Рабочая программа
по внеурочной деятельности

Название	«Информационная безопасность или на расстоянии одного вируса»
Класс	9В, 9М, 9Б
Ф.И.О. педагога	Артемова Елена Владимировна
Количество часов по учебному плану	34 часа

г. Красноярск, 2020-2021 учебный год

Пояснительная записка

Рабочая программа «Информационная безопасность или на расстоянии одного вируса» разработана для учащихся 9-х классов муниципального автономного общеобразовательного учреждения «Лицей № 3».

Рабочая программа разработана на основе следующих ***нормативно-правовых актов*:**

- Письмо Министерства образования и науки РФ «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования» от 12 мая 2011 г. № 03–2960.
- Методические рекомендации Министерства образования и науки РФ от 18.08.2017 г. № 1672 («О внеурочной деятельности и реализации дополнительных общеобразовательных программ».
- Примерная основная образовательная программа основного общего образования от 8.04.2015 № 1/15;
- Основная образовательная программа основного общего образования МАОУ Лицей № 3 (Приказ от 10.08.2020 № 202).

Направленность программы – общекультурное.

Актуальность реализации внеурочного курса «Информационная безопасность или на расстоянии одного вируса».

Курс «Информационная безопасность или на расстоянии одного вируса» разработан с учётом возрастных особенностей обучающихся: 14 – 16-летние подростки - активные пользователи Интернета. Доступ несовершеннолетних к сайтам в сети Интернет дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимать в них участие и использовать сеть Интернет в качестве источника для собственного развития. Однако использование интернета вместе с возможностями несет и риски.

Курс является важной составляющей работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры и т.п.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Реализация программы даёт возможность сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовывать информационный процесс). Курс поможет подростку определиться со способами защиты от противоправных посягательств в Интернете, защиты личных данных.

Значительное внимание в курсе уделяется формированию компетенций поиска, подбора, анализа и интерпретации информации из различных источников, представленных как на электронных, так и на твёрдых носителях.

Программа разработана на основе: Наместникова М.С., Информационная безопасность или на расстоянии одного вируса: сборник рабочих программ по внеурочной деятельности начального, основного, общего образования - М.: Просвещение, 2020.

Учебные пособия «Информационная безопасность или на расстоянии одного вируса» разработано совместными усилиями специалистов АО «Лаборатория Касперского» - международной компании, специализирующейся на разработке систем защиты от различных киберугроз, и АО «Издательство «Просвещение»; Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020.

Цель: создание условий для безопасного поведения учащихся в информационном пространстве.

Задачи:

- формировать у учащихся ценность безопасного образа жизни: навык в получении знаний и умения выявлять информационную угрозу, определять степень её опасности, предвидеть последствия информационной угрозы и противостоять им:

- дать представления учащимся о негативных тенденциях в развитии информационной культуры , необходимости обеспечивать себя от информационных рисков и угроз

- способствовать освоению учащимися социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах.

Время, отведенное на реализацию программы учебного курса.

Курс реализуется в 9-м классе из расчета 1 час в неделю. Всего 34 часа.

Курс «Информационная безопасность или на расстоянии одного вируса» реализуется в соответствии с учебно-календарным графиком – с 1.09.2020 по 24.05.2021 г.

Планируемы результаты освоения учебного предмета, курса (личностные, метапредметные, предметные результаты).

Требования к личностным результатам освоения курса:

- 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 учётом устойчивых познавательных интересов;
- сформированность ценности безопасного образа жизни;
- интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Требования к интеллектуальным (метапредметным) результатам освоения курса:

В ходе изучения учебного курса обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.

Регулятивные:

- умение самостоятельно обнаруживать и формулировать проблему в сфере информационной безопасности, выдвигать версии её решения, определять последовательность своих действий по её решению;
- проявление познавательной и творческой инициативы в применении полученных знаний и умений для решения задач в области общекультурных навыков работы с информацией;
- умение осуществлять самоконтроль, оценку, взаимооценку и самооценку выполнения действий по изучению вопросов информационной безопасности на основе выработанных критериев;
- умение описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач в сфере информационной безопасности;
- умение самостоятельно планировать действия по изучению вопросов информационной безопасности, в том числе в области личной безопасности, безопасности семьи.

Познавательные:

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

- умение находить различные способы защиты устройств от вредоносного кода;
- умение анализировать источники информации и правильно организовывать информационный процесс;

- умение переводить сложную по составу (многоаспектную) информацию из графического или формализованного (символьного) представления в текстовое, и наоборот;
- умение анализировать опыт разработки и реализации учебного проекта, исследования (теоретического, эмпирического) на основе предложенной проблемной ситуации, поставленной цели и/или заданных критериев оценки продукта/результата;
- определение необходимых ключевых поисковых слов и запросов;
- осуществление взаимодействия с электронными поисковыми системами, словарями, социальными сетями;
- умение анализировать способы защиты от противоправных посягательств в Интернете.

Коммуникативные:

- умение вступать в коммуникацию со сверстниками и учителем, понимать и продвигать предлагаемые идеи;
- умение анализировать и интерпретировать информацию, полученную из различных источников;
- умение организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.)
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбор и использование адекватной информационной модели для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использование компьютерных технологий (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.;
- использование информации с учётом этических и правовых норм;
- соблюдение информационной гигиены и правил информационной безопасности.

Требования к предметным результатам освоения курса:

- владение понятиями: вредоносные коды, источники информации, доменные имена компьютеров, адреса документов в Интернете, источники угроз, виды угроз, личная информация, фишинг, кибербулинг, киберпространство, киберкультура, киберугроза, социальная инженерия, нормы информационной этики и права.

владение знаниями:

- о современном информационном обществе,
- о безопасном использовании средств коммуникации,
- о безопасном применении способов самозащиты при попытке мошенничества,
- о безопасном использовании ресурсов Интернета
- об информационной безопасности личности и государства

Содержание учебного предмета, курса с указанием предметных и метапредметных результатов по разделам.

Содержание программы соответствует темам ПООП ООО по учебным предметам «Основы безопасности жизнедеятельности» и «Информационно-коммуникационные технологии и ИКТ», а также расширяет их за счёт привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и т.д.) по темам, позволяющим правильно ввести ребёнка в цифровое пространство и корректировать его поведение в виртуальном мире.

Перечень и название разделов, глав и тем реализуемого курса с указание количества часов

Номер темы/блока	Название темы/блока	Кол-во часов
Тема 1	Безопасность общения	16
Тема 2	Безопасность устройств	8
Тема 3	Безопасность информации	10
Итого		34

Содержание курса «Информационная безопасность или на расстоянии одного вируса»

Тема 1. Безопасность общения

Базовые понятия и знания:

- мессенджеры, социальные сети;
- пароли, онлайн генераторы паролей;
- аутентификация, приватность и конфиденциальность в мессенджерах;
- персональные данные;
- правила создания и хранения паролей;
- кибербулинг, фишинг.

Личностные характеристики и установки:

- понимание необходимости защиты персональных данных;
- осознание того, что фишинговые сайты могут получить доступ к конфиденциальным данным пользователей — логинам и паролям;
- готовность к повышению своего образовательного уровня и продолжению обучения с использованием средств и методов информатики и ИКТ;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, технических условий безопасной эксплуатации средств ИКТ;

Умения:

- распознавать фишинговые сайты;
- определять кибербулинг;
- создавать надежный пароль;
- настраивать приватность и конфиденциальность в разных социальных сетях;
- развивать критическое мышление.

Компетенции:

- оценивать последствия безопасного входа в аккаунты с чужого компьютера;
- оценивать последствия кибербулинга;
- оценивать безопасность настройки приватности и конфиденциальности в различных социальных сетях.

Тема 2. Безопасность устройств

Базовые понятия и знания:

- виды вредоносных кодов, возможности и деструктивные функции вредоносных кодов;
- вредоносные рассылка, скрипты;
- правила безопасности при установке приложений на мобильном телефоне.

Личностные характеристики и установки:

- понимание необходимости защиты мобильных устройств от вредоносного кода;
- осознание необходимости установки антивирусных программ.

Умения:

- распознавать вредоносные коды;
- определять оптимальные способы защиты устройств от вредоносных кодов;
- устанавливать антивирусные программы;
- развивать критическое мышление.

Компетенции:

- оценивать оптимальность способов защиты устройств от вредоносных кодов;
- оценивать последствия распространения вредоносного кода;
- оценивать уровень безопасности при установке приложений на мобильные устройства.

Тема 3. Безопасность информации.

Базовые понятия и знания:

- фейки, поддельные страницы;
- транзакции, онлайн покупки, безопасность банковских сервисов;
- правила безопасности при использовании публичных и непубличных сетей;
- правила безопасности при виртуальных контактах.

Личностные характеристики и установки:

- понимание необходимости защиты личной информации;
- ответственное отношение к информации с учетом правовых и этических аспектов ее распространения;
- осознание необходимости создания резервных копий на различных устройствах.

Умения:

- распознавать ложную информацию в Интернете;
- совершать безопасно онлайн покупки;
- распознавать фейковые новости, поддельные страницы;
- развивать критическое мышление.

Компетенции:

- оценивать последствия при подключении к публичной сети;
- оценивать безопасность банковских сервисов.

Формы, методы и инструменты осуществляемого контроля

Оценивание результатов обучения осуществляется в трёх формах: текущего контроля, промежуточного контроля и итогового контроля знаний.

Текущий контроль знаний осуществляется на занятиях-играх, практикумах и семинарах. Проверяется конструктивность работы учащегося на занятии, степень активности в поиске информации и отработке практических способов действий в сфере информационной безопасности, а также участие в групповом и общем обсуждении проблем (задач) и способов их решения.

Промежуточный контроль знаний проводится по результатам изучения каждого модуля. Данный вид контроля помогает проверить степень усвоения учебного материала, овладения предметными и метапредметными умениями и компетенциями по значительному ряду вопросов, объединённых в одном модуле. Задача промежуточного контроля - выявить те вопросы, которые учащиеся усвоили слабо (например, не смогли настроить приватность и конфиденциальность в различных социальных сетях).

Итоговый контроль знаний осуществляется по результатам изучения курса. Он направлен на проверку и оценку реальных достижений учащихся в освоении основ информационной безопасности, на выявление степени усвоения системы знаний, овладения умениями и навыками, полученными в процессе изучения курса.

Итоговый контроль может осуществляться в формате имитационно-ролевой или деловой игры. Игра позволит смоделировать конкретную жизненную ситуацию (или комплекс ситуаций), в которой учащийся сможет применить знания, умения и компетенции, освоенные в ходе обучения. Итоговый контроль проводится также в формате контрольной работы, включающей различные типы заданий.

Оценка учебных достижений

Оценка результатов учебной деятельности обучающихся осуществляется на основе определённых критериев, т. е. правил и признаков, по которым можно отличить одно явление от другого.

В ходе учебной деятельности учащиеся будут осуществлять различные виды деятельности, следовательно, за каждый вида деятельности и её результат определяются разные критерии оценки.

Оценочный лист учебных достижений по модулю

ФИО:	Модуль:	
Дата	Текущий контроль	Промежуточный контроль

Отметка								

Итоговый оценочный лист

	Результаты промежуточного контроля по каждому модулю			Итоговый контроль	Общая итоговая отметка
Номер раздела	1	2	3		
Дата					
Отметка					
Прим.					

Знакомство учащихся с критериями оценки осуществляется до начала работы. Очень важно, чтобы учащиеся знали, по каким основаниям будет оцениваться их работа на уроках. Ниже представлены критерии оценки той или иной учебной деятельности и учебных результатов, а также методика проведения оценки.

Оценка решения практических задач

Одним из важнейших умений, которое учащиеся осваивают в ходе обучения, является умение решать практические задачи в сфере информационной безопасности.

Объектом оценки является устный или письменный ответ, содержащий ход решения задачи.

Критерии оценки практической задачи следующие:

- определение (выявление в результате поиска) алгоритма решения практической задачи;
- оценка альтернатив;
- обоснование итогового выбора.

Учащиеся заранее (на первом занятии) знакомятся с критериями оценивания и способами оформления решения практических задач.

Оценка предметных знаний и умений

Проверка уровня овладения учащимися предметных знаний и умений может осуществляться в форме письменной контрольной работы или устного опроса.

Оценка устного ответа более субъективна, чем оценка письменного, тем не менее можно выделить несколько общих принципов оценивания:

- учащийся не отвечает на большинство вопросов (более 50%) или даёт неверные ответы – 1 балл;
- ученик правильно отвечает на половину вопросов или на большинство вопросов частично – 2 балла;
- учащийся даёт верные ответы на большинство вопросов (более 70%) или отвечает почти на все вопросы, но делает несколько существенных ошибок – 3 балла;
- учащийся правильно отвечает на все вопросы, делает несколько несущественных ошибок – 4 балла.

Оценивание письменной контрольной работы осуществляется следующим образом:

- за каждый правильный ответ на тестовый вопрос - 1 балл;
- за каждую решённую предметную задачу - 2, 3 или 4 балла;
- за каждую практическую мини-задачу - 3, 4 или 5 баллов;
- за развёрнутый письменный ответ на вопрос - 5, 6, 7 или 8 баллов.

Первую очередь оценивает качественный прирост в результатах творческо-учебной деятельности ученика.

Оценка выполнения проекта.

Критерии оценивания проекта:

- постановка проблемы, решаемой в ходе реализации проекта;
- сформированность и реализованность целей и задач проекта;
- разработанность плана по подготовке и реализации проекта;
  использование разнообразных информационных источников;
- качество реализации и представления проекта.

Требования к содержанию итоговых индивидуальных и групповых проектов

Критерии содержания текста проектов.

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом чётко определена, в необходимости исследования есть аргументы

2. Правильно составлен научный аппарат работы: точность формулировки проблемы, чёткость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствует теме работы

3. Есть планирование проектной деятельности, корректировка её в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта - распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно

4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников

5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектной работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены

6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения

7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях

Критерии презентации проектной работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержания работы, достаточная осведомлённость в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.

2. Умение чётко отвечать на вопросы после презентации работы

3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд — презентацию на соответствующем возрасту уровне

4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне

5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.)

6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение чётко обозначить пути создания сетевого продукта

7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути её исследования и проектного решения

Задания для оценивания результатов обучения:

- тематический тест – проверяет усвоение предметных знаний по данному разделу, формулируется в виде вопроса с несколькими вариантами ответа.
- тематические задания — проверяют усвоение предметных знаний и формирование умений, формулируются в виде заданий с открытым ответом;
- практические мини-задачи — проверяют овладение умениями и компетенциями в изучаемой области финансовой грамотности; формулируются в виде описания практической жизненной ситуации с указанием конкретных обстоятельств, в которых учащимся необходимо найти решение, используя освоенные знания и умения.

Календарно-тематическое планирование курса
«Информационная безопасность или на расстоянии одного вируса»

№	Тема	Основное содержание	Количество часов	9 М	9 В	9 Б
Тема 1. «Безопасность общения»						
1	Общение в социальных сетях и мессенджерах.	Социальная сеть. История социальных сетей. Мессенджеры..	**1**	5.09.20	5.09.20	5.09.20
2		Назначение социальных сетей и мессенджеров. Пользовательский контент	**1**	12.09.20	12.09.20	12.09.20
3	С кем безопасно общаться в интернете.	Правила добавления друзей в социальных сетях. Профиль пользователя.	**1**	19.09.20	19.09.20	19.09.20
4		Анонимные социальные сети.	**1**	26.09.20	26.09.20	26.09.20
5	Пароли для аккаунтов социальных сетей.	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	**1**	3.10.20	3.10.20	3.10.20
6	Безопасный вход в аккаунты	Виды аутентификации.	**1**	10.10.20	10.10.20	10.10.20
7		Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта	**1**	17.10.20	17.10.20	17.10.20
8	Настройки конфиденциальности в социальных сетях.	Настройки приватности и конфиденциальности в разных социальных сетях.	**1**	24.10.20	24.10.20	24.10.20
9		Приватность и конфиденциальность в мессенджерах.	**1**	31.10.20	31.10.20	31.10.20
10	Публикация информации в социальных сетях.	Персональные данные. Публикация личной информации.	**1**	14.11.20	14.11.20	14.11.20
11	Кибербуллинг.	Определение кибербуллинга.	**1**	21.11.20	21.11.20	21.11.20
12		Возможные причины кибербуллинга и как его избежать.	**1**	28.11.20	28.11.20	28.11.20
13	Публичные аккаунты.	Настройки приватности публичных страниц. Правила	**1**	5.12.20	5.12.20	5.12.20

		ведения публичных страниц.				
14	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга.	**1**	12.12.20	12.12.20	12.12.20
15		Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	**1**	19.12.20	19.12.20	19.12.20
16	Обобщение результатов работы	Выполнение тренировочных заданий, тестовый контроль	**1**	26.12.20	26.12.20	26.12.20
Тема 2. «Безопасность устройств»						
17	Что такое вредоносный код.	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов	**1**	16.01.21	16.01.21	16.01.21
18	Распространение вредоносного кода.	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.	**1**	23.01.21	23.01.21	23.01.21
19		Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах	**1**	30.01.21	30.01.21	30.01.21
20	Методы защиты от вредоносных программ.	Способы защиты устройств от вредоносного кода.	**1**	6.02.21	6.02.21	6.02.21
21		Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов	**1**	13.02.21	13.02.21	13.02.21
22	Распространение вредоносного кода для мобильных устройств.	Расширение вредоносных кодов для мобильных устройств.	**1**	20.02.21	20.02.21	20.02.21
23		Правила безопасности при установке приложений на мобильные устройства	**1**	27.02.21	27.02.21	27.02.21
24	Обобщение результатов работы	Выполнение тренировочных заданий, тестовый контроль	**1**	6.03.21	6.03.21	6.03.21
Тема 3 «Безопасность информации»						
25	Социальная инженерия: распознать и избежать.	Приемы социальной инженерии.	**1**	13.03.21	13.03.21	13.03.21
26		Правила безопасности при виртуальных контактах.	**1**	20.03.21	20.03.21	20.03.21
27	Ложная информация в Интернете.	Фейковые новости. Поддельные страницы.	**1**	23.03.21	23.03.21	23.03.21
28	Безопасность при использовании платежных карт в Интернете.	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	**1**	3.04.21	3.04.21	3.04.21
29	Беспроводная	Уязвимости Wi-Fi-соединений.	**1**	10.04.21	10.04.21	10.04.21

	технология связи.	Публичные и непубличные сети. Правила работы в публичных сетях				
30	Резервное копирование данных.	Безопасность личной информации. Создание резервных копий на различных устройствах	**1**	17.04.21	17.04.21	17.04.21
31	Выполнение теста.	Обсуждение тем индивидуальных и групповых проектов	**1**	24.04.21	24.04.21	24.04.21
32-34	Выполнение и защита индивидуальных и групповых проектов		**3**	8.05.21 15.05.21 22.05.21	8.05.21 15.05.21 22.05.21	8.05.21 15.05.21 22.05.21

Список литературы и интернет-ресурсов

1. АО «Лаборатория Касперского», АО «Издательство «Просвещение»; Информационная безопасность или на расстоянии одного вируса М.: Просвещение, 2020
2. Г.Э.Курис Азбука защиты информации, АО «Лаборатория Касперского», 2019
3. Колисниченко Д. Анонимность и безопасность в Интернете. От «чайника» к пользователю М: Просвещение, 2012
4. Наместникова М.С., Информационная безопасность или на расстоянии одного вируса: сборник рабочих программ по внеурочной деятельности начального, основного, общего образования - М.: Просвещение, 2020
5. Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020
6. Щаньгин В.Ф. Защита информации в компьютерных системах и сетях, М: Просвещение, 2018
7. https://pmdatalesson.1c.ru/data/
8. https://единыйурок.рф/index.php/proekty/urok
9. https://урокцифры.рф/