Муниципальное автономное общеобразовательное учреждение

средняя общеобразовательная школа №65 города Тюмени

|  |  |  |
| --- | --- | --- |
| РАССМОТРЕНО |  | УТВЕРЖДЕНО |
| на заседании методического совета Протокол №  от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_г. |  | приказом директора  МАОУ СОШ№65  города Тюмени  от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г №\_\_\_\_\_ |

# Дополнительная общеобразовательная общеразвивающая программа

# по направлению «Кибергигиена и работа с большими данными»

# Кибергигиена 2.0

Возраст обучающихся: 11—17 лет Срок реализации программы: 1 год Количество часов в год: 72

Тюмень 2023

**Пояснительная записка**

Дополнительная общеразвивающая программа «Кибербезопасность» является программой *технической* направленности. Программа ориентирована на обучение детей среднего и старшего школьного возраста от 11 до 17 лет в течение 1 года.

Данная программа способствует формированию навыков безопасной деятельности в современном информационном пространстве.

Программа реализуется в центре цифрового образования детей «IT-куб» МАОУ СОШ№65 города Тюмени.

Кибергигиена представляет собой набор действий, выполняемых пользователями компьютеров и других устройств для повышения сетевой безопасности и обеспечения работоспособности системы. Кибергигиена – это образ мышления и привычки с фокусом на безопасность, помогающие пользователям и организациям снизить количество нарушений в интернете. Основополагающий принцип кибергигиены – войти в повседневную жизнь.

Нормативная база

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)

2. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 31.07.2020) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2020)

3. Паспорт национального проекта «Образование» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 N 16)

4. Государственная программа Российской Федерации «Развитие образования» (Утверждена Постановлением Правительства РФ от 26.12.2017 N 1642 (ред. от 22.02.2021) «Об утверждении государственной программы Российской Федерации «Развитие образования»

5. Стратегия развития воспитания в Российской Федерации на период до 2025 года (Утверждена распоряжением Правительства РФ от 29.05.2015 N 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»)

6. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании), (воспитатель, учитель)» (ред. от 16.06.2019 г.) (Приказ Министерства труда и социальной защиты РФ от 18 октября 2013г. № 544н, с изменениями, внесенными приказом Министерства труда и соцзащиты РФ от 25 декабря 2014г. № 1115н и от 5 августа 2016г. № 422н)

7. Профессиональный стандарт «Педагог дополнительного образования детей и взрослых» (Приказ Министерства труда и социальной защиты РФ от 5 мая 2018 г. N 298н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»)

8. Федеральный государственный образовательный стандарт основного общего образования (Утвержден приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. N 1897) (ред. 21.12.2020)

9. Федеральный государственный образовательный стандарт среднего общего образования (Утвержден приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. N 413) (ред.11.12.2020)

10. Методические рекомендации по созданию и функционированию центров цифрового образования «IT-куб» (Утверждены распоряжением Министерства просвещения Российской Федерации от 12 января 2021 г. N Р-5)

11. Федеральный закон о защите детей от информации, причиняющей вред их здоровью и развитию 436-ФЗ в ред. Федерального закона от 28.07.2012

12. Федеральный закон “О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации”.

15. Законодательство в области борьбы с преступлениями против несовершеннолетних

**Актуальность программы.**

Данная программа отвечает социальному заказу общества, задачам федеральных проектов «Успех каждого ребенка» и «Цифровая образовательная среда» (в рамках национального проекта РФ «Образование»), в рамках которых, действует Центр цифрового образования детей «IT-куб», потребностям учащихся среднего и старшего школьного возраста.

Массовое распространение информационных технологий во всех сферах деятельности человека выводит проблему кибербезопасности в разряд наиболее актуальных. Актуальной задачей в рамках реализации данной программы является подготовка подрастающего поколения к жизни, будущей профессиональной деятельности в высокоразвитом информационном обществе.

**Программа** составлена на основе программы **«Кибербезопасность»,** автор Авдеев Никита Юрьевич,педагог дополнительного образования МОУ ДО «ЦДОД «Росток» г. о. Электросталь Московской области

**Цель программы:** *формирование у учащихся способности к разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства.*

**Задачи программы**:

1. Сформировать у учащихся представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных.
2. Ознакомить учащихся с основами исследовательской деятельности (принципами построения исследования, процедурой и этикой его проведения, количественными и качественными методами обработки полученных данных).
3. Ознакомить учащихся с методами и средствами поиска информации в интернет-пространстве.
4. Сформировать у учащихся навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум».
5. Сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество.
6. В защищенной среде продемонстрировать учащимся возможные угрозы и риски интернет-пространства.
7. Сформировать у учащихся способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях.
8. Сформировать у учащихся способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях.
9. Сформировать у учащихся способность распознавать опасный и вредный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях.
10. Обучить учащихся приемам противодействия негативным воздействиям в интернет-пространстве.
11. Привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации.
12. Способствовать ранней профориентации учащихся.

**Педагогическая целесообразность программы.** В ходе освоения программы у учащихся формируются навыки планирования и проведения исследований интернет-пространства, эффективного поиска и качественного анализа информации, выявлению и систематизации информационных поводов. Подростки учатся обнаруживать источники информации, каналы и овладевают способами ее распространения. На занятиях формируются адекватное восприятие в оценке информации, ее критическое осмысление на основе нравственных и культурных ценностей. Программа позволяет получить представления о персональных данных в Интернете и возможности работы с ними, получить практические навыки анализа и структурирования данных, составления информационных отчетов и прогнозов, использования статистических методов в реальной жизни. Учащиеся приобретают опыт распознавания опасного и вредного контента, наличия манипулирования сознанием, внушения потенциально опасных идей в интернет-пространстве. Учащиеся овладевают навыками критического мышления, осуществляется поддержка личностного роста учащихся, успешной социализации. Полученные знания и умения позволяют подросткам критически оценивать и классифицировать получаемую в интернет-пространстве информацию, использовать ее в позитивных целях и нейтрализовать ее негативное влияние. Активизируются профессиональное самоопределение учащихся в информационном обществе, гражданская инициатива.

**Особенности организации учебного процесса**

Особенностью программы является модульный принцип построения содержания. В программе реализуются два модуля по 36 часов каждый.

Учебно-тематический план программы включает всего 6 обязательных кейсов (вводный и 5 базовых).

Для подачи теоретического материала используются интерактивные формы проведения лекций: проблемная лекция, лекция-визуализация, лекция-беседа, лекция-дискуссия и т.п.

Практическая работа за компьютером и самостоятельная работа учащихся осуществляется преимущественно в интернете, непосредственно в социальных сетях и системе мониторинга и анализа социальных медиа «Крибрум».

Самостоятельная работа в рамках большинства кейсов рассчитана на малые группы – 2 или 3 человека.

Результат работы над каждым кейсом представляется в виде групповой презентации (общей для всей группы или своя в каждой малой группе) или общий документ в другом формате (интеллект-карта, лента времени и т.п.).

**Режим занятий:**

Продолжительность одного занятия может составлять 2 академических часа (1 академический час равен 40 минутам) с десятиминутным перерывом 1 раз в неделю, что определяется санитарно-эпидемиологическими правилами и нормативами СанПиН 2.4.4.3172-14; занятие может составлять 1 академический час 2 раза в неделю.

**Количество обучающихся в группе:** 12 человек.

## Результаты освоения программы:

*Предметные результаты:*

* понимание структуры интернет-пространства, знание типов источников информации и разновидностей контента;
* владение методологией исследования информации в интернет-пространстве;
* умение работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве и системой «Крибрум»;
* умение анализировать информацию в интернет-пространстве при помощи количественных и качественных методов, формировать целостное представление об объекте, ситуации или социальной группе на основе разных источников с применением системы «Крибрум» и без;
* знание признаков рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности) и умение идентифицировать их в социальных сетях;
* понимание и принятие правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;
* умение определять индивидуальные особенности людей на основе аккаунтов в

социальных сетях.

*Личностные и межличностный результаты:*

* развитие аналитического (логического), практического и логического мышления; способность ставить цели, планировать свою работу и следовать намеченному плану, критически оценивать достигнутые результаты;
* развитие самостоятельности и самоорганизации;
* умение работать в команде, развитие коммуникативных навыков;
* умение представлять результаты своей работы окружающим, аргументировать свою позицию;
* способность свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения собственных задач;
* способность рационально и безопасно использовать социальные сети;
* способность грамотно представлять в интернет-пространстве свои личные и персональные данные, формировать и поддерживать собственный позитивный имидж в социальных сетях;
* способность распознавать признаки рискованного и опасного поведения в своем окружении в социальных сетях;
* способность избегать «ловушек», связанных с коммуникационными, контентными, потребительскими и некоторыми технологическими рисками интернет-пространства.
* сформируется критическое мышление, определится направление в будущей профессии.

**Способы определения результативности.**

Используются следующие методы отслеживания результативности: педагогическое наблюдение; педагогический анализ результатов анкетирования, тестирования, зачетов, опросов; выполнения обучающимися диагностических заданий.

Мониторинг результатов реализации программы осуществляется по следующим критериям: ***теоретическая подготовка (знания в области техники безопасности; теоретические знания в области кибергигиены и цифровой безопасности); практическая подготовка; личностные результаты (мотивация учебной деятельности; критическое и рациональное мышление, умение объективно оценивать свои результаты; коммуникабельность; трудолюбие).***

**УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование темы** | **Количество часов** | | | **Формы контроля** |
| **всего** | **теория** | **практика** |
| **Модуль 1. (36 час.)** | | | | | |
| **Вводный кейс: «Инструктаж по ТБ, ППБ, ПДД. Основы анализа информации в интернет-пространстве» (8 часов)** | | | | | |
| 1. | Вводное занятие.Инструктаж по ТБ, ППБ, ПДД. | **2** | 1,5 | 0,5 | Собеседование, педагогическое наблюдение. |
| 2. | Поиск и оценка информации. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 3. | Поисковые запросы. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 4. | Графическое представление информации. | **2** | 0,5 | 1,5 | Педагогическое наблюдение.  Анализ выполнения практической работы. Самоанализ. |
| **Кейс: «Анализ мнений интернет-пользователей» (14 часов)** | | | | | |
| 5. | Социальные сети и проблема лайков. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 6. | Методы исследования мнений в сети. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 7. | Крибрум. Анализ статистики фильма. | **2** | 1 | 1 | Устный опрос,  практическое задание. |
| 8. | Сбор информации, сайт Kinopoisk. | **2** | 0,5 | 1,5 | Практическое задание. |
| 9. | Анализ мнений, работа над проектом. | **2** | 0,5 | 1,5 | Практическое задание. |
| 10. | Представление результатов работы. | **4** | 1 | 3 | Устный опрос,  контроль проекта. |
| **Кейс: «Порядок действий ликвидации последствий сбоев системы, кибератак. Возможные пути решения проблемы» (14 часов)** | | | | | |
| 11. | Сбой системы и синий экран. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 12. | Фейковые сообщения и вредоносное ПО. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 13. | Проблема хакерства и кибератак. | **2** | 1,5 | 0,5 | Устный опрос,  педагогическое наблюдение. |
| 14. | Персональные данные и вредоносное ПО. | **2** | 0,5 | 1,5 | Устный опрос,  педагогическое наблюдение. |
| 15. | Проблемы банковских карт и сайтов продаж. | **2** | 0,5 | 1,5 | Устный опрос,  педагогическое наблюдение. |
| 16. | Представление результатов работы. | **4** | 1 | 3 | Устный опрос,  контроль проекта. |
| Всего: | | **36** | **14,5** | **21,5** |  |
| **Модуль 2. (36 час.)** | | | | | |
| **Кейс: Анализ социальных групп на основе данных интернет-пространства**  **(8 часов)** | | | | | |
| 17. | Изучение интернет, структуры сообществ. | **2** | 0,5 | 1,5 | Устный опрос,  практическое задание. |
| 18. | Правила поведения в сообществах. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 19. | Анализ активности сообщества. | **2** | 0,5 | 1,5 | Устный опрос,  практическое задание. |
| 20. | Представление результатов работы. | **2** | - | 2 | Устный опрос,  контроль проекта. |
| **Кейс: «Безопасное и рациональное использование личных и персональных данных в социальных сетях» (14 часов)** | | | | | |
| 21. | Защита личных данных. Безопасный пароль. Рекомендации. | **2** | 1 | 1 | Беседа, устный опрос, практическое задание. |
| 22. | Вводная в криптографию. | **2** | 1 | 1 | Устный опрос,  практическое задание. |
| 23. | Политики и соглашения соц. сетей. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 24. | Настройки приватности профиля соц. сети. | **2** | 0,5 | 1,5 | Устный опрос,  практическое задание. |
| 25. | Небезопасное использование личных данных. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 26. | Риски знакомств и манипулирование в соц. сетях. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 27. | Представление результатов работы. | **2** | - | 2 | Устный опрос,  контроль проекта. |
| **Кейс: «Распознавание опасного и вредного контента в интернет-пространстве» (12 часов)** | | | | | |
| 28. | Контентные риски. Противодействие. | **2** | 1 | 1 | Устный опрос,  практическое задание.  Самоанализ. |
| 29. | Фишинг. Противодействие фишингу. | **2** | 1 | 1 | Устный опрос,  практическое задание. |
| 30. | Благотворительность и её риски. Реклама в соц. сети. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 31. | Подозрительные объявления. | **2** | 1 | 1 | Устный опрос,  педагогическое наблюдение. |
| 32. | Проблема поддельных услуг и работы в соц. сетях. | **2** | 1,5 | 0,5 | Беседа, устный опрос. |
| 33. | Представление результатов работы. | **2** | 0 | 2 | Устный опрос,  контроль проекта. |
| **Итоговое занятие (2 часа)** | | | | | |
| 34. | Итоговое занятие. | **2** | - | 2 | Тест, анализ итогов. |
| Всего: | | **36** | **13** | **23** |  |
| **Итого:** | | **72** | **27,5** | **44,5** |  |

**Содержание**

**Модуль 1 (36 час.)**

**Вводный кейс: «Инструктаж по ТБ, ППБ, ПДД. Основы анализа информации в интернет-пространстве» (8 часов)**

**Форма работы:** Инструктаж, беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1. Вводное занятие. (2 часа)**

*Теория:*Знакомство с детьми. Инструктаж по технике безопасности и правилам поведения в Центре. Инструктаж по правилам дорожного движения.

Информационная структура интернета, поисковые системы. Ознакомление с инструментом представления результатов работы в рамках курса, принципами подготовки эффективной презентации.

*Практика:* Поиск в интернете различными способами, изучение интерфейса программы презентации, подготовка презентаций.

**Тема 2. Поиск и оценка информации. (2 часа)**

*Теория:* Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.

*Практика:* Поиск в интернете, подготовка презентаций по эффективному поиску в интернете.

**Тема 3. Поисковые запросы. (2 часа)**

*Теория:* Правила поиска в интернете. Поисковый запрос: простой и расширенный, язык запросов, поиск различных типов контента.

*Практика:* Изучение правил поиска, подготовка презентаций с правилами поиска.

**Тема 4. Графическое представление информации. (2 часа)**

*Теория:* Представление результатов работы. Ознакомление с инструментом представления результатов работы в рамках курса, принципами подготовки брошюр и плакатов с помощью сайтов для создания графики.

*Практика:* Изучение элементов сайта*.* Тренировка в создании брошюр.

**Кейс: «Анализ мнений интернет-пользователей» (14 часов)**

**Форма работы:** Инструктаж, беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1. Соц. сети и проблема лайков. (2 часа)**

*Теория:*Социальные сети и социальные медиа, поведение молодежи в сети, проблема лайков.

*Практика:* Поиск в интернете, подготовка презентаций по соцсетям, заполнение анкет «На что вы готовы ради лайка»

**Тема 2. Методы исследования мнений в сети. (2 часа)**

*Теория:* Элементы контента социальных сетей. Постановка задачи исследования мнений интернет-пользователей. Программа исследования и методы исследования.

*Практика:* Сравнение результатов анкетирования с исследованиями по теме. Знакомство с платформой Крибрум.

**Тема 3. Крибрум. Анализ статистики фильма. (2 часа)**

*Теория:* Анализ упоминаний фильма, сообщений и авторов с помощью системы «Крибрум».

*Практика:* Работа с платформой Крибрум, анализ сообщений по выбранному фильму.

**Тема 4. Сбор информации, сайт Kinopoisk. (2 часа)**

*Теория:* Сбор информации об оценках фильма зрителями и критиками на сайте kinopoisk.ru.

*Практика:* Проведение исследования, подготовка презентации по результатам. Работа с сайтом kinopoisk.ru

**Тема 5. Анализ мнений, работа над проектом. (2 часа)**

*Теория:* Завершение анализа мнений пользователей в сообщениях социальных сетей с помощью системы «Крибрум», подготовка к представлению результатов проделанной работы.

*Практика:* Самостоятельная работа над проектом, отчеты о ходе работы

**Представление результатов работы. (4 часа)**

*Теория:* Представление результатов работы.

*Практика:* Выступление групп с презентациями, обсуждение работ, оценка работ, прохождение теста.

**Кейс: «Порядок действий ликвидации последствий сбоев системы, кибератак. Возможные пути решения проблемы» (14 часов)**

**Форма работы:** Беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1. Сбой системы и синий экран. (2 часа)**

*Теория:*Понятие сбоя системы и синего экрана. Способы восстановления системы. Постановка задачи исследования. Изучение сообщений о синем экране в интернете.

*Практика:* Анализ сообщений по теме «синий экран» в сети, составление плана по решению проблемы.

**Тема 2. Фейковые сообщения и вредоносное ПО. (2 часа)**

*Теория:* Изучение фейковых сообщений и вредоносного ПО в сети Интернет и с помощью сети. Способы распространения и заражения. Изучение действий при столкновении.

*Практика:* Работа в интернете, составление плана действий по решению проблемы

**Тема 3. Проблема хакерства и кибератак. (2 часа)**

*Теория:* Рассмотрение наиболее крупных взломов системы и кибератак. Проблема хакерства. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.

*Практика:* Исследование информации о проблеме в сети, подведение итогов исследования.

**Тема 4. Персональные данные и вредоносное ПО. (2 часа)**

*Теория:* Проблема краж персональных данных с помощью вредоносного ПО. Исследование сообщений в системе «Крибрум».

*Практика:* Поиск и сбор информации для презентации.

**Тема 5. Проблемы банковских карт и сайтов продаж. (2 часа)**

*Теория:* Проблема краж с помощью банковских карт. Обзор сайтов онлайн-продаж. Исследование сообщений в системе «Крибрум».

*Практика:* Подготовка презентации по темам 4 и 5.

**Представление результатов работы. (4 часа)**

*Теория:* Представление результатов работы.

*Практика:* Выступление с презентациями, обсуждение, прохождение теста.

**Модуль 2. (36 час.)**

**Кейс: Анализ социальных групп на основе данных интернет-пространства**

**(8 часов)**

**Форма работы:** Беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1.** **Изучение интернет, структуры сообщества. (2 часа)**

*Теория:*Понятие социальная группа, сообщество, субкультура, фэндом. Постановка задачи исследования. Изучение сообщений о сообществе в социальных сетях. Изучение структуры сообщества, авторов сообщений в социальной сети «ВКонтакте».

*Практика:* Поиск в интернет информации о субкультуре, подготовка презентаций по различным сообществам, анализ сообщений сообщества. Разработка плана презентаций, изучение структуры сообществ.

**Тема 2.** **Правила поведения в сообществах. (2 часа)**

*Теория:* Изучение правил функционирования сетевых сообществ. Правила сетевого общения.

*Практика:* Изучение правил поведения в сообществах, анализ сообщений в сообществе. Подготовка презентаций

**Тема 3.** **Анализ активности сообщества. (2 часа)**

*Теория:* Анализ с помощью системы «Крибрум» активности участников группы сообщества, связей, поведенческих особенностей, предпочтений и интересов сообщества (в том числе с использованием контент-анализа).

*Практика:* выполнение контент-анализа сообщений сообщества.

**Представление результатов работы. (2 часа)**

*Теория:* Представление результатов работы.

*Практика:* Подготовка презентаций, выступление, обсуждение, прохождение теста.

**Кейс: «Безопасное и рациональное использование личных и персональных данных в социальных сетях» (14 часов)**

**Форма работы:** Беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1.** **Защита личных данных.** **Безопасный пароль. Рекомендации. (2 часа)**

*Теория:*Защищенность данных в сети. Проблемы утечки данных. Действия при взломе аккаунтов. Безопасные пароли. Подготовка к групповой работе по разработке рекомендаций по рациональному и безопасному использованию личных и персональных данных в социальных сетях. Разработка рекомендаций по созданию безопасных паролей и их хранению. Понятие персональных данных. Законодательство о защите персональных данных.

*Практика:* Изучение тематических статей, подготовка презентации о действиях при взломе в сетях. Подготовка брошюр по теме.

**Тема 2.** **Вводная в криптографию. (2 часа)**

*Теория:* Криптография: история развития и способы шифровки данных.

*Практика:* Выполнена самостоятельная работа по расшифровке данных и поиску информации в интернете с помощью полученных данных.

**Тема 3.** **Политики и соглашения соц. сетей. (2 часа)**

*Теория:* Политика социальных сетей в области конфиденциальности пользовательских данных. Структура аккаунта пользователя социальной сети. Пользовательские соглашения.

*Практика:* Изучение политики конфиденциальности соцсетей, подготовка презентации.

**Тема 4.** **Настройки приватности профиля соц. сети. (2 часа)**

*Теория:* Настройки приватности в социальных сетях. Самопрезентация пользователя в социальных сетях.».

*Практика:* Изучение настройки приватности, подготовка презентации. Разработка рекомендаций по настройке приватности.

**Тема 5.** **Небезопасное использование личных данных. (2 часа)**

*Теория:* Риски нерационального и небезопасного использования личных и персональных данных в социальных сетях. Проблемы использования в сообщениях геотегов, столкновения с неразумным и агрессивным поведением в сети. Анализ сообщений в сети.

*Практика:* Созданы брошюры на тему «Безопасность персональных данных в соц. сетях»

**Тема 6.** **Риски знакомств и манипулирование в соц. сетях. (2 часа)**

*Теория:* Проблемы рискованного поведения, нежелательных и сомнительных знакомств, манипулирования и вовлечения в опасное поведение в социальных сетях. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.

*Практика:* Разработаны презентации на тему: “Соц. сети. Безопасное общение.”

**Представление результатов работы. (2 часа)**

*Теория:* Представление результатов работы.

*Практика:* Выступление с презентациями, обсуждение результатов, прохождение теста.

**Кейс: «Распознавание опасного и вредного контента в интернет-пространстве» (12 часов)**

**Форма работы:** Беседа, интерактивная лекция, практическая работа, самостоятельная работа, конференция.

**Оборудование:** компьютер, интерактивная доска, рабочая тетрадь.

**Тема 1.** **Контентные риски. Противодействие. (2 часа)**

*Теория:*Проблема контентных рисков и меры противодействия им. Механизмы защиты социальных сетей от негативного контента. Постановка задачи исследования по подготовке интеллектуальной карты реагирования при столкновении с подозрительным контентом в сети.

*Практика:* Подготовка презентаций на основе изучения сайтов: Роскомнадзор, «Лига безопасного интернета», РОЦИТ, проект «Дети России Онлайн», проект «Медиагвардия».

**Тема 2.** **Фишинг. Противодействие фишингу. (2 часа)**

*Теория:* Проблема фишинга в сети. Исследование фишинговых и коротких ссылок. Правила противодействия фишингу.

*Практика:* Проверка ссылок из соцсетей на фишинг и вирусы.

**Тема 3.** **Благотворительность и её риски. Реклама в соц. сети. (2 часа)**

*Теория:* Благотворительность с помощью интернет. Исследование подозрительных объявлений о пожертвованиях в благотворительные фонды и частных сборах на лечение. Риски потребительского поведения. Правила социальных сетей по размещению рекламы. Анализ объявлений о продаже в социальных сетях.

*Практика:* Создание плана реагирования для проверки сообщений о сборах на благотворительность.

**Тема 4.** **Подозрительные объявления. (2 часа)**

*Теория:* Торговля в интернете. Анализ подозрительных объявлений о дарении, об акциях, розыгрышах призов и конкурсах репостов в социальных сетях.

*Практика:* Работа в интернете - анализ интернет-магазинов, акций. Подготовка отчёта.

**Тема 5.** **Проблема поддельных услуг и работы в соц. сетях. (2 часа)**

*Теория:* Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях, анализ подозрительных сообщений в сети. Составление интеллектуальной карты действий при столкновении с подозрительным контентом.».

*Практика:* Работа в интернете, анализ различных услуг. Подготовка интеллектуальной карты.

**Представление результатов работы. (2 часа)**

*Теория:* Представление результатов работы.

*Практика:* Выступление с интеллектуальными картами, обсуждение, оценка работ. Получение темы для создания итоговой работы.

**Итоговое занятие (2 часа)**

*Теория:* Подведение итогов занятий по курсу.

*Практика:* Прохождение итогового теста, обсуждение рисков, пути преодоления, перспективы развития интернета.

**Методическое обеспечение программы**

Учебный кабинет площадью и освещенностью в соответствии с нормами СанПиН (площадь кабинета не менее 2 кв. м. на чел., наименьшая освещенность должна быть не менее 20 Вт на кв.м).

**Материально-технические условия**

***Оборудование аудитории****:*

1. Набор мебели (компьютерный стол, стул) на 13 человек
2. Магнитно-маркерная доска – 1 шт.
3. Компьютерное оборудование:
4. Ноутбук с доступом в интернет – 13 шт.
5. Акустическая система – 1 шт.
6. Интерактивная доска – 1шт.
7. Программное обеспечение:
8. Система «Крибрум» с массивами данных для кейсов.
9. Пакет «Microsoft Office».
10. Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер».
11. Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.).
12. Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.).

***Методические материалы:***

Учебно-методический комплект для преподавателя (программа, описание кейсов, опорные теоретические материалы для наставников, список ресурсов). Руководство пользователя системы «Крибрум».

Учебно-тематический план не является жестко регламентированным. Количество часов, выделяемое на каждый кейс или другой вид учебной деятельности, может варьироваться в зависимости от условий, уровня группы и пр.

**Список использованной литературы**

1. Ашманов И.С. Идеальный поиск в Интернете глазами пользователя. – М.: Питер, 2011.
2. Ашманов И.С., Иванов А.А. Продвижение сайта в поисковых системах. – М.: Вильямс, 2007.
3. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова Ю.Н. Мельников. - М.: КноРус, 2019. - 432 c.
4. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 c.
5. Бехтерев С.В. Майнд-менеджмент. Решение бизнес-задач с помощью интеллект-карт. – М.: Альпина Паблишер, 2012.
6. Богачева Т.Ю., Соболева А.Н., Соколова А.А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. – М.: АНО «ЦНПРО», 2015.
7. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. – М.: Академический проект; Фонд «Мир», 2010.
8. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2013.
9. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 160 c.
10. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 c
11. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. - М.: Юнити, 2015. - 239 c.
12. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Русайнс, 2017. - 64 c.
13. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 c.
14. Слугина Н. Активные пользователи социальных сетей Интернета. – СПб.: Питер, 2013.
15. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. – М.: Google, 2013.
16. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 c.
17. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. – М.: Книжный мир, 2012.

**Список литературы, рекомендуемой обучающимся:**

1. Выжить в цифровом мире. Иллюстрированные советы от "Лаборатории Касперского" – СПБ.: Питер, 2015
2. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 c.
3. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 c.
4. Запечников, С.В. Информационная безопасность открытых систем. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 c.
5. Запечников, С.В. Информационная безопасность открытых систем. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. ТолстоГЛТ, 2018. — 558 c.

**Ресурсы информационно-телекоммуникационной сети «Интернет»**

1. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернете. [Электронный ресурс] URL:

<http://www.ifap.ru/library/book331.pdf>

2. Безопасность детей в Интернете URL:

<http://www.microsoft.com/rus/childsafety>

3. Борьба с вредоносными программами http://support.kaspersky.ru/viruses

4. Проект компании Positive Technologies. http://www.securitylab.ru/

5. Новостной сайт об информационной безопасности от Kaspersky Lab. <https://threatpost.com/>

6. Информационно-аналитический центр, посвященный информационной безопасности. <https://www.anti-malware.ru/>

7. Популярный хаб сайта geektimes.ru про информационную безопасность. <https://geektimes.ru/hub/infosecurity/>

8. Видеоканал компании CISCOhttps://www.youtube.com/playlist?list=PLEnXkMoWGlq2ZroboDpbUjwrqB3wIcMYC