

**Государственное бюджетное общеобразовательное учреждение Самарской
области средняя общеобразовательная школа с. Екатериновка
муниципального района Приволжский Самарской области**

РАССМОТРЕНА

руководитель ШМО
учителей естественно-
научного цикла и
гуманитарных наук
Анисимова О.Н.

Протокол № 1 от 28 августа
2023 г.

ПРОВЕРЕНА

заместитель
директора по УВР
Тимина С.В.
25 августа 2023 г.

УТВЕРЖДЕНА

директор ГБОУ СОШ с.
Екатериновка
Измайлова Е.Н.
Приказ № 70/2 от 31 августа
2023г.

РАБОЧАЯ ПРОГРАММА

Предмета внеурочной деятельности **«Информационная безопасность»**

для обучающихся 7 класса

с. Екатериновка 2023 год

Пояснительная записка

Рабочая программа по внеурочной деятельности «Информационная безопасность» в 7 классе разработана в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);
- ФГОС ООО, утвержденным приказом Министерства просвещения России от 31.05.2021 N 287 "Об утверждении федерального государственного образовательного стандарта основного общего образования" (с изменениями и дополнениями);
- ООП ООО ГБОУ СОШ с Екатериновка, утвержденной приказом № 70/2 от 31.08.2023 г.

Программа курса «Информационная безопасность» разработана на основе примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019). Цифровая гигиена: Самара, 2019 г.,

Общая характеристика курса внеурочной деятельности

«Информационная безопасность»

Курс внеурочной деятельности «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. Данный курс предполагает организацию работы в соответствии с содержанием модуля, предназначенных для обучающихся 7 класса.

Модуль . «Информационная безопасность»

1. Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7 класса.

Цели изучения курса внеурочной деятельности «Информационная безопасность»:

- 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 ответственного отношения 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 обучающихся, связанного с компьютерными технологиями и Интернетом.
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Место учебного курса (Модуль 1) в учебном плане

Программа учебного курса «Информационная безопасность» (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 «Информационная безопасность» отводится 1 час в неделю в 7 классе. Учебные занятия по программе реализованы в течение одного учебного года в 7 классе.

Содержание курса внеурочной деятельности «Информационная безопасность»

Тема раздела 1 «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час. Теоретические сведения: Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

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. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

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

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

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

Тема 8. Публичные аккаунты. 1 час.

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

Тема 9. Фишинг. 2 часа.

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. 3 часа.

Тестирование.

Темы проектов:

1. Влияние социальных сетей на образ жизни современных подростков.
2. Сленг, используемый в социальных сетях.
3. Случайны ли орфографические ошибки при общении в социальных сетях и мессенджерах?

Тема раздела 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

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. 2 часа.

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

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

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

Тестирование по теме «Безопасность устройств»

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Темы проектов:

1. Спрос рождает предложение или предложение рождает спрос на рынке антивирусного программного обеспечения.
2. Нормативно-правовая база в законодательстве РФ по вопросам охраны баз данных, защиты личной информации и электронной подписи, авторского права на программу или приложение, права распространения информации и использования персональных данных в Интернете.
3. Полезные навыки для обеспечения безопасности устройств.

Тема раздела 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

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

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

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

Тема 4. Беспроводная технология связи. 1 час.

Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к данной рабочей программе Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. Тестирование по теме «Безопасность информации»

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Темы проектов:

1. Фейки – это хорошо или плохо?
2. Как проводить маркетинговые исследования онлайн?
3. Достоинства и недостатки онлайн-шопинга.

Повторение. Резерв. 3 часа.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микро обучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу,

определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микро обучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

Планируемые результаты освоения курса внеурочной деятельности **«Информационная безопасность»:**

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.

Предметные: Ученик 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.

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

Ученик получит возможность научиться:

- основам соблюдения норм информационной этики и права;
- основам самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- приемам безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Метапредметные.

Регулятивные универсальные учебные действия. Ученик научится:

- 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.

Ученик научится:

- 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.

Ученик научится:

- 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.

Тематическое планирование

7 класс

№ п/п	Тема урока	Кол-во часов	Характеристика основных видов учебной деятельности обучающихся	Электронные образовательные ресурсы
Тема раздела 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах форма (практикум)	1	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
2	С кем безопасно общаться в интернете форма (тренинг)	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
3	Пароли для аккаунтов социальных сетей	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07

	форма (практическая работа)			07
4	Безопасный вход в Аккаунты форма (видеоролик)	1	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа в Интернет с чужого компьютера..	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
5	Настройки конфиденциальности	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
6	Публикация информации в социальных сетях форма (тренинг)	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
7	Кибербуллинг форма (лекция)	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.	https://lesson.edu.ru/lesson/96e9fb5d-15b0-498b-ad01-3693e7989970?backUrl=%2F05%2F09
8	Публичные аккаунты форма (практикум)	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.	https://lesson.edu.ru/lesson/e3d08803-0bab-49ab-b40d-5c4753f5a9d3?backUrl=%2F05%2F07
9-10	Фишинг форма (лекция)	2	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.	https://lesson.edu.ru/lesson/96e9fb5d-15b0-498b-ad01-3693e7989970?backUrl=%2F05%2F09
11-13	Выполнение защита индивидуальных и групповых проектов (проектирование)	3	Самостоятельная работа.	
Тема раздела 2. «Безопасность устройств»				
14	Что такое вредоносный код форма (составление памяток)	1	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07

			средства и сервисы адекватно задаче.	
15	Распространение вредоносного кода(анализ защищенности собственных аккаунтов в социальных сетях)	1	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
16-17	Методы защиты от вредоносных программ форма (презентация)	2	Изучает виды антивирусных программ и правила их установки.	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
18	Распространение вредоносного кода для мобильных устройств форма (презентация, памятка)	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
19-21	Выполнение и защита индивидуальных и групповых проектов (проектирование)	3	Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.	
Тема раздела 3 «Безопасность информации»				
22	Социальная инженерия: распознать и избежать форма (практикум)	1	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.	
23	Ложная информация в Интернете (анализ проверки аккаунтов) форма (практическая работа)	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
24	Безопасность при использовании платежных карт в	1	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить	

	Интернете форма (игра)		источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.	
25	Беспроводная технология связи форма (путешествие в Интернет)	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
26	Резервное копирование данных форма (работа с памяткой)	1	Создает резервные копии.	https://lesson.edu.ru/lesson/e3d08803-0bab-49ab-b40d-5c4753f5a9d3?backUrl=%2F05%2F07
27-28	Основы государственной политики в области формирования культуры информационной безопасности форма (работа с видеороликом)	2	Умеет привести выдержки из законодательства РФ: -обеспечивающего конституционное право на поиск, получение и распространение информации; -отражающего правовые аспекты защиты киберпространства.	https://lesson.edu.ru/lesson/02544700-f7db-4e42-8dae-65a55af5fedb?backUrl=%2F05%2F09
29-31	Выполнение и защита индивидуальных и групповых проектов (Проектирование)	3		
32-34	Повторение резерв	3		
	Итого	34		

Поурочное планирование внеурочной деятельности

7 класс

№ п/п	Тема урока	Кол-во часов	Характеристика основных видов учебной деятельности обучающихся	Электронные образовательные ресурсы
Тема раздела 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах форма (практикум)	1	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
2	С кем безопасно общаться в интернете форма (тренинг)	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
3	Пароли для аккаунтов социальных сетей форма (практическая работа)	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
4	Безопасный вход в Аккаунты форма (видеоролик)	1	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа в Интернет с чужого компьютера..	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
5	Настройки конфиденциальности	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
6	Публикация информации в социальных сетях форма (тренинг)	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
7	Кибербуллинг форма (лекция)	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных	https://lesson.edu.ru/lesson/96e9fb5d-15b0-498b-ad01-3693e7989970?backUrl=%2F05%2F09

			собеседников.	
8	Публичные аккаунты форма (практикум)	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.	https://lesson.edu.ru/lesson/e3d08803-0bab-49ab-b40d-5c4753f5a9d3?backUrl=%2F05%2F07
9	Фишинг форма (лекция)	1	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых.	https://lesson.edu.ru/lesson/96e9fb5d-15b0-498b-ad01-3693e7989970?backUrl=%2F05%2F09
10	Фишинг форма (лекция)	1	Разработка и распространение чек-листа (памятки) по противодействию фишингу.	https://lesson.edu.ru/lesson/96e9fb5d-15b0-498b-ad01-3693e7989970?backUrl=%2F05%2F09
11	Выполнение защита индивидуальных и групповых проектов (проектирование)	1	Самостоятельная работа.	https://lesson.edu.ru/lesson/0e60abadd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
12	Выполнение защита индивидуальных и групповых проектов (проектирование)	1	Самостоятельная работа.	
13	Выполнение защита индивидуальных и групповых проектов (проектирование)	1	Самостоятельная работа.	
Тема раздела 2. «Безопасность устройств»				
14	Что такое вредоносный код форма (составление памяток)	1	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.	https://lesson.edu.ru/lesson/7f85d5add-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
15	Распространение вредоносного кода(анализ защищенности собственных)	1	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.	https://lesson.edu.ru/lesson/7f85d5add-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07

	аккаунтов в социальных сетях)			
16	Методы защиты от вредоносных программ форма (презентация)	1	Изучает виды антивирусных программ и правила их установки.	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
17	Методы защиты от вредоносных программ форма (практические задания)	1	Устанавливает антивирусные программы на гаджеты,	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
18	Распространение вредоносного кода для мобильных устройств форма (презентация, памятка)	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.	https://lesson.edu.ru/lesson/7f85d5ad-e71a-4b16-8a0e-60ba7b5ac559?backUrl=%2F05%2F07
19	Выполнение и защита индивидуальных и групповых проектов (проектирование)	1	Умеет работать индивидуально и в группе. Приемы работы индивидуально, в группе.	https://lesson.edu.ru/lesson/0e60abadd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
20	Выполнение и защита индивидуальных и групповых проектов (проектирование)	1	Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.	https://lesson.edu.ru/lesson/0e60abadd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
21	Выполнение и защита индивидуальных и групповых проектов (проектирование)	1	Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.	https://lesson.edu.ru/lesson/0e60abadd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
Тема раздела 3 «Безопасность информации»				
22	Социальная инженерия: распознать и избежать форма (практикум)	1	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07

23	Ложная информация в Интернете (анализ проверки аккаунтов форма (практическая работа)	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
24	Безопасность при использовании платежных карт в Интернете форма (игра)	1	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.	
25	Беспроводная технология связи форма (путешествие в Интернет)	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
26	Резервное копирование данных форма (работа с памяткой)	1	Создает резервные копии.	https://lesson.edu.ru/lesson/e3d08803-0bab-49ab-b40d-5c4753f5a9d3?backUrl=%2F05%2F07
27	Основы государственной политики в области формирования культуры информационной безопасности форма (работа с видеороликом)	1	Умеет привести выдержки из законодательства РФ: -обеспечивающего конституционное право на поиск, получение и распространение информации; -отражающего правовые аспекты защиты киберпространства.	https://lesson.edu.ru/lesson/02544700-f7db-4e42-8dae-65a55af5fedb?backUrl=%2F05%2F09
28	Основы государственной политики в области формирования культуры информационной безопасности форма (работа с видеороликом)	1	Умеет привести выдержки из законодательства РФ: -обеспечивающего конституционное право на поиск, получение и распространение информации; -отражающего правовые аспекты защиты киберпространства.	https://lesson.edu.ru/lesson/02544700-f7db-4e42-8dae-65a55af5fedb?backUrl=%2F05%2F09

29	Выполнение и защита индивидуальных и групповых проектов (Проектирование)	1	Умеет грамотно заполнить документацию (портфолио) по проекту.	https://lesson.edu.ru/lesson/0e60abd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
30	Выполнение и защита индивидуальных и групповых проектов (Проектирование)	1	Умеет разрабатывать проект, следуя всем этапам работы над проектом.	https://lesson.edu.ru/lesson/0e60abd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
31	Выполнение и защита индивидуальных и групповых проектов (Проектирование)	1	Организует презентацию и защиту проекта в группе и индивидуально	https://lesson.edu.ru/lesson/0e60abd-6d9f-4a6b-b065-5ca7de183395?backUrl=%2F20%2F06
32	Повторение. Безопасность общения в Интернете (тестирование)	1	Рассматривает вопросы по безопасности общения. Разрабатывает памятку « Безопасное общение в интернете»	https://lesson.edu.ru/lesson/be05adc3-1aaf-4591-89e4-2196f4951e73?backUrl=%2F05%2F07
33	Повторение. Организация безопасности устройств (игра « Что? Где?Когда?»)	1	Рассматривает вопросы по организации безопасности устройств.	https://lesson.edu.ru/lesson/e75a619c-3285-44ef-ac0a-2fb7e5d11aa3?backUrl=%2F05%2F07
34	Повторение. Организация безопасности при обращении с информацией.	1	Рассматривает вопросы по безопасности общения. Разрабатывает памятку « Безопасное общение в интернете»	
	Итого	34		