

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Свердловской области
Управление образования Березовского муниципального округа
БМАОУ СОШ №45

РАССМОТРЕНО

руководитель предметной
кафедры

СОГЛАСОВАНО

заместитель директора по
УВР

УТВЕРЖДЕНО

директор БМАОУ СОШ
№45

А.С. Элрик

Т.Г. Вараксина

Л.В. Нохрина

Протокол от «25» августа
2025 г. № 1

«26» августа 2025 г.

Приказ от «29» августа
2025 г. № 102

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
(ID 7469908)

Информационная безопасность
для обучающихся 7-9 классов

Березовский, 2025

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

"Информационная безопасность"

Программа внеурочной деятельности разработана на основании следующих нормативных актов:

Конституция Российской Федерации;

Конвенция о правах ребенка;

Федеральный Закон «Об образовании в Российской Федерации» от 29.12.2012 г. № 273 – ФЗ;

Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

Постановление Министерства труда и социального развития Российской Федерации от 27.09.1996 № 1 «Об утверждении Положения о профессиональной ориентации и психологической поддержке населения в Российской Федерации»;

Приказ об утверждении ФГОС ООО Министерства образования и науки РФ от 17 декабря 2010 года №1897 (зарегистрирован Минюстом России 1 февраля 2011 года №19644);

Письмо Министерства образования и науки РФ от 12 мая 2011 г. № 03-296 "Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования";

Постановление Главного государственного санитарного врача РФ от 29 декабря 2010 года № 189 «Об утверждении СанПиН 2.4.2.28210 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях».

Устав БМАОУ СОШ № 45;

Рабочая программа воспитания БМАОУ СОШ № 45.

Программа курса «Информационная безопасность» составлена для учащихся 7-9 классов, учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

Курс «Информационная безопасность» («Информационная безопасность») является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

"Информационная безопасность"

Основными целями изучения курса «Информационная безопасность» являются:

обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственными отношениями к взаимодействию в современной информационно-телекоммуникационной среде;

сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;

сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "Информационная безопасность" В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

На освоение учебного курса внеурочной деятельности «Информационная безопасность» отведен 51 учебный час, 17 часов в 7 классе, 17 часов в 8 классе, 17 часов в 9 классе.

Срок освоения рабочей программы: 7-8 классы – 3 года.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "Информационная безопасность"

1. **Лекции и презентации:** Теоретические занятия, на которых учащиеся знакомятся с основами информационной безопасности, изучают угрозы и методы защиты данных.

2. **Практические упражнения:** Выполнение заданий, направленных на освоение инструментов и методов защиты информации, таких как установка антивирусного ПО, настройка параметров безопасности в социальных сетях и на устройствах.

3. **Квесты и игры:** Интерактивные игры и квесты, направленные на развитие навыков распознавания фишинговых атак, защиты от вредоносного ПО и других угроз.

4. **Дискуссии и дебаты:** Обсуждение актуальных тем, связанных с информационной безопасностью, развитие навыков критического мышления и анализа информации.

5. **Тренинги и мастер-классы:** Интенсивные занятия, направленные на отработку конкретных навыков, таких как создание надежных паролей, защита от кибербуллинга и управление конфиденциальной информацией.

6. **Групповые проекты:** Совместная работа над проектами, требующими анализа и решения проблем информационной безопасности, что способствует развитию командных навыков и умений работать в коллективе.

7. **Кинотренинги:** Просмотр и обсуждение фильмов или видеороликов, посвященных теме информационной безопасности, с последующим анализом поведения персонажей и обсуждением эффективных стратегий защиты данных.

8. **Индивидуальные консультации:** Предоставление возможности учащимся получить индивидуальную консультацию по вопросам, связанным с информационной безопасностью, и получить персональные рекомендации.

9. **Онлайн-курсы и вебинары:** Использование цифровых платформ для проведения занятий и предоставления дополнительного материала для самостоятельного изучения.

10. **Хакатоны и соревнования:** Участие в соревнованиях по информационной безопасности, где учащиеся могут продемонстрировать свои навыки и знания в решении реальных задач.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «Информационная безопасность»

Отбор тематики **содержания курса** осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов.

В преподавании курса «Информационная безопасность» могут использоваться разнообразные форматы обучения: коллективная и групповая формы работы, тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат. Содержание программы курса внеурочной деятельности «Информационная безопасность» («Информационная безопасность») соответствует темам основной образовательной программы основного общего образования (ООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами: «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

7 класс

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей.

Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях.

Настройки приватности и конфиденциальности в разных социальных сетях.

Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов.

8 класс

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов.

9 класс

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям.

Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Планируемые результаты освоения курса внеурочной деятельности.

Личностные

осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;

освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;

сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

идентифицировать собственные проблемы и определять главную проблему; выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;

ставить цель деятельности на основе определенной проблемы и существующих возможностей;

выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;

составлять план решения проблемы (выполнения проекта, проведения исследования);

описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;

оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;

находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;

работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;

принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

выделять явление из общего ряда других явлений;

определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;

строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;

излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;

самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;

критически оценивать содержание и форму текста;

определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

строить позитивные отношения в процессе учебной и познавательной деятельности;

критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;

договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;

делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.

целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;

выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;

использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;

использовать информацию с учетом этических и правовых норм;

создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные

Выпускник научится:

анализировать доменные имена компьютеров и адреса документов в интернете;

безопасно использовать средства коммуникации,

безопасно вести и применять способы самозащиты при попытке мошенничества,

безопасно использовать ресурсы интернета.

Выпускник овладеет:

приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

основами соблюдения норм информационной этики и права;

основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных. Соблюдать нормы информационной этики и права.

Тематическое планирование

7 класс (17 часов)

№ занятия	Название раздела, темы	Кол-во часов
1	Общение в социальных сетях и мессенджерах	2
2	С кем безопасно общаться в интернете	1
3	Пароли для аккаунтов социальных сетей	1
4	Безопасный вход в аккаунты	2
5	Настройки конфиденциальности в социальных сетях	2
6	Публикация информации в социальных сетях	1
7	Кибербуллинг	2
8	Публичные аккаунты	1
9	Фишинг	2
10	Выполнение теста	1
11	Выполнение и защита индивидуальных и групповых проектов	2
Итого		17

8 класс (17 часов)

№ занятия	Название раздела, темы	Кол-во часов
1	Что такое вредоносный код	3
2	Распространение вредоносного кода	3
3	Методы защиты от вредоносных программ	4
4	Распространение вредоносного кода для мобильных устройств	3
5	Выполнение теста	1
6	Выполнение и защита индивидуальных и групповых проектов	3
Итого		17

9 класс (17 часов)

№ занятия	Название раздела, темы	Кол-во часов
1	Социальная инженерия: распознать и избежать	3
2	Ложная информация в Интернете	2
3	Безопасность при использовании платежных карт в Интернете	2
4	Беспроводная технология связи	2
5	Резервное копирование данных	2

6	Основы государственной политики в области формирования культуры информационной безопасности	2
7	Выполнение теста	1
8	Выполнение и защита индивидуальных и групповых проектов	3
Итого		17

Календарно – тематическое планирование

7 класс

<i>№ урока</i>	<i>Темы занятий</i>	<i>Форма проведения занятий</i>	<i>Кол-во час.</i>	<i>Цифровые образовательные ресурсы (электронные)</i>
1	Общение в социальных сетях и мессенджерах	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
2	Источники угроз, поступающих на мобильный телефон, компьютер. Способы кодирования информации.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
3	С кем безопасно общаться в интернете	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
4	Пароли для аккаунтов социальных сетей	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
5	Безопасный вход в аккаунты	Практическая работа.	1	Защита детей — Методические материалы для учителей
6	Правила регистрации на сайтах без распространения личных данных. Передача информации	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
7	Настройки конфиденциальности в социальных сетях	Практическая работа.	1	Защита детей — Методические материалы для

				учителей
8	Правила выбора полезных ресурсов в Интернете. Хранение информации.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
9	Публикация информации в социальных сетях	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
10	Кибербуллинг	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
11	Правила защиты от нежелательных сообщений и контактов.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
12	Публичные аккаунты	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
13	Фишинг	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
14	Правила использования аватара с учетом защиты личных данных.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
15	Выполнение теста	Практическая работа.	1	Защита детей — Методические материалы для учителей
16	Выполнение и защита индивидуальных и групповых проектов	Защита проектов	1	Защита детей — Методические материалы для учителей
17	Резервный урок	Резервный урок	1	Защита детей — Методические материалы для учителей

Календарно – тематическое планирование

8 класс

№ урока	Темы занятий	Форма проведения занятий	Кол- во час.	Цифровые образовательные (электронные) ресурсы
1	Что такое вредоносный код. Виды вредоносных кодов.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
2	Принципы распространение вредоносного кода.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
3	Вредоносная рассылка. Вредоносные скрипты.	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
4	Распространение вредоносного кода	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
5	Способы выявления наличия вредоносных кодов на устройствах.	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
6	Действия при обнаружении вредоносных кодов на устройствах.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
7	Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
8	Антивирусные программы и их характеристики.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
9	Антивирусные программы и их различия.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
10	Правила защиты от вредоносных кодов.	Поиск информации. Мини-доклады.	1	Защита детей — Методические

				материалы для учителей
11	Распространение вредоносного кода для мобильных устройств.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
12	Расширения вредоносных кодов для мобильных устройств.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
13	Правила безопасности при установке приложений на мобильные устройства.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
14	Выполнение теста	Практическая работа.	1	Защита детей — Методические материалы для учителей
15	Выполнение индивидуальных проектов	Практическая работа. Поиск информации.	1	Защита детей — Методические материалы для учителей
16	Выполнение групповых проектов	Практическая работа. Поиск информации.	1	Защита детей — Методические материалы для учителей
17	Выполнение и защита индивидуальных и групповых проектов	Защита проектов	1	Защита детей — Методические материалы для учителей

Календарно – тематическое планирование

9 класс

<i>№ урока</i>	<i>Темы занятий</i>	<i>Форма проведения занятий</i>	<i>Кол-во час.</i>	<i>Цифровые образовательные ресурсы (электронные)</i>
1	Социальная инженерия: распознать и избежать.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей

2	Правила безопасности при виртуальных контактах.	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
3	Персональные данные как основной капитал личного пространства в цифровом мире.	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
4	Ложная информация в Интернете	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
5	Фейковые новости. Поддельные страницы	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
6	Безопасность при использовании платежных карт в Интернете	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
7	Транзакции и связанные с ними риски. Правила совершения онлайн-покупок. Безопасность банковских сервисов	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
8	Беспроводная технология связи	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
9	Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
10	Резервное копирование данных	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей
11	Безопасность личной информации. Создание резервных копий на различных устройствах	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
12	Основы государственной политики в области формирования культуры информационной безопасности	Эвристическая беседа. Поиск информации.	1	Защита детей — Методические материалы для учителей

13	Основы культуры информационной безопасности.	Поиск информации. Мини-доклады.	1	Защита детей — Методические материалы для учителей
14	Выполнение теста	Практическая работа.	1	Защита детей — Методические материалы для учителей
15	Выполнение индивидуальных проектов	Практическая работа. Поиск информации.	1	Защита детей — Методические материалы для учителей
16	Выполнение групповых проектов	Практическая работа. Поиск информации.	1	Защита детей — Методические материалы для учителей
17	Защита индивидуальных и групповых проектов	Защита проектов	1	Защита детей — Методические материалы для учителей

Список источников:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К.
2. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
3. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов;
4. Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
5. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
6. Дети в информационном обществе // <http://detionline.com/journal/about> Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.
7. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
8. Защита детей by Kaspersky // <https://kids.kaspersky.ru/> Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайт, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
10. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>

11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Расказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.
14. Цветкова М.С., Хлобыстова И.Ю. Информационная безопасность. Кибербезопасность. 7–9 класс. Учебник.