

Министерство образования Тульской области

**Государственное профессиональное образовательное учреждение
Тульской области «Донской политехнический колледж»**

**Методическая разработка единого кураторского часа
«Информационная безопасность»**

Автор:

С.М. Гвоздев, преподаватель ГПОУ ТО «ДПК»

2023 г.

Лист согласования:

Автор разработки: С.М. Гвоздев, преподаватель ГПОУ ТО «ДПК»

Рецензенты:

Ишутина О.В., заведующий методическим кабинетом ГПОУ ТО «ДПК»;

Евтехова О.А., заместитель директора по учебной и научно-методической работе ГПОУ ТО «ДПК»;

Панченко Т.А., заместитель директора по учебно-методической работе ГПОУ ТО «ДПК»;

Чупкина Л.А., заместитель директора по воспитательной работе ГПОУ ТО «ДПК».

Разработка представляет собой тематическое занятие и может быть использована для формирования культуры безопасного и осознанного пребывания студентов в цифровом пространстве, а также повышения уровня цифровой грамотности.

СОГЛАСОВАНО

на заседании ПЦК дисциплин профессионального цикла отделения «Информационные системы и кибербезопасность»

Протокол № 02
от «02» 10. 2023г.

Председатель ПЦК С.М. Гвоздев

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Тематическое направление: Информационная безопасность.

Тема занятия: Защита данных и медиабезопасность.

Актуальность: Необходимость защищать конфиденциальность и целостность информации в условиях растущих киберугроз, распространения дезинформации и регулирования сбора данных.

Цель занятия: формирование культуры безопасного и осознанного пребывания студентов в цифровом пространстве, а также повышение уровня цифровой грамотности.

Задачи занятия:

- познакомить студентов с основами правового регулирования в сфере информационной безопасности в Российской Федерации;
- рассмотреть меры и уровни защиты личной информации в интернете;
- познакомить студентов с правилами сетевой культуры и сетевого этикета в глобальных медиа;
- повысить уровень знаний о медиабезопасности в условиях информационных войн.

Планируемые результаты:

студенты должны знать

- основы правового регулирования в сфере информационной безопасности в Российской Федерации;
- меры и уровни защиты личной информации в Интернете;
- правила сетевой культуры и сетевого этикета в глобальных медиа;
- важность медиабезопасности в условиях информационных войн.

Форма проведения занятия: эвристическая беседа.

Педагогические технологии: информационно-коммуникационная технология, игровые технологии, здоровьесберегающие технологии, проблемное обучение.

Длительность занятия: 55 минут.

Ресурсное обеспечение: персональный компьютер, интерактивная доска, сценарий, презентация.

Ход занятия:

Введение (5 минут)

СЛАЙД 1

СЛАЙД 2

Преподаватель:

Приветствие студентов и краткое введение в тему занятия. Объявление целей и ожидаемых результатов.

Студенты:

Мотивация: почему важно обсуждать медиабезопасность и интернет-угрозы?

Правовое регулирование информационной безопасности в России (10 минут)

СЛАЙД 3

Преподаватель:

Краткий обзор законодательных актов о защите информации и интернет-коммуникаций в Российской Федерации. Обсуждение основных норм и ответственности за нарушения.

Меры и уровни защиты личной информации в Интернете (10 минут)

СЛАЙД 4

Преподаватель:

Понятие личной информации и её значимость. Обзор основных методов и средств защиты личных данных: пароли, двухфакторная аутентификация, шифрование и др.

СЛАЙД 5

Демонстрация практических советов по безопасности в сети.

Сетевая культура и сетевой этикет (10 минут)

СЛАЙД 6

Преподаватель:

Понятие сетевой культуры и сетевого этикета. Обсуждение правил вежливого общения в интернете и в социальных сетях.

Студенты:

СЛАЙДЫ 7-15

Ролевая игра:

Разбор и обсуждение ситуаций, требующих соблюдения сетевого этикета. Студенты разделяются на 5 команд по 5 человек в каждой, в 4-ех командах выбирается капитан, который после небольшого совещания с командой отвечает на предлагаемую ситуацию. 5-я команда сопоставляет ответы 4-ех команд и выявляет победителя. Так же капитаны команд могут оспорить решение 5-ой команды, но при этом должны привести веские доводы в правоту своего ответа.

(на слайдах последовательно выведены 4 ситуации с возможными вариантами решений).

Медиабезопасность и информационные войны (10 минут)

СЛАЙД 16

Преподаватель:

Объяснение понятия медиабезопасности и её важности в условиях информационных войн. Анализ примеров фейковых новостей и манипуляций в медиа. Обсуждение стратегий определения достоверных источников информации (Приложение 1).

Обсуждение и заключение (10 минут)

СЛАЙДЫ 17-18

Преподаватель и студенты:

Ответы на вопросы студентов и обсуждение впечатлений от занятия. Подведение итогов, подчеркивая важность обучения информационной

безопасности и сетевой культуры. Выдача дополнительных ресурсов для самостоятельного изучения.

Вопросы:

- Какие основные угрозы для безопасности данных существуют в современном цифровом мире?
- Как можно защитить свои личные данные от киберпреступников и хакеров?
- Какие принципы безопасности следует соблюдать при использовании общественных Wi-Fi-сетей?
- Как различить настоящие новости от фейковых новостей в социальных медиа?
- Какие меры безопасности следует принимать при совершении онлайн-покупок?
- Каковы основные аспекты законодательства о защите данных и конфиденциальности?
- Как обезопасить свои аккаунты в социальных сетях от взлома?
- Что такое двухфакторная аутентификация и как она помогает укрепить безопасность данных?
- Какие роли и обязанности имеют организации в области защиты данных своих клиентов?
- Какие технические средства и программное обеспечение помогают обеспечить медиабезопасность при использовании интернета?

СЛАЙД 19

Индивидуальное задание: "Исследование цифровых следов"

Цель: развить навыки анализа цифровых следов и осознанности в соблюдении медиабезопасности в сети.

Инструкция:

Исследование цифровых следов: Найдите в сети (в Интернете) свой цифровой след. Это могут быть: ваш профиль в социальных сетях, комментарии, фотографии, посты и т.д. Обратите внимание на то, какая

информация о вас доступна публично и какие могут быть потенциальные угрозы для вашей медиабезопасности.

Анализ цифровых следов: Составьте краткий отчет о том, что вы обнаружили в своих цифровых следах. Опишите, какие данные о вас доступны, и насколько они могут быть конфиденциальными. Сделайте выводы о том, насколько хорошо вы соблюдаете медиабезопасность в интернете и какие шаги могли бы предпринять для улучшения своей цифровой безопасности.

План действий: Опишите план действий по улучшению своей медиабезопасности. Какие шаги вы предпримете, чтобы сделать свои цифровые следы более защищенными? Включите в план использование паролей, двухфакторной аутентификации, обновление настроек конфиденциальности и т.д.

Рефлексия: Напишите небольшое эссе о том, что вы узнали из этого исследования и какие уроки извлекли для себя. Обсудите свои новые навыки и осознанность в соблюдении медиабезопасности.

Медиабезопасность и информационные войны

Объяснение понятия медиабезопасности и её важности в условиях информационных войн.

В современном информационном обществе, находящемся в плотной связи с технологическим прогрессом и интернетом, одной из самых актуальных проблем стала медиабезопасность. Это понятие охватывает комплекс мер и принципов, направленных на обеспечение безопасного использования медиаинструментов, информационных и коммуникационных технологий.

Медиабезопасность – это неотъемлемая часть информационной безопасности, которая состоит в защите от негативных воздействий, связанных с процессом передачи и получения информации. В условиях информационных войн, когда манипуляции информацией становятся одним из ключевых орудий борьбы, медиабезопасность становится особенно важной.

Вооруженные конфликты не только происходят на поле боя, но и проливаются на информационное пространство. В руках правительств, группировок и отдельных лиц оказывается немало мощных инструментов манипуляции мнениями и формирования определенных представлений у широкой аудитории. Это может привести к нарушению стабильности и единства общества, повышению психологической напряженности и разрушению доверия властям и международным отношениям.

Медиабезопасность в условиях информационных войн становится оружием противостояния. Она включает в себя такие составляющие, как защита информационной инфраструктуры, контроль за деятельностью СМИ и социальных сетей, противодействие дезинформации и фейковым новостям, а также развитие критического мышления у граждан.

Защита информационной инфраструктуры – это процесс обеспечения безопасности информационных систем и сетей.

В условиях информационных войн все чаще осуществляются хакерские атаки, целью которых является повреждение или уничтожение информационных систем противника или их захват. Для предотвращения таких атак необходимо постоянное обновление систем защиты, а также развитие навыков кибербезопасности у пользователей.

Контроль за деятельностью СМИ и социальных сетей – это механизм, позволяющий предотвращать распространение ложной информации или пропагандистских материалов, которые могут вызвать конфликтную ситуацию или даже нарушить национальное единство. Ведется работа по созданию алгоритмов и программных решений, которые позволят автоматизировать процесс фильтрации контента и определения неправдивой информации.

Анализ примеров фейковых новостей и манипуляций в медиа.

Пример 1: Фейковая новость о здоровье продукта

Заголовок: "Исследование доказывает, что шоколад помогает похудеть!"

Этот пример фейковой новости основан на манипуляции информацией о здоровье продукта. В статье может быть утверждено, что новые исследования выявили связь между потреблением шоколада и снижением веса, что является весьма сомнительным. Такая манипуляция может ввести читателей в заблуждение и привести к неправильным решениям в их диете.

Пример 2: Манипуляции с фотографиями и комментариями

Заголовок: "Лидер оппозиции оскорбил министра: скандал на высшем уровне!"

В этом примере могут использоваться фотографии лидера оппозиции и министра, на которых они будут выглядеть, как будто один из них оскорбляет другого. Комментарии к фотографии также могут содержать информацию, которая подталкивает читателя к тому, чтобы считать, что представитель оппозиции совершил неуважительные действия по отношению к министру. Такая манипуляция может вызвать конфликтные ситуации и

негативное отношение общественности к определенным политическим фигурам.

Обсуждение стратегий определения достоверных источников информации.

Первая стратегия - проверка адекватности источника. При определении достоверности источника следует анализировать, насколько объективно и нейтрально он представляет информацию. Если источник предлагает слишком сенсационные и однобокие утверждения, то это может быть признаком его недостоверности. Также следует обращать внимание на профессионализм автора, его квалификацию и опыт в области, о которой он пишет.

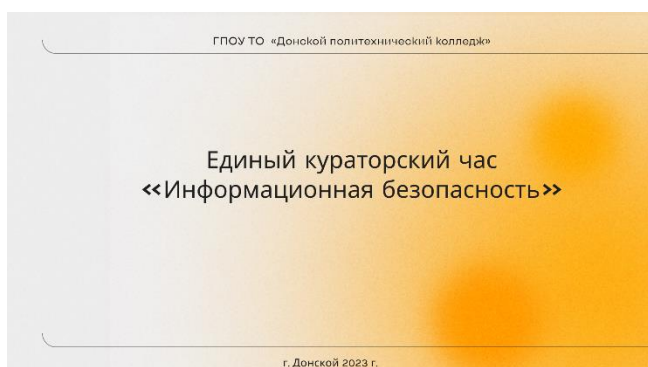
Вторая стратегия - проверка фактов и данных. Достоверный источник информации должен предоставлять проверяемые факты, а не сколько-нибудь утверждений. Проверка данных, приведенных в статье или исследовании, позволяет оценить их надежность и правдоподобность. При этом, следует убедиться, что источник ссылается на другие исследования или авторитетных экспертов, подтверждающих представленные данные.

Третья стратегия - сравнение с другими источниками. Если информация предоставлена только одним источником, то это не является достаточной основой для суждений о ее достоверности. Важно провести дополнительные исследования и найти другие источники, подтверждающие или опровергающие данную информацию. Сравнение мнений и выводов разных экспертов помогает более объективно оценить достоверность источника.

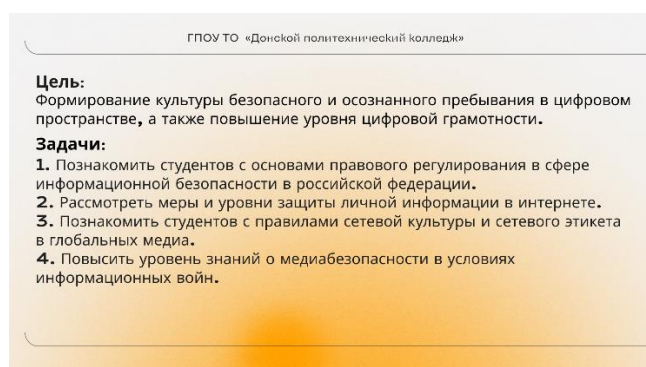
Четвертая стратегия - применение критического мышления. Всегда следует задавать себе вопросы о целях и интересах автора информации. Мотивы источника могут исказить представление об объекте исследования, поэтому важно осознавать их и учитывать в процессе оценки достоверности. Критическое мышление помогает относиться к информации с определенной долей скептицизма и осознания ее возможных проблем и ограничений.

В заключение, определение достоверных источников информации требует применения нескольких стратегий. Анализ адекватности источника, проверка фактов и данных, сравнение с другими источниками, а также критическое мышление - все эти подходы помогают отделить правдивую информацию от ложной. Умение определять достоверные источники является важной компетенцией в современном мире информации.

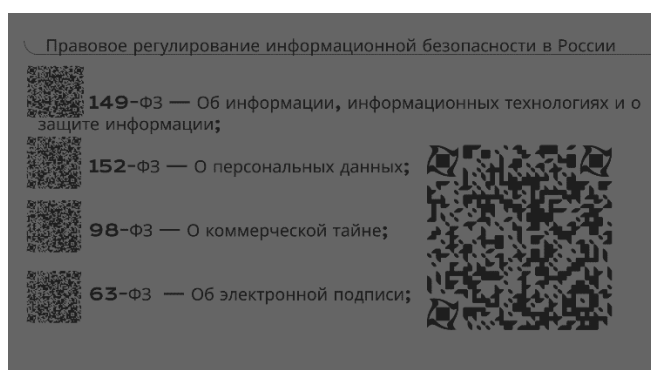
Презентационный материал



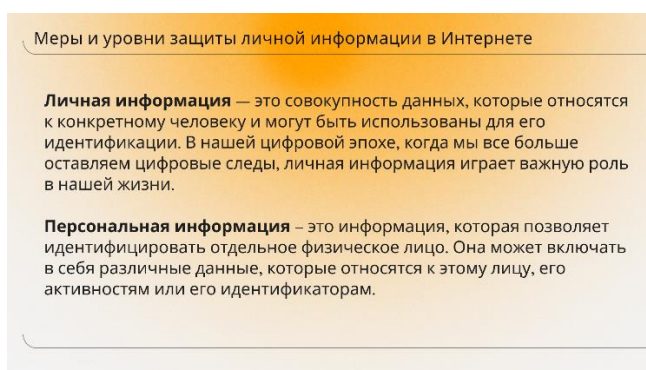
1



2



3



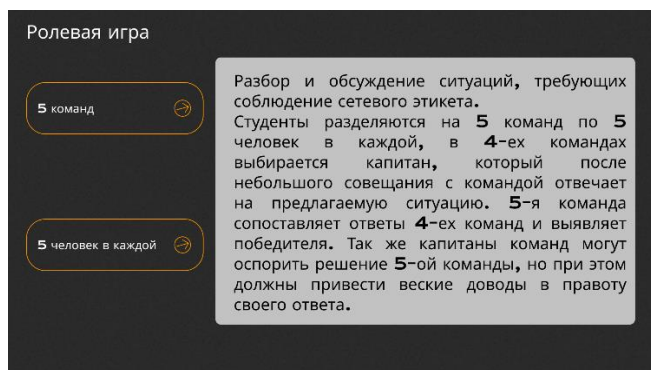
4



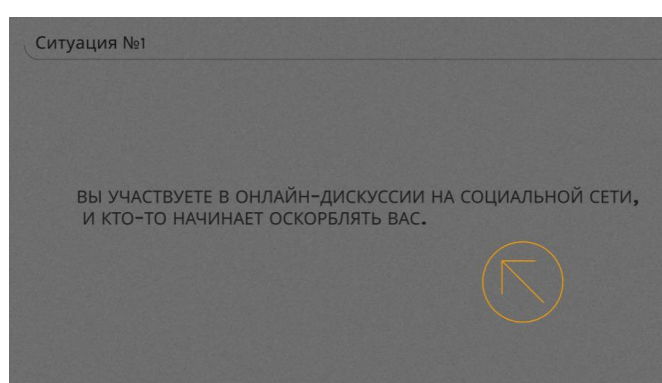
5



6




7



8

Ответ




ПОПРОБУЙТЕ ОСТАТЬСЯ СПОКОЙНЫМ И ВЕЖЛИВЫМ, ИГНОРИРУЙТЕ ОСКОРБЛЕНИЯ ИЛИ ОТВЕЬТЕ УВАЖИТЕЛЬНО, ПЫТАЯСЬ РАЗРЕШИТЬ КОНФЛИКТ. ЕСЛИ ЭТО НЕ ПОМОГАЕТ, СООБЩИТЕ АДМИНИСТРАТОРУ ИЛИ МОДЕРАТОРУ О НАРУШЕНИИ ПРАВИЛ

9


Ситуация №2

ВАМ НЕОБХОДИМО ОТПРАВИТЬ ПИСЬМО ИЛИ ЭЛЕКТРОННОЕ СООБЩЕНИЕ ПРОФЕССИОНАЛЬНОГО ХАРАКТЕРА



10

Ответ




СФОРМУЛИРУЙТЕ СООБЩЕНИЕ ВЕЖЛИВО И ЯСНО, ИСПОЛЗУЙТЕ ФОРМАЛЬНОЕ ОБРАЩЕНИЕ И ПРОЯВЛЯЙТЕ УВАЖЕНИЕ К ПОЛУЧАТЕЛЮ. ПРОВЕРЬТЕ ТЕКСТ НА ГРАММАТИЧЕСКИЕ И ОРФОГРАФИЧЕСКИЕ ОШИБКИ ПЕРЕД ОТПРАВКОЙ.

11


Ситуация №3

ВЫ ПРИНИМАЕТЕ УЧАСТИЕ В ОНЛАЙН-ФОРУМЕ ИЛИ БЛОГЕ, И ХОТИТЕ ВЫРАЗИТЬ СВОЕ МНЕНИЕ О СПОРНОЙ ТЕМЕ.



12

Ответ




ПОСТАРАЙТЕСЬ БЫТЬ КОНСТРУКТИВНЫМ УВАЖИТЕЛНЫМ, ПОДДЕРЖИВАЙТЕ СВОИ АРГУМЕНТЫ ФАКТАМИ И ДОКАЗАТЕЛЬСТВАМИ, ИЗБЕГАЙТЕ ИСПОЛЬЗОВАНИЯ ОСКОРБЛЕНИЙ ИЛИ АГРЕССИИ, ГОТОВЬТЕСЬ К ВОЗМОЖНОЙ ДИСКУССИИ, НО НЕ ПОЗВОЛЯЙТЕ ЕЙ ПЕРЕРАСТИ В ОСКОРБЛЕНИЯ.

13


Ситуация №4

ВЫ ПОЛЬЗУЕТЕСЬ ОБЩЕДОСТУПНОЙ **WI-FI** СЕТЬЮ В КАФЕ ИЛИ АЭРОПОРТУ.



14

Ответ




УБЕДИТЕСЬ, ЧТО ВЫ СОБЛЮДАЕТЕ ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЕТИ, НЕ ВМЕШИВАЙТЕСЬ В РАБОТУ СЕТИ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ И НЕ СКАЧИВАЙТЕ НЕЛЕГАЛЬНЫЙ КОНТЕНТ, ЕСЛИ СЕТЬ ТРЕБУЕТ ПАРОЛЬ, ПОЛУЧИТЕ ЕГО У СОТРУДНИКОВ ЗАВЕДЕНИЯ

15

Медиабезопасность и информационные войны

Информационные войны преследуют несколько целей:

1. Нанесение ущерба критически важным структурам государства;
2. Подрыв политической, социальной, экономической систем;
3. Массированная психологическая обработка населения для дестабилизации государства и принуждения его руководства к принятию решений в интересах противоположной стороны.



16

Вопросы:

1. Какие основные угрозы для безопасности данных существуют в современном цифровом мире?
2. Как можно защитить свои личные данные от киберпреступников и хакеров?
3. Какие принципы безопасности следует соблюдать при использовании общественных Wi-Fi-сетей?
4. Как различить настоящие новости от фейковых новостей в социальных медиа?
5. Какие меры безопасности следует принимать при совершении онлайн-покупок?

17

Вопросы:

6. Каковы основные аспекты законодательства о защите данных и конфиденциальности?
7. Как обезопасить свои аккаунты в социальных сетях от взлома?
8. Что такое двухфакторная аутентификация и как она помогает укрепить безопасность данных?
9. Какие роли и обязанности имеют организации в области защиты данных своих клиентов?
10. Какие технические средства и программное обеспечение помогают обеспечить медиабезопасность при использовании интернета?

18

Индивидуальное задание: "Исследование цифровых следов"

Исследование цифровых следов: найдите в сети (в Интернете) свой цифровой след. Это могут быть: ваш профиль в социальных сетях, комментарии, фотографии, посты и т.д. Обратите внимание на то, какая информация о вас доступна публично и какие могут быть потенциальные угрозы для вашей медиабезопасности.

Анализ цифровых следов: Составьте краткий отчет о том, что вы обнаружили в своих цифровых следах. Опишите, какие данные о вас доступны, и насколько они могут быть конфиденциальными. Сделайте выводы о том, насколько хорошо вы соблюдаете медиабезопасность в интернете и какие шаги могли бы предпринять для улучшения своей цифровой безопасности.



19