СЕТЕВАЯ ПРОГРАММА

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ДЛЯ ОДАРЕННЫХ ДЕТЕЙ «ПОИСК»

УТВЕРЖДАЮ:
И.о. директора Центра «Поиск»
_____
С.А. Томилина
приказ № _168_ от _19.04.2024__ г.

Дополнительная общеобразовательная общеразвивающая
программа технической направленности

«Кибергигиена и работа с большими данными»

Направление: Наука

Возраст обучающихся: 11-17 лет

Объем программы: 136 часа

Срок освоения: 1 год

Форма обучения: очная

Авторы программы: Невзорова Валерия Алексеевна, педагог дополнительного образования ЦЦО «IT-куб»
Жалыбина Юлия Витальевна, заведующий ЦЦО «IT-куб»
Савельева Ольга Александровна, методист ЦЦО «IT-куб»

Минеральные Воды, 2024

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа «Кибергигиена и работа с большими данными» разработана в соответствии с требованиями нормативных документов:

Федерального закона РФ от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

Концепции развития дополнительного образования детей, утвержденной распоряжением Правительства РФ от 4 сентября 2014 г. № 1726-р.

Приказа Минпросвещения РФ от 09.11.2018 г. N 196 «Об утверждении

Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».

Постановления Главного государственного санитарного врача РФ от 28.09.2020 г. № 28 СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

Методических рекомендаций по проектированию дополнительных общеразвивающих программ (письмо Минобрнауки РФ от 18.11.2015 г. N 09-3242).

Методических рекомендаций по созданию и функционированию центров цифрового образования «IT-куб» (утв. распоряжением Министерства просвещения Российской Федерации от 12.01.2021 № Р-5). Паспорт национального проекта «Образование» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16).

Государственной программы Российской Федерации «Развитие образования» (утв. постановлением Правительства РФ от 26.12.2017 № 1642 (ред. от 15.03.2021) «Об утверждении государственной программы Российской Федерации “Развитие образования”»).

Стратегии развития воспитания в Российской Федерации на период до 2025 года (утв. распоряжением Правительства РФ от 29.05.2015 № 996-р «Об

утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»).

1. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММЫ

1.1. Направленность программы

Дополнительная общеобразовательная общеразвивающая программа «Кибергигиена и работа с большими данными» имеет техническую направленность.

1.2. Адресат программы

Программа адресована обучающимся от 11 до 17 лет.

Программа предназначена для одаренных школьников 5-10 классов, проявляющих повышенный интерес к информатике, математике, анализу данных.

Возрастная категория обучающихся – разновозрастная.

Необходимы базовые знания по следующим школьным предметам: информатика, математика.

Наличие определенной физической и практической подготовки для изучения учебной программы не требуется.

1.3. Актуальность программы

В ходе освоения программы, учащиеся получат навыки исследовательской деятельности и анализа информации в интернет-пространстве, смогут обнаруживать источники информации, каналы и способы ее распространения. Также учащиеся научатся распознавать опасный и вредоносный контент, манипулирование сознанием и внушение потенциально опасных идей в интернет-пространстве. Полученные знания и умения позволят критически оценивать и классифицировать получаемую в интернет-пространстве информацию, использовать ее в положительных целях и нейтрализовать ее негативное влияние.

1.4. Новизна программы

Программа «Кибергигиена и работа с большими данными» в целом строится на концепции подготовки учащихся к профессии киберследователя – профессии будущего, выделенной в «Атласе новых профессий» (проект «Агентства стратегических инициатив» по исследованию рынка труда) и предполагающей проведение расследований киберпреступлений посредством поиска и обработки информации в интернет-пространстве.

Уровень освоения программы – базовый.

1.5 Объем и срок освоения программы

Объем программы – 136 часов.

Срок реализации программы – 1 год.

1.6 Цели и задачи программы

Цель - формирование у учащихся способности к разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства, привлечение к проектно-исследовательской деятельности.

Задачи программы

1. Образовательные:

сформировать у учащихся представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;

ознакомить учащихся с методами и средствами поиска информации в интернет-пространстве;

сформировать у учащихся способность распознавать опасный и вредоносный контент и идентифицировать явления манипулирования сознанием

в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях;

сформировать у учащихся способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;

обучить учащихся приемам противодействия негативным воздействиям в интернет-пространстве.

2. Развивающие:

сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;

сформировать у учащихся способность успешной самопрезентации и создания позитивного имиджа в социальных сетях;

развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность;

способствовать развитию коммуникативных навыков, психологической совместимости и адаптации в учебной группе.

3. Воспитательные:

сформировать у учащихся культуру позитивного использования интернет-пространства;

привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации.

1.7. Планируемые результаты освоения программы

1. Предметные результаты:

–знание структуры интернет-пространства, типы источников информации и разновидностей контента;

–владение методологией исследования информации в интернет-пространстве;

–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;

–знание правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

2. Метапредметные результаты:

−умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности

3. Личностные результаты:

−умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности;

−развивать мотивы и интересы своей познавательной деятельности.

2. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

2.1 Язык реализации программы

Реализация дополнительной общеобразовательной общеразвивающей программы «Кибергигиена и работа с большими данными» осуществляется на государственном языке Российской Федерации.

2.2. Форма обучения:

очная.

2.3. Особенности реализации программы

Программа реализуется по кейсовому принципу.

2.4. Условия набора и формирования групп

Условия набора обучающихся.

На обучение зачисляются обучающиеся 5-10 классов общеобразовательных организаций Ставропольского края.

Зачисление на обучение по программе осуществляется при наличии свободных мест в соответствии с Правилами приема обучающихся в государственное автономное образовательное учреждение дополнительного образования «Центр для одаренных детей «Поиск» на 2024 – 2025 учебный год, г. Минеральные Воды.

Условия формирования групп: разновозрастная.

2.5. Формы организации и проведение занятий

Формы организации занятий:

– аудиторные (под непосредственным руководством преподавателя).

Формы проведения занятий:

- теоретические;
- практические;
- лабораторные;
- контрольные.

Формы организации деятельности обучающихся:

Интерактивные проблемные лекции - предполагает наиболее полное вовлечение всех участников лекционного занятия в процесс изучаемого материала, демонстрация слайд-презентации или фрагментов учебных фильмов.

Мозговой штурм - предполагает генерацию идей, которую применяют для выявления проблем или поиска решений

Практикум – предполагает выполнение практических заданий.

Режим занятий.

Очная форма обучения: 5-10 классы – 4 урока 2 раза в неделю. Программа реализуется в г. Минеральные Воды.

УЧЕБНЫЙ ПЛАН

Наименование модуля, учебного курса	Количество часов			
	Теория	**Практика**	**Всего**	**Форма контроля/ аттестации**
Вводный кейс. Настройки безопасности персонального компьютера. Порядок действий ликвидации последствий сбоев системы.	12	16	28	Контрольный тест
Кейс 1. Основы анализа информации в интернет-пространстве.	4	4	8	Контрольный тест
Кейс 2. Угрозы в интернет-пространстве, методы противодействия.	10	14	24	Контрольный тест
Кейс 3. Основы работы в социальных сетях.	7	11	18	Контрольный тест
Кейс 4. Распознавание опасного и вредного контента в интернет-пространстве.	9	11	20	Контрольный тест
Кейс 5. Безопасность мобильных устройств.	4	6	10	Контрольный тест
Кейс 6. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.	6	8	14	Контрольный тест
Кейс 7. Проектная деятельность.	6	8	14	Представление результатов проделанной работы.
Итого:	**62**	**74**	**136**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование модуля, учебного курса	Год обучения	Дата начала обучения	Дата окончания обучения	Количество учебных недель	Количество учебных дней	Количество учебных часов	Режим занятий
Образовательная программа «Кибергигиена и работа с большими данными»	1 год обучения	02.09.2024	30.05.2025	37	74	136 ч.	2 урока 2 раза в неделю

РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА
«Кибергигиена и работа с большими данными»

5-10 классы

Курс «Кибергигиена и работа с большими данными» предназначен для обучающихся 5-10 классов.

Программа знакомит учащихся с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы.

Тематический план курса

№	Наименование кейса, темы	Количество часов		
		Теория	Практика	Всего
Вводный кейс. Настройки безопасности персонального компьютера. Порядок действий ликвидации последствий сбоев системы.		**12**	**16**	**28**
1.	Тема 1. Основы работы с ПК. Настройка оборудования для работы.	1	1	2
1.	Тема 2. Разграничение прав пользователей.	1	1	2
2.	Тема 3. Брандмауэры и фаерволы. Работа в браузере. Настройки безопасности.	1	1	2
3.	Тема 4. Основы адресации в интернете.	4	4	8
4.	Тема 5. Создание безопасных паролей. Менеджеры и генераторы паролей.	1	1	2
5.	Тема 6. Понятие сбоя системы и синего экрана. Способы восстановления системы. Изучение сообщений о синем экране с помощью системы «Крибрум».	2	2	4
6.	Тема 7. Офисный пакет Microsoft.	2	4	6
7.	Тестирование.	0	2	2

Кейс 1. Основы анализа информации в интернет-пространстве.		**4**	**4**	**8**
8.	Тема 1.1 Информационная структура интернета, поисковые системы.	2	2	4
9.	Тема 1.2. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.	2	2	4
Кейс 2. Угрозы в интернет-пространстве, методы противодействия.		**10**	**14**	**24**
10.	Тема 2.1. Защищенность данных в сети. Проблемы утечки данных.	1	1	2
11.	Тема 2.2. Вирусные атаки ПК. Классы вирусов, способы защиты. Изучение сообщений о вирусных атаках с помощью системы «Крибрум».	2	2	4
12.	Тема 2.3. Антивирусные программы. Методология выбора оптимальной антивирусной программы для личного ПК.	2	4	6
13.	Тема 2.4. Фейковые сообщения и вредоносное ПО в сети Интернет.	1	1	2
14.	Тема 2.5. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.	2	2	4
15.	Тема 2.6. Проблема краж персональных данных с помощью вредоносного ПО.	1	1	2
16.	Тема 2.7. Проблема краж с помощью банковских карт.	1	1	2
17.	Тестирование.		2	2
Кейс 3.Основы работы в социальных сетях.		**7**	**11**	**18**
18.	Тема 3.1. Понятие социальная группа, сообщество, субкультура. Правила функционирования сетевых сообществ. Правила сетевого общения. Анализ сообществ с помощью системы «Крибрум».	1	1	2

19.	Тема 3.2. Социальные сети и социальные медиа.	1	1	2
20.	Тема 3.3. Социальные сети: пользовательские соглашения, права и обязанности.	1	1	2
21.	Тема 3.4. Поведение молодежи в сети, проблема лайков.	1	1	2
22.	Тема 3.5. Структура аккаунта пользователя социальной сети. Самопрезентация пользователя в социальных сетях. Проблема репостов, юридический аспект.	1	1	2
23.	Тема 3.6. Геотегирование. Проблемы использования в сообщениях геотегов.	1	1	2
24.	Тема 3.7. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.		2	2
25.	Тема 3.8. Понятие интернет-зависимости, компьютерной зависимости и причин их возникновения. Интернет-сообщество. Зависимость от интернет-общения. Виртуальная личность.	1	1	2
26.	Тестирование.		2	2
Кейс 4. Распознавание опасного и вредного контента в интернет-пространстве.		**9**	**11**	**20**
27.	Тема 4.1. Проблема контентных рисков и меры противодействия им.	1	1	2
28.	Тема 4.2. Правила противодействия фишингу. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».	1	1	2
29.	Тема 4.3. Интернет-коммерция. Площадки для Интернет-торговли. Проверка подлинности интернет-магазина.	1	1	2

30.	Тема 4.4. Благотворительность с помощью интернет.	1	1	2
31.	Тема 4.5. Риски потребительского поведения. Объявления о дарении, конкурсы репостов. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.	1	1	2
32.	Тема 4.6. Сетевые игры: польза и вред. (Сетевые игры как массовые развлечения. Бесплатные и платные игры. Для чего может быть полезен ПК и Интернет и как польза превращается во вред.)	1	1	2
33.	Тема 4.7. Киберугрозы Интернета. Кибертерроризм и кибервойны. Кибершпионаж. Кибероружие.	1	1	2
34.	Тема 4.8. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массового поражения.	1	1	2
35.	Тема 4.9. Развлечения в Интернет. Признаки зависимости. Сайты знакомств. Управление личностью через сеть. Киберкультура и личность. Типы интернет-зависимости.	1	1	2
36.	Тестирование.		2	2
Кейс 5. Безопасность мобильных устройств.		**4**	**6**	**10**
37.	Тема 5.1. Безопасность мобильных устройств в информационных системах.	1	1	2
38.	Тема 5.2. Источники заражения мобильных устройств.	1	1	2
39.	Тема 5.3. Угрозы для IOS-устройств. Угрозы для Android-устройств.	1	1	2
40.	Тема 5.4. Рост числа угроз для мобильных устройств. Вирусы для	1	1	2

	мобильных устройств.			
41.	Тестирование.		2	2
Кейс 6. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.		**6**	**8**	**14**
42.	Тема 6.1. Общие понятия об устройстве WiFi-сетей	1	1	2
43.	Тема 6.2. Угрозы безопасности WiFi-сетей	1	1	2
44.	Тема 6.3. Анализ трафика. Сниффинг.	1	1	2
45.	Тема 6.4. Методы защиты сетей WiFi. Меры безопасности для пользователя WiFi.	1	1	2
46.	Тема 6.5. Настройка безопасности сетей WiFi	1	1	2
47.	Тема 6.6. Онлайн сервисы для безопасности пользователя в интернете.	1	1	2
48.	Тестирование.		2	2
Кейс 7. Проектная деятельность.		**6**	**8**	**14**
49.	Тема 7.1. Знакомство с понятием «Проект».	2		2
50.	Тема 7.2. Жизненный цикл проекта.	2		2
51.	Тема 7.3. Выбор темы проекта. Проблематизация, целеполагание и постановка задач пути решения выбранной темы.	2	4	6
52.	Тема 7.4. Анализ выполненной работы, подготовка выступления к представлению результатов проделанной работы.		2	2
53.	Тема 7.5. Представление результатов проделанной работы.		2	2
	Итого	**62**	**74**	**136**

СОДЕРЖАНИЕ КУРСА «Кибергигиена и работа с большими данными»

Вводный кейс. Настройки безопасности персонального компьютера. Порядок действий ликвидации последствий сбоев системы.

В рамках вводного кейса учащиеся смогут настроить базовую безопасность персонального компьютера, разграничить права пользователей, настроить работу брандмауэра и также научатся создавать безопасные пароли. Проблемная ситуация подводит учащихся к необходимости изучения правильной защиты своего ПК и ликвидаций последствий сбоев системы.

Учащиеся должны знать:

–и применять базовые методы защиты персонального ПК;

–особенности работы с ПК.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–искать информацию в интернет-пространстве при помощи системы «Крибрум»;

–проводить контент-анализ;

–описывать и резюмировать результаты исследования;

–создавать презентации;

–использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная работа.

Тема 1. Основы работы с ПК. Настройка оборудования для работы.

Теория. Основы работы с ПК. Настройка оборудования для работы.

Практика. Настройка оборудования для дальнейшей комфортной

работы за ПК.

Тема 2. Разграничение прав пользователей.

Теория. Разграничение прав пользователей.

Практика. Настройка разграничения прав пользователей на ПК.

Тема 3. Брандмауэры и фаерволы. Работа в браузере. Настройки безопасности.

Теория. Брандмауэры и фаерволы. Работа в браузере. Настройки безопасности.

Практика. Настройки безопасности на ПК.

Тема 4. Основы адресации в интернете.

Теория. Основы адресации в интернете. Понятия: IP-адрес, адрес доменный, URL. Цифровая IP-адресация, DNS – адресация, URL, хост, домен, порт, протокол, SOCKS, прокси, IP, VPN.

Практика. Основы адресации в интернете.

Тема 5. Понятие сбоя системы и синего экрана. Способы восстановления системы. Изучение сообщений о синем экране с помощью системы «Крибрум».

Теория. Понятие сбоя системы и синего экрана. Способы восстановления системы.

Практика. Изучение сообщений о синем экране с помощью системы «Крибрум».

Тема 6. Создание безопасных паролей. Менеджеры и генераторы паролей.

Теория. Способы создания безопасных паролей. Менеджеры и генераторы паролей.

Практика. Создание безопасных паролей для различных сервисов.

Тема 7. Офисный пакет Microsoft.

Теория. Знакомство с приложениями для работы с документами, таблицами, презентациями, рисунками, бизнес-диаграммами и пр.

Практика. Создание презентации с помощью Microsoft PowerPoint

Форма подведения итогов: тестирование.

Кейс 1. Основы анализа информации в интернет-пространстве.

В рамках кейса 1 учащиеся научатся анализировать информацию в интернет-пространстве, исходя из информационной структуры интернета. Задача кейса основывается на структурировании и оценке информации в глобальной сети «Интернет». Проблемная ситуация подводит учащихся к необходимости изучения правил эффективного поиска и анализа информации в интернете.

Учащиеся должны знать:

–и применять методы обработки информации;

–особенности и закономерности эффективного поиска информации в интернете.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–проводить контент-анализ;

–описывать и резюмировать результаты исследования;

–создавать презентации;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя (навыки публичных выступлений);

–использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная работа,

конференция.

Тема 1.1. Информационная структура интернета, поисковые системы.

Теория. Информационная структура интернета, поисковые системы. Постановка задачи исследования. Технология WWW.

Практика. Информационная структура интернета, поисковые системы. Знакомство с поисковыми системами на практике.

Тема 1.2. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.

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

Практика. Использование эффективного поиска информации в интернете. Принципы оценки качества источников информации с помощью системы «Крибрум»

Кейс 2. Угрозы в интернет-пространстве, методы противодействия.

В рамках кейса 2 учащиеся научатся определять кибератаки и сбои в системе. Задача кейса основывается на анализе информации о способах защиты от вредоносного программного обеспечения. Проблемная ситуация подводит учащихся к необходимости рассматривать и принимать во внимание меры защиты программного обеспечения, изучению способов профилактики и лечения вирусов.

Учащиеся должны знать:

–и применять методы обработки информации.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–строить картограммы для визуализации данных исследования;

–выявлять и оценивать вредоносного программного обеспечения;

–выявлять опасности пользования онлайн-платежами;

–описывать и резюмировать результаты исследования;

–создавать презентации;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя (навыки публичных выступлений);

–использовать интернет-пространство для формирования целостного представления о ситуации и выделения ключевых событий.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 2.1. Защищенность данных в сети. Проблемы утечки данных.

Теория. Защищенность данных в сети. Проблемы утечки данных. Действия при взломе аккаунтов. Безопасные пароли. Понятие персональных данных. Законодательство о защите персональных данных.

Практика. 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.

Тема 2.2. Вирусные атаки ПК. Классы вирусов, способы защиты. Изучение сообщений о вирусных атаках с помощью системы «Крибрум».

Теория. Вирусные атаки ПК. Классы вирусов, способы защиты.

Практика. Изучение сообщений о вирусных атаках с помощью системы «Крибрум».

Тема 2.3. Антивирусные программы. Методология выбора оптимальной антивирусной программы для личного ПК.

Теория. Принципы работы антивирусных программ. Методология выбора оптимальной антивирусной программы для личного ПК.

Практика. Методология выбора оптимальной антивирусной программы

для личного ПК. Установка и настройка антивируса

Тема 2.4. Фейковые сообщения и вредоносное ПО в сети Интернет.

Теория. Фейковые сообщения и вредоносное ПО в сети Интернет.

Практика. Поиск фейковых сообщений в сети Интернет.

Тема 2.5. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.

Теория. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.

Практика. Хакерские атаки, виды атак. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем с помощью системы «Крибрум».

Тема 2.6. Проблема краж персональных данных с помощью вредоносного ПО.

Теория. Проблема краж персональных данных с помощью вредоносного ПО.

Практика. Изучение сообщений с помощью системы «Крибрум» проблема краж персональных данных с помощью вредоносного ПО.

Тема 2.7. Проблема краж с помощью банковских карт.

Теория. Проблема краж с помощью банковских карт.

Практика. Исследование сообщений в системе «Крибрум» проблема краж с помощью банковских карт.

Форма подведения итогов: тестирование.

Кейс 3. Основы работы в социальных сетях.

В рамках кейса 3 учащиеся познакомятся с понятиями социальные сети и социальные медиа, научатся определять особенности социальных групп, исходя из их самопрезентации и поведения в социальных сетях. Задача кейса основывается на анализе соц. сети и фанатских сообществ. Проблемная ситуация подводит учащихся к необходимости изучения соц.сети, жизни сообщества и ситуаций, в которые оно вовлечено, для его оценки. Учащимися

будет проанализирована актуальная информация о фанатских сообществах в различных источниках и их группы в социальных сетях при помощи системы «Крибрум» и без.

Учащиеся должны знать:

–и применять методы обработки информации;

–особенности и закономерности функционирования социальных групп на основе различных интернет-источников, поведенческих особенностей, предпочтений и интересов сообщества.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–искать информацию в интернет-пространстве при помощи системы «Крибрум»;

–проводить контент-анализ;

–описывать и резюмировать результаты исследования;

–создавать презентации;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя (навыки публичных выступлений);

–использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 3.1. Понятие социальная группа, сообщество, субкультура. Правила функционирования сетевых сообществ. Правила сетевого общения.

Теория. Понятие социальная группа, сообщество, субкультура. Правила

функционирования сетевых сообществ. Правила сетевого общения.

Практика. Анализ с помощью системы «Крибрум» активности участников группы сообщества, связей, поведенческих особенностей, предпочтений и интересов сообщества (в том числе с использованием контент-анализа); подготовка к представлению результатов проделанной работы.

Тема 3.2. Социальные сети и социальные медиа.

Теория. Понятие социальные сети и социальные медиа.

Практика. Изучение сообщений о социальных сетях и социальных медиа с помощью системы «Крибрум».

Тема 3.3. Социальные сети: пользовательские соглашения, права и обязанности.

Теория. Политика социальных сетей в области конфиденциальности пользовательских данных.

Практика. Изучение пользовательских соглашений и политики безопасности социальных сетей.

Тема 3.4. Поведение молодежи в сети, проблема лайков.

Теория. Поведение молодежи в сети, проблема лайков.

Практика. Поведение молодежи в сети, проблема лайков. Изучение сообщений о поведении молодежи в социальных сетях с помощью системы «Крибрум».

Тема 3.5. Структура аккаунта пользователя социальной сети. Самопрезентация пользователя в социальных сетях. Проблема репостов, юридический аспект.

Теория. Структура аккаунта пользователя социальной сети.

Практика. Настройки приватности в социальных сетях. Самопрезентация пользователя в социальных сетях.

Тема 3.6. Геотегирование. Проблемы использования в сообщениях геотегов.

Теория. Понятие геотегирования. 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.

Практика. Анализ сообщений с использованием системы «Крибрум».

Тема 3.7. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.

Практика. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях. Анализ сообщений с использованием системы «Крибрум».

Тема 3.8. Понятие интернет-зависимости, компьютерной зависимости и причин их возникновения.

Интернет-сообщество. Зависимость от интернет-общения. Виртуальная личность.

Теория. Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости.

Практика. Методы предотвращения появления зависимости. Критическая оценка информации, получаемой из сети Интернет.

Форма подведения итогов: тестирование.

Кейс 4. Безопасное и рациональное использование личных и персональных данных в социальных сетях.

В рамках кейса 4 учащиеся научатся определять по аккаунтам в социальных сетях социально-демографические характеристики и индивидуальные особенности человека, распознавать признаки рискованного и опасного поведения, рационально и безопасно использовать в социальных сетях личные и персональные данные. Задача кейса основывается на анализе собственного профиля в социальных сетях. Проблемная ситуация подводит учащихся к необходимости проверки личных и персональных данных,

указанных в их аккаунтах, и при необходимости редактирования этих данных. Учащимся будет предложено изучить собственный аккаунт, в том числе при помощи системы «Крибрум», и сделать заключение о том, что стоит скорректировать. Также учащимся будут продемонстрированы примеры и последствия необдуманного размещения личных данных в социальных сетях. В заключение учащимся предлагается разработать рекомендации по безопасному и рациональному использованию личных и персональных данных в социальных сетях.

Учащиеся должны знать:

–и применять методы обработки информации;

–принципы создания безопасных паролей и их хранения;

–принципы безопасного и рационального использования личных и персональных данных в социальных сетях.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–выявлять индивидуальные особенности пользователя в системе «Крибрум»;

–проводить контент-анализ;

–выявлять проблемы утечки данных, действия при взломе аккаунтов;

–исследовать аккаунты в социальных сетях с использованием контент-анализа, анализировать личные профили в социальных сетях;

–описывать и резюмировать результаты исследования;

–готовить презентацию и другие материалы для публичного представления;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя;

–определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;

–создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 4.1. Проблема контентных рисков и меры противодействия им.

Теория. Проблема контентных рисков и меры противодействия им. Механизмы защиты социальных сетей от негативного контента.

Практика. Постановка задачи исследования по подготовке интеллектуальной карты реагирования при столкновении с подозрительным контентом в сети.

Тема 4.2. Правила противодействия фишингу. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».

Теория. Проблема фишинга в сети. Правила противодействия фишингу.

Практика. Исследование фишинговых и коротких ссылок с помощью системы «Крибрум».

Тема 4.3. Интернет-коммерция. Площадки для Интернет-торговли. Проверка подлинности интернет-магазина.

Теория. Проблемы торговли через сеть Интернет. Популярные площадки. Мошеннические схемы, применяемы при работе на оналйн-площадках для торговли.

Практика. Методы опознания поддельных интернет-магазинов. Поиск мошеннических интернет-магазинов, объявлений о продаже.

Тема 4.4. Благотворительность с помощью интернет.

Теория. Благотворительность с помощью интернет. Методы опознания подлинного сайта благотворительного фонда.

Практика. Исследование с помощью «Крибрум» подозрительных объявлений о пожертвованиях в благотворительные фонды и частных сборах на лечение. Сравнение сайтов благотворительных фондов - опознание

подлинности.

Тема 4.5. Риски потребительского поведения. Объявления о дарении, конкурсы репостов.

Теория. Рекомендации по проверке добросовестности организаторов конкурсов и акций.

Практика. Исследование объявлений о дарении и конкурсов репостов в социальных сетях с помощью системы «Крибрум».

Тема 4.6. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.

Теория. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.

Практика. Анализ подозрительных сообщений с использованием системы «Крибрум», составление интеллектуальной карты действий при столкновении с подозрительным контентом.

Тема 4.7. Правила социальных сетей по размещению рекламы.

Теория. Основные правила размещения рекламы в социальных сетях. Отличие рекламы от публикаций в социальных сетях.

Практика. Работа SMM-специалиста. Изучение законодательства.

Тема 4.8. Сетевые игры: польза и вред.

Теория. История развития компьютерных игр, их виды и влияние на развитие и здоровье школьников. Для чего может быть полезен ПК и Интернет и как польза превращается во вред.

Практика. Сетевые игры как массовые развлечения. Бесплатные и платные игры. Исследование популярных сетевых игр с помощью системы «Крибрум».

Тема 4.9. Киберугрозы Интернета. Кибертерроризм и кибервойны.

Теория. Понятие кибертерроризма и кибервойны. Деятельность кибервойск. Методы защиты от кибератак.

Практика. Анализ самых громких кибератак.

Тема 4.10. Борьба с использованием Интернета в террористических,

сепаратистских и экстремистских целях. Интернет как оружие массового поражения.

Теория. Понятие экстремизма, сепаратизма и терроризма. Почему сеть интернет идеально подходит для пропаганды.

Практика. Законодательные и организационные меры, направленные на борьбу с распространение террористических, сепарастических и экстремистских материалов в интернет.

Тема 4.12 Развлечения в Интернет. Признаки зависимости. Сайты знакомств. Управление личностью через сеть. Киберкультура и личность. Типы интернет-зависимости.

Теория. Деструктивная информация в Интернете – как ее избежать. Психологическое воздействие информации на человека. Столкновение с неразумным и агрессивным поведением в сети.

Практика. Критерии зависимости с точки зрения психологов. Как развивается зависимость. Интернет как наркотик. Классификация интернет-зависимостей. Опрос- выявление интернет-зависимости у учащихся).

Тема 4.13. Представление результатов проделанной работы.

Практика. Подготовка к защите проекта (исследования).

Форма подведения итогов: представление результатов исследований – защита проектов.

Кейс 5. Безопасность мобильных устройств.

В рамках кейса 5 учащиеся научатся распознавать источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты). Рассмотрят угрозы для IOS-устройств и Android-устройств, изучат вирусы мобильных устройств (мобильные банкеры и др.) и методы борьбы с ними. Задача кейса основывается на анализе собственного мобильного устройства. Проблемная ситуация подводит учащихся к необходимости принятия мер для защиты своих данных. В заключение учащимся будет предложено алгоритмизировать действия по защите своего мобильного устройства и

представить их на интеллект-карте.

Учащиеся должны знать:

–источники заражения мобильных устройств;

–как отражать и предотвращать атаки на устройства.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–описывать и резюмировать результаты исследования;

–строить интеллект-карт;

–выявлять аккаунты (людей и групп), транслирующих опасный и вредный контент и демонстрирующих опасное поведение в социальных сетях;

–работать в команде и давать обратную связь;

–представить свой проект, свою команду и себя (навыки публичных выступлений);

–использовать интернет-пространство для формирования целостного представления о сложном феномене.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 5.1. Безопасность мобильных устройств в информационных системах.

Теория. Операционные системы для мобильных устройств. Факторы риска для владельцев мобильных устройств.

Практика. Сравнительный анализ популярных ОС.

Тема 5.2. Источники заражения мобильных устройств.

Теория. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).

Практика. Популярные типы вредоносного мобильного ПО.

Тема 5.3. Угрозы для IOS-устройств. Угрозы для Android-устройств.

Теория. Сравнительный анализ мобильных операционных систем IOS и Android.

Практика. Распространенные виды угроз для IOS-устройств и Android-устройств.

Тема 5.4. Рост числа угроз для мобильных устройств. Вирусы для мобильных устройств.

Теория. Типы вирусов мобильных устройств (мобильные банкеры и др.) и методы борьбы с ними.

Практика. Проверка на безопасность различных приложений, установка, удаление. Работа с антивирусом на мобильном телефоне.

Тема 5.5. Представление результатов проделанной работы.

Практика. Подготовка к защите проекта (исследования).

Форма подведения итогов: представление результатов исследований – защита проектов.

Кейс 6. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.

В рамках кейса 6 учащиеся изучат общие понятия о работе с сетями WiFi, научатся распознавать угрозы безопасности WiFi-сетей, рационально и безопасно использовать сервисы для проверки безопасности пользователя (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС и др.). Задача кейса основывается на анализе сети WiFi в ЦЦО IT-Куб. Проблемная ситуация подводит учащихся к необходимости использования сервисов для безопасности пользователя в интернете и настройке безопасности в сетях WiFi. Учащимся будет предложено изучить сеть WiFi в ЦЦО IT-Куб, сделать анализ и составить мнение о том, есть ли угрозы данной сети.

Учащиеся должны знать:

–и применять методы защиты сетей WiFi;

–принципы настройки безопасности сетей WiFi, пользователя в интернете.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–проверять компьютер и файлы на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС;

–описывать и резюмировать результаты исследования;

–готовить презентацию и другие материалы для публичного представления;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя;

–определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;

–создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 6.1. Общие понятия об устройстве WiFi сетей.

Теория. Передача информации по беспроводному интерфейсу IEEE 802.11.

Практика. Точки доступа AP (Access Point).

Тема 6.2. Угрозы безопасности WiFi-сетей.

Теория. Прямые и косвенные угрозы. Опасности при работе с открытыми

WiFi-сетями.

Практика. Разработка рекомендаций по безопасной работе в открытых WiFi-сетях.

Тема 6.3. Анализ трафика. Сниффинг.

Теория. Сетевая атака, сниффинг пакетов. Понятие сниффинга, правовое регулирование.

Практика. Работа сниффера на примере незащищенного соединения http.

Тема 6.4. Методы защиты сетей WiFi. Меры безопасности для пользователя WiFi. Настройка безопасности.

Теория. Типы шифрования в Wi-Fi. Методы ограничения доступа. Методы аутентификации.

Практика. Установка и настройка Wi-Fi-роутера.

Тема 6.5. Настройка безопасной WiFi сети.

Теория. Атаки на сети WiFi.

Практика. Установка и настройка Wi-Fi-роутера.

Тема 6.6. Онлайн сервисы для безопасности пользователя в интернете.

Теория. Знакомство с полезными онлайн сервисами для безопасности пользователя в интернете.

Практика. Проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС.

Тема 6.7. Представление результатов проделанной работы.

Практика. Подготовка к защите проекта (исследования).

Форма подведения итогов: представление результатов исследований – защита проектов.

Кейс 7. Проектная деятельность.

В рамках кейса 7 учащиеся научатся определять совокупность мероприятий для разработки нового продукта или улучшения существующего продукта. Изученный материал подводит учащихся к необходимости создания

собственного проекта, где решаются актуальные вопросы, связанные с темой направления. Учащимся будет предложена формулировка цели в соответствии с принципами «smart», которую можно применять и в жизни. Также учащиеся смогут продемонстрировать собственные умения и навыки, представление результатов проделанной работы.

Учащиеся должны знать:

–и применять методы обработки информации;

–принципы безопасного и рационального использования личных и персональных данных в социальных сетях.

Учащиеся должны уметь:

–планировать исследование;

–работать в системах совместного редактирования документов;

–строить таблицы и диаграммы для визуализации данных исследования;

–выявлять индивидуальные особенности пользователя в системе «Крибрум»;

–проводить контент-анализ;

–выявлять большие данные;

–исследовать нейросети;

–описывать и резюмировать результаты исследования;

–создавать презентацию и другие материалы для публичного представления;

–работать в команде и давать обратную связь;

–представлять свой проект, свою команду и себя;

–определять социально-демографические характеристики и индивидуальные особенности людей на основе аккаунтов в социальных сетях;

–создавать позитивный имидж в социальных сетях.

Формы занятий, используемые при изучении данного модуля:

интерактивная лекция,

практическая работа,

самостоятельная командная работа,

защита проектов.

Тема 7.1. Знакомство с понятием «Проект».

Теория. Понятие «Проект». Использование инструментов и доступных ресурсов в проектной деятельности.

Тема 7.2. Жизненный цикл проекта.

Теория. Жизненный цикл проекта.

Тема 7.3. Выбор темы проекта. Проблематизая, целеполагание и постановка задач пути решения выбранной темы.

Теория. Выбор темы проекта. Проблематизая, целеполагание и постановка задач пути решения выбранной темы.

Практика. Подготовка к защите проекта (исследования).

Тема 7.4. Анализ выполненной работы, подготовка выступления к представлению результатов проделанной работы.

Теория. Анализ выполненной работы, подготовка выступления к представлению результатов проделанной работы.

Практика. Подготовка к защите проекта (исследования).

Тема 7.5. Представление результатов проделанной работы.

Практика. Подготовка к защите проекта (исследования).

Форма подведения итогов: представление результатов исследований – защита проектов.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Во время проведения курса предполагается текущий, промежуточный и итоговый контроль. Промежуточная аттестация обучающихся по данной программе проводится в форме опросов, тестирований, практических работ по каждому кейсу. Кроме того, проверка результатов освоения программы осуществляется постоянно: после изучения каждого раздела программы, учащиеся проходят контрольные тестирования.

Входной контроль – не проводится.

Текущий контроль осуществляется на занятиях в течение всего обучения для отслеживания уровня освоения учебного материала программы.

Формы:

−опрос теоретического материала;

−контрольные тесты.

Промежуточная аттестация проводится с целью выявления уровня освоения программ обучающимися и уровня развития личностных качеств по завершению каждого курса программы.

Формы:

−опрос теоретического материала;

−контрольные тесты;

−практические работы;

−лабораторные работы.

Итоговое оценивание проводится в конце обучения по курсу.

Форма: представление результатов исследований – итоговая защита проектов.

Оценка	**Результат**
Высокий уровень	- Сформированы систематическое знание основных понятий информационной безопасности, - Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет. - Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию. - Самостоятельно, неординарно решает задачи, способен сам найти свой путь решения. - Проявляет интерес и творческое отношение к изучаемым темам, стремится получить дополнительную информацию. - Может самостоятельно оценить свои возможности в выполнении задания, учитывая изменения известных способов действия. - Проявляет самостоятельность, пунктуальность и ответственность в подготовке к занятиям.
Средний уровень	- Знания в области основных понятий информационной безопасности не систематизированы, хаотичны, частично ошибочные. - Навыки безопасного поведения при работе с компьютерными программами, информацией в сети интернет частично имеются. Иногда нужна помощь. - Интерес возникает к новому материалу, но не к способам его применения на практике. - Может с помощью педагога безопасно работать с информацией, анализировать и обобщать полученную информацию. - Проявляет самостоятельность, но при подготовке к занятиям требуется внешняя стимуляция.
Низкий уровень	- Знания в области основных понятий информационной безопасности отсутствуют. Имеющиеся представления часто ошибочны. - Учащийся не умеет, не пытается и не испытывает потребности в оценке своих действий – ни самостоятельной, ни по просьбе педагога. - Уровень самостоятельности учащихся низкий, при подготовке к занятиям требуется постоянная внешняя стимуляция. - В совместной деятельности не пытается договориться, не может прийти к согласию, настаивает на своем, конфликтует или игнорирует других.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Тема кейса	Форма занятий	Приёмы и методы организации образовательного процесса	Дидактический материал. Электронные источники	Техническое оснащение и расходный материал	Форма подведения итогов
Кейс 1. Основы анализа информации в интернет-пространстве.	Комбинированная	Метод проектов. Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. Бодалев А.А., Столин В.В. Общая психодиагностика. СПб.: Речь, 2000. 2. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004. 3. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010. 4. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012. 5. Елисеев О.П. Практикум по психологии личности. СПб.: Питер, 2001. 6. Кравченко А.И. Методология и методы социологических исследований. Учебник. М.: Юрайт, 2015. 7. Словарь молодежного и интернет-сленга / Авт.-сост. Н.В. Белов. Минск: Харвест, 2007. 8. Слугина Н. Активные пользователи	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное оборудование.	Тестирование

			социальных сетей Интернета. СПб.: Питер, 2013. 9. 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.	● Магнитно-маркерная доска.	
Кейс 2. Угрозы в интернет-пространстве, методы противодействия.	Комбинированная	Метод проектов. Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. 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. 2. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013. 3. 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. 4. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2013. 5. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное	Тестирование

			всероссийского исследования. М.: Фонд Развития Интернет, 2013. 6. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66.	оборудование. ● Магнитно-маркерная доска.	
Кейс 3. Основы работы в социальных сетях.	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. 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. 2. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004. 3. . Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010. 4. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012. 5. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции,	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное	Тестирование

			безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2013. 6. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011. 7. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.	оборудование. ● Магнитно-маркерная доска.	
Кейс 4. Распознавание опасного и вредного контента в интернет-пространстве.	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012. 2. 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. 3. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011. 4. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.).	Тестирование

				● Презентационное оборудование. ● Магнитно-маркерная доска.	
Кейс 5. Безопасность мобильных устройств.	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. 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. 2. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004. 3. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010. 4. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012. 5. 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. 6. Ших К. Эра Facebook. М.: Манн,	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное оборудование. Магнитно-маркерная доска.	Тестирование

			Иванов и Фербер, 2011. 7. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.		
Кейс 6. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. 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. 2. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004. 3. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010. 4. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012. 5. 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.	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное оборудование. Магнитно-маркерная доска.	Тестирование

			6. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011. 7. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.		
Кейс 7. Проектная деятельность.	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	1. В.С. Лазарев, Проектная деятельность в школе Учебное пособие для учащихся 7 – 11 классов. М.: Книжный мир, 2019 2. Шагеева Г.Р. Проектная деятельность. Организация проектной деятельности на территории знаний в учебных заведениях. Проект как неотъемлемая часть учебного процесса. Учебно-методическое пособие. СПб.: Учебный дом, 2023.	● Ноутбуки с мышкой, наушниками и доступом к сети Интернет. ● Программное обеспечение: – система «Крибрум» с массивами данных для кейсов. – Пакет «Microsoft Office». – Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер». – Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.). – Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.). ● Презентационное оборудование. Магнитно-маркерная доска.	Презентация проделанной работы

КАДРОВОЕ ОБЕСПЕЧЕНИЕ

Преподавание данной программы могут осуществлять педагогические работники, владеющие набором профессиональных навыков в области информационно-коммуникационных технологий, при наличии необходимых компетенций и уровня профильной подготовки.

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО КУРСУ

Для реализации курса «Кибергигиена и работа с большими данными» помещение должно соответствовать следующим характеристикам:

− аудитории, оборудованы интерактивной доской, проектором, ноутбуком.

− каждый обучающийся выполняет практические работы за отдельным компьютером с сохранением результатов в облачном хранилище.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

1. Перечень литературы, необходимой для освоения программы:

1.1. Перечень литературы, использованной при написании программы:

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. Баскаков А.Я., Туленков Н.В. Методология научного исследования: Учеб. пособие. К.: МАУП, 2004.

4. Бек У. Общество риска. На пути к другому модерну. М.: Прогресс Традиция, 2000.

5. Бережнова Е.В., Краевский В.В. Основы исследовательской деятельности студентов: учеб. пособие для студ. сред. учеб. заведений. М.: Издат. центр «Академия», 2007.

6. Бехтерев С.В. Майнд-менеджмент. Решение бизнес-задач с помощью интеллект-карт. М.: Альпина Паблишер, 2012.

7. 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.

8. Бодалев А.А., Столин В.В. Общая психодиагностика. СПб.: Речь, 2000.

9. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004.

10. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010.

1.2. Перечень литературы, рекомендованной обучающимся:

2. Говор С.А., Теделури М.М., Шулаева О.В. Рабочая программа по направлению «Кибергигиена». – Москва, 2019 г.

3. Методическое пособие по направлению «Dataквантум». – Москва, 2018 г.

1.3. Перечень литературы, рекомендованной родителям:

1. Крупник А.Б. Поиск в Интернете: самоучитель. СПБ.: Питер, 2004.

2. Лукина М.М. Интернет-СМИ: Теория и практика. М.: Аспект-Пресс. 2010.

1.4 Перечень раздаточного материала:

1. Тематические презентации.

2. Информационное обеспечение

Программное обеспечение:

Операционная система (Windows, Linux, macOS). Офисное программное обеспечение.

2.1 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения программы:

1. https://uchi.ru
2. https://урок.рф
3. https://education.yandex.ru
4. https://resh.edu.ru