каждый. Если вы попали в непростую ситуацию, помните: всегда есть специалисты, которые готовы вам помочь. Не бойтесь обращаться к ним и к окружающим вас людям.

34

Уважаемые слушатели! Мы подошли к финалу сегодняшней лекции.
Надеюсь, материал оказался полезным и интересным, позволил вам расширить кругозор и глубже разобраться в изучаемой теме. Если у вас остались какие-либо вопросы, мы всегда готовы их обсудить, в том числе на последующих мероприятиях.

Закрепление материала

Для развития практических навыков противодействия киберугрозам рекомендуем провести тренинг «Вербовка: как противостоять манипуляциям» из II Сборника сценариев профилактических мероприятий.

Тренинг «Вербовка: как противостоять манипуляциям»

Для обсуждения дополнительных вопросов формирования медиабезопасности можно воспользоваться материалами АНО «Интернет без угроз» и сообщества «Здесь медиабезопасно».

АНО «Интернет без угроз»

«Здесь медиабезопасно»

Заметки по материалу