РОССИЙСКАЯ ФЕДЕРАЦИЯ
Краснодарский край
Администрация муниципального образования город Краснодар
Муниципальное автономное общеобразовательное учреждение муниципального образования город Краснодар средняя общеобразовательная школа №32 имени Дзержинского Феликса Эдмундовича

РАССМОТРЕНО МО учителей химии, физики, биологии, географии	СОГЛАСОВАНО	УТВЕРЖДЕНО решением педагогического совета
Руководитель МО_____ К.В. Процай	Заместитель директора _____ А.С. Листкова	Председатель _____ Недилько Т.В.
_____	_____	_____
«___»_____ 2023г.	«___»_____ 2023г.	«___»_____ 2023г.

ПОДПИСАНО ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Директор МАОУ СОШ № 32 города Краснодара
Недилько Татьяна Владиславовна

РАБОЧАЯ ПРОГРАММА

РАБОЧАЯ ПРОГРАММА КУРСА

«Технологии информационной безопасности»

для обучающихся 10-го класса

Краснодар, 2023г.

Оглавление

Пояснительная записка

Общая характеристика.

Программа курса «Технологии информационной безопасности» (далее – программа) для 10 класса составлена на основе положений и требований к результатам освоения основной образовательной программы, представленных в федеральном государственном образовательном стандарте среднего общего образования и федеральной образовательной программе (приказ Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования» (Зарегистрирован Минюстом России 7 июня 2012 г. № 24480); приказ Министерства просвещения Российской Федерации от 12.08.2022 № 732 «О внесении изменений в федеральный государственный образовательный стандарт среднего общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413» (Зарегистрирован Минюстом России 12.09.2022 № 70034); приказ Министерства просвещения Российской Федерации от 18.05.2023 № 371 «Об утверждении федеральной образовательной программы среднего общего образования» (Зарегистрирован Минюстом России 12.07.2023 № 74228).

Актуальность реализации программы

Программой предусмотрено формирование современного теоретического уровня знаний, а также практического опыта работы с современными электронно-вычислительными машинами, средствами защиты информации, средствами криптографической защиты информации, средствами защиты персональных данных, овладение приемами исследовательской деятельности. Методы организации образовательной и научно-исследовательской деятельности предусматривают формирование у обучающихся нестандартного творческого мышления, свободы самовыражения и индивидуальности суждений. Для полного учета потребностей обучающихся в программе используется дифференцированный подход, что стимулирует обучающегося к увеличению потребности в индивидуальной, интеллектуальной и познавательной деятельности и развитию научно-исследовательских навыков.

Таким образом, вовлеченность обучающихся в данную внеурочную деятельность позволит обеспечить их самоопределение, расширить зоны поиска своих интересов в различных сферах естественно-научных знаний, переосмыслить свои связи с окружающими, свое место среди других людей. В целом реализация программы вносит вклад в нравственное и социальное формирование личности.

Содержательные элементы программы предполагают организацию вокруг них поисково-исследовательской деятельности обучающихся, результаты которой могут быть оформлены и представлены для презентации и оценки в рамках выполнения:

– учебных исследований и проектов по учебному предмету «Информатика»;

– предметного или междисциплинарного «индивидуального проекта»,

являющегося обязательным для обучающихся 10–11 классов.)

Цели курса внеурочной деятельности

Целями изучения курса «**Технологии информационной безопасности**» являются:

воспитание ответственного и избирательного отношения к информации;

умения работать с различными видами информации, самостоятельно планировать и осуществлять индивидуальную и коллективную информационную деятельность, представлять и оценивать её результаты;

понимание более глубоко процессы работы информационных систем, что позволит применять полученные знания с целью обеспечения правильных, оперативных способов защиты информации.

формирование и развитие компетенций обучающихся в области использования информационно-коммуникационных технологий, в том числе знаний, умений и навыков работы с информацией, коммуникации в современных цифровых средах в условиях обеспечения информационной безопасности личности обучающегося.

Основные задачи курса «**Технологии информационной безопасности**» — сформировать у обучающихся:

владение основами информационной безопасности;

разбираться в видах и свойствах информации и ее защиты;

понимание принципов устройства и функционирования объектов цифрового окружения, представления об истории и тенденциях развития информатики периода цифровой трансформации современного общества;

умения и навыки формализованного описания поставленных задач;

умения и навыки эффективного использования основных типов прикладных программ (приложений) общего назначения и информационных систем для решения с их помощью практических задач;

умение грамотно интерпретировать результаты решения практических задач с помощью информационных технологий, применять полученные результаты в практической деятельности.

Место курса внеурочной деятельности

«Технологии информационной безопасности» В УЧЕБНОМ ПЛАНЕ

34 учебных часа — по 1 ч в неделю в 10х классах

Срок реализации программы — один год.

Для класса предусмотрено резервное учебное время, которое может быть использовано участниками образовательного процесса в целях формирования вариативной составляющей содержания конкретной рабочей программы. В резервные часы входят часы на повторение и на занятия, посвящённые презентации продуктов практической деятельности.

Планируемые результаты освоения курса «Технологии информационной безопасности»

Личностные результаты

Патриотическое воспитание:

ценностное отношение к отечественному культурному, историческому и научному наследию;

понимание значения информатики как науки в жизни современного общества.

Духовно-нравственное воспитание:

ориентация на моральные ценности и нормы в ситуациях нравственного выбора;

готовность оценивать своё поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм, с учётом осознания последствий поступков;

активное неприятие асоциальных поступков, в том числе в Интернете.

Гражданское воспитание:

представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах;

соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде;

ориентация на совместную деятельность при выполнении учебных и познавательных задач, создании учебных проектов;

стремление оценивать своё поведение и поступки своих товарищей с позиции нравственных и правовых норм, с учётом осознания последствий поступков.

Ценность научного познания:
наличие представлений об информации, информационных процессах и информационных технологиях, соответствующих современному уровню развития науки и общественной практики;

интерес к обучению и познанию;

любознательность;

стремление к самообразованию;

овладение начальными навыками исследовательской деятельности, установка на осмысление опыта, наблюдений, поступков и стремление совершенствовать пути достижения индивидуального и коллективного благополучия;

наличие базовых навыков самостоятельной работы с учебными текстами, справочной литературой, разнообразными средствами информационных технологий, а также умения самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности.

Формирование культуры здоровья:
установка на здоровый образ жизни, в том числе и за счёт освоения и соблюдения требований безопасной эксплуатации средств ИКТ.

Трудовое воспитание:
интерес к практическому изучению профессий в сферах деятельности, связанных с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса.

Экологическое воспитание:
наличие представлений о глобальном характере экологических проблем и путей их решения, в том числе с учётом возможностей ИКТ.

Адаптация обучающегося к изменяющимся условиям социальной среды:
освоение обучающимися социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, в том числе в виртуальном пространстве.

Метапредметные результаты

Универсальные познавательные действия

Базовые логические действия:

умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логические рассуждения, делать умозаключения (индуктивные, дедуктивные и по аналогии) и выводы;

умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

самостоятельно выбирать способ решения учебной задачи(сравнивать несколько вариантов решения, выбирать наиболее подходящий с учётом самостоятельно выделенных критериев).

Базовые исследовательские действия:

формулировать вопросы, фиксирующие разрыв между реальным и желательным состоянием ситуации, объекта, и самостоятельно устанавливать искомое и данное;

оценивать применимость и достоверность информации, полученной в ходе исследования;

прогнозировать возможное дальнейшее развитие процессов,

событий и их последствия в аналогичных или сходных ситуациях, а также выдвигать предположения об их развитии в новых условиях и контекстах.

Работа с информацией:

выявлять дефицит информации, данных, необходимых для решения поставленной задачи;

применять основные методы и инструменты при поиске и отборе информации из источников с учётом предложенной учебной задачи и заданных критериев;

выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;

выбирать оптимальную форму представления информации и иллюстрировать решаемые задачи несложными схемами, диаграммами, иными графическими объектами и их комбинациями;

оценивать достоверность информации по критериям, предложенным учителем или сформулированным самостоятельно;

запоминать и систематизировать информацию.

Универсальные коммуникативные действия

Общение:

сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;

публично представлять результаты выполненного опыта (исследования, проекта);

выбирать формат выступления с учётом задач презентации и особенностей аудитории и в соответствии с ним составлять устные и письменные тексты с использованием иллюстративных материалов.

Совместная деятельность (сотрудничество):

понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, в том числе при создании информационного продукта;

принимать цель совместной информационной деятельности по сбору, обработке, передаче и формализации информации, коллективно строить действия по её достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы;

выполнять свою часть работы с информацией или информационным продуктом, достигая качественного результата по своему направлению и координируя свои действия с другими

членами команды;

оценивать качество своего вклада в общий информационный продукт по критериям, самостоятельно сформулированным участниками взаимодействия;

сравнивать результаты с исходной задачей и вклад каждого члена команды в достижение результатов, разделять сферу ответственности и проявлять готовность к предоставлению отчёта перед группой.

Универсальные регулятивные действия

Самоорганизация:

выявлять в жизненных и учебных ситуациях проблемы, требующие решения;

видеть возможности и опасности влияния информации и информационной безопасности в жизни общества;

составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учётом имеющихся ресурсов и собственных возможностей, аргументировать выбор варианта решения задачи;

составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм

с учётом получения новых знаний об изучаемом объекте.

Самоконтроль (рефлексия):

владеть способами самоконтроля, самомотивации и рефлексии;

учитывать контекст и предвидеть трудности, которые могут

возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;

вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;

оценивать соответствие результата цели и условиям.

Эмоциональный интеллект:

ставить себя на место другого человека, понимать мотивы и намерения другого.

Принятие себя и других:

осознавать невозможность контролировать всё вокруг даже в условиях открытого доступа к любым объёмам информации.

Предметные результаты

10 класс

применять правила безопасности при работе за компьютером;

знать основные методы защиты информации;

знать нормативные акты определяющие понятия и требования информационной безопасности;

уметь классифицировать виды информации и информационной безопасности;

классифицировать угрозы и методы противодействия;

знать принципы обработки данных в информационных системах;

различать виды информации;

дифференцировать информацию по назначению;

Знать виды конфиденциальной информации;

Уметь определять персональные данные;

ознакомиться с 152, 5485-1, 149 Федеральными законами;

познакомиться с Указом Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Указом Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»;

познакомиться с Федеральным законом от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных»;

знать причины появления проблем информационной безопасности;

понимать представление понятия защита информации и меры ее реализации;

знать классификацию средств защиты информации;

знать основные обязанности обладателя информации и оператора информационной системы;

знать неформальными средства защиты информации;

знать формальные средства защиты информации;

уметь классифицировать формальные средства защиты информации;

знать о самых масштабных нарушениях безопасности;

уметь находить в информационных базах информацию о уязвимостях информационных систем;

знать классы уязвимостей систем безопасности;

знать основные возможные уязвимости систем безопасности;

уметь производить расчет степени опасности за счет ранжирования уязвимостей систем безопасности;

знать источники угрозы информационной безопасности;

знать классификацию источников угроз информационной безопасности;

знать основные цели и мотивы злоумышленника;

знать способы осуществления несанкционированного доступа к информации;

понимать степень возможного наносимого ущерба от действий злоумышленника;

знать основные понятия криптографии;

знать криптографические примитивы;

знать модели основных криптографических атак;

понимать основ работы инфраструктуры открытых ключей;

понимать функции и задачи удостоверяющего центра;

знать понятия ключевая пара, открытый, собственный закрытый ключ;

понимать, как определяется подлинность электронной подписи;

уметь работать с личными сертификатами;

знать архитектуры PKI;

понимать, почему существует проблема государственных удостоверяющих центров и таких как корневые хранилища Mozilla и Microsoft;

различать и уметь пользоваться корневыми, промежуточными и личными хранилищами сертификатов;

знать понятие и применение сертификатов отзыва;

уметь создавать учетные записи в операционных системах;

знать, как настраивается учетная политика безопасности в операционной системе;

понимать назначение групп пользователей и их возможности;

уметь назначать и разграничивать доступ к файлам;

понимать, как работает наследие прав;

уметь поменять владельца файла;

уметь разграничить доступ к запуску программного обеспечения пользователям или группам пользователей;

уметь работать с журналом аудита;

знать принципы технологии аутентификации;

иметь представление использования смарт-карт и usb ключей для аутентификации;

знать назначение Rutoken;

уметь производить настройку и установку Rutoken;

уметь шифровать документы и задание пароля для их открытия;

уметь защищать информацию в архивных копиях;

уметь работать с программой вскрытия паролей AZPR;

знать назначение и принципы работы Firewall;

уметь работать с программным сетевым экраном Agnitum Outpost;

иметь представление о работе сканеров сети;

знать и уметь использовать резервное копирование данных средствами операционной системы;

уметь использовать внешнее программное обеспечение для копирования образа системы;

уметь применять шифрование используя шифр Цезаря;

уметь применять шифрование используя шифр Тритемиуса;

уметь применять шифрование используя шифр Вижинера;

уметь применять шифрование используя классические шифры перестановки;

уметь применять шифрование используя перестановки с ключом;

уметь применять шифрование используя метод перестановки по маршрутам;

использование методов и средств противодействия угрозам информационной безопасности,

соблюдение мер безопасности, предотвращающих незаконное распространение персональных данных,

соблюдение требований техники безопасности и гигиены при работе с компьютерами и другими компонентами цифрового окружения,

понимание правовых основ использования компьютерных программ, баз данных и работы в сети Интернет;

Содержание курса «Технологии информационной безопасности»

10 КЛАСС

1. Информация. Информационная безопасность. (раздел Цифровая грамотность)

Правила безопасности при работе за компьютером. Информация и ее классификация. Конфиденциальные данные. Персональные данные. Основные носители информации. Агрегация информации. Актуальность проблемы информационной безопасности. 10 самых громких атак.

2. Средства защиты информации. (раздел Цифровая грамотность)

Нормативные (неформальные). Нормативные(законодательные). Административные(организационные). Морально-этические средства. Технические (формальные). Физические средства защиты информации. Аппаратный средства защиты информации. Программные средства защиты информации. DLP-системы. SIEM-системы. Математические (криптографические).

3. Классификация средств защиты информации. (раздел Цифровая грамотность)

Что обязаны обеспечить обладатели информации. Нормативные (неформальные) средства защиты. Технические (формальные) средства защиты. Внедрение средств криптографической защиты.

4. Угрозы информационной безопасности. (раздел Цифровая грамотность)

Разновидности уязвимостей ИБ. Классификация уязвимостей систем безопасности. Ранжирование уязвимостей. Источники угрозы информационной безопасности. Примеры нарушения защиты информации и доступа к данным

5. Криптография. (раздел Цифровая грамотность)

Криптография как наука. Участники взаимодействия. Объекты и операции. Криптографические примитивы. Алгоритмы шифровании. Криптографические хэш-функции. Криптографические генераторы псевдослучайных чисел. Модели основных криптографических атак. Атака на основе шифртекста. Атака на основе открытого текста. Атака на основе подобранного открытого текста. Атака на основе адаптивного подобранного открытого текста. Анализ стойкости криптографических примитивов

6. Электронно-цифровая подпись. (раздел Цифровая грамотность)

Цифровой сертификат. Электронная подпись. Процессы работы с личными сертификатами. Корневые хранилища сертификатов в браузерах. Основные доверенные центры Интернета. PKI. Объекты PKI. Архитектуры PKI.

7. Некоторые практические методы защиты информации. (раздел Цифровая грамотность)

Аутентификация в операционных системах при помощи физического объекта. Идентификация и аутентификация. Технологии аутентификации. Аутентификация по многоразовым паролям. Протоколы аутентификации для удаленного доступа. Аутентификация по предъявлению цифрового сертификата. Использование смарт-карт и USB-ключей. Rutoken. Архитектура Rutoken. Назначение Rutoken. Практическая часть. Установка и настройка Rutoken. Управление драйверами Rutoken. rtAdmin. exe. Утилита администрирования Rutoken. rtCert. exe. Браузер сертификатов Rutoken. Администрирование учётных записей пользователей в операционной системе Windows. Управление учётными записями локальных пользователей. Настройка политики учётной записи. Групповые политики. Выполнение практической работы «Настройка учетных записей». Дискреционный механизм разграничения доступа к файловым объектам. Основные права доступа к файловым объектам. Элементы разрешений на доступ. «Владелец» файла. Наследование прав доступа. Разграничение доступа к принтерам. Выполнение практической работы «Разграничение доступа к файлам». Разграничение доступа к запуску программного обеспечения. Ограниченное использование программ. Настройки ограничения доступа к программам. Выполнение практической работы «Разграничение доступа к запуску программного обеспечения». Аудит событий безопасности операционной системы. Политика аудита. Аудит входа/выхода пользователей. Аудит событий, связанных с администрированием. Аудит событий, связанных с работой операционной системы. Аудит доступа пользователей к ресурсам. Управление журналом аудита. Выполнение практической работы «Аудит событий безопасности». «Защита документов MS Office». Шифрование документа и задание пароля для его открытия. Создание надёжных паролей. Выполнение практической работы «Защита документов MS Office». «Работа с программой вскрытия паролей AZPR». Проблема: забытые пароли. Методы восстановления пароля. Установка пароля на архивы ZIP и RAR. Работа с программами взлома на примере AZPR. Выполнение практической работы «Работа с программой вскрытия паролей». Настройка межсетевого экрана. Теоретические сведения. Архитектура firewall. Использование Outpost. Выполнение практической работы «Настройка межсетевого экрана». Резервное копирование программ, системных параметров и файлов. Панели управления Архивация и восстановление. Настройка параметров регулярного резервного копирования. Создание образа системы.

Рекомендации по резервному копированию. Выполнение практической работы «Резервное копирование». Использование методов замены для шифрования данных. Примеры классических шифров замены. Шифр Цезаря. Шифр Тритемиуса. Шифр Вижинера. Выполнение практической работы «Шифрование. Методы замены». Использование методов перестановки для шифрования данных. Классические шифры перестановки. Перестановки с ключом. Шифрование методом перестановки по маршрутам. Выполнение практической работы «Шифрование. Методы перестановки».

Тематическое планирование курса «Технологии информационной безопасности»

10 класс, 1ч. в неделю, всего 34 ч.

Темы, раскрывающие данный раздел программы, и число часов на их изучение	Содержание программы	Основные виды деятельности обучающегося при изучении темы
Информация. Информационная безопасность(4ч.)		
Цифровая грамотность	Правила безопасности при работе за компьютером. Информация и ее классификация. Конфиденциальные данные. Персональные данные. Основные носители информации. Агрегация информации. Актуальность проблемы информационной безопасности. 10 самых громких атак.	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.
Средства защиты информации(2ч.)		
Цифровая грамотность	Нормативные (неформальные). Нормативные(законодательные). Административные(организационные). Морально-этические средства. Технические (формальные). Физические средства защиты информации. Аппаратный средства защиты информации. Программные средства защиты информации. DLP-системы. SIEM-системы. Математические (криптографические).	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.

Классификация средств защиты информации. (2ч.)		
Цифровая грамотность	Что обязаны обеспечить обладатели информации. Нормативные (неформальные) средства защиты. Технические (формальные) средства защиты. Внедрение средств криптографической защиты.	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.
Угрозы информационной безопасности. (2ч.)		
Цифровая грамотность	Разновидности уязвимостей ИБ. Классификация уязвимостей систем безопасности. Ранжирование уязвимостей. Источники угрозы информационной безопасности. Примеры нарушения защиты информации и доступа к данным	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.
Криптография.		
Цифровая грамотность	Криптография как наука. Участники взаимодействия. Объекты и операции. Криптографические примитивы. Алгоритмы шифровании. Криптографические хэш-функции. Криптографические генераторы псевдослучайных чисел. Модели основных криптографических атак. Атака на основе шифртекста. Атака на основе открытого текста. Атака на основе подобранного открытого текста. Атака на основе адаптивного подобранного открытого текста. Анализ стойкости криптографических примитивов	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.

Электронно-цифровая подпись. (2ч.)		
Цифровая грамотность	Цифровой сертификат. Электронная подпись. Процессы работы с личными сертификатами. Корневые хранилища сертификатов в браузерах. Основные доверенные центры Интернета. PKI. Объекты PKI. Архитектуры PKI.	Характеризовать сущность понятий «информационная безопасность», «защита информации». Формулировать основные правила информационной безопасности. Анализировать законодательную базу, касающуюся информационной безопасности.
Некоторые практические методы защиты информации. (21ч.)		
Цифровая грамотность	Аутентификация в операционных системах при помощи физического объекта. Идентификация и аутентификация. Технологии аутентификации. Аутентификация по многоразовым паролям. Протоколы аутентификации для удаленного доступа. Аутентификация по предъявлению цифрового сертификата. Использование смарт-карт и USB-ключей. Rutoken. Архитектура Rutoken. Назначение Rutoken. Практическая часть. Установка и настройка Rutoken. Управление драйверами Rutoken. rtAdmin. exe. Утилита администрирования Rutoken. rtCert. exe. Браузер сертификатов Rutoken. Администрирование учётных записей пользователей в операционной системе Windows. Управление учётными записями локальных пользователей. Настройка политики учётной записи. Групповые политики. Выполнение практической работы «Настройка учетных записей». Дискреционный механизм разграничения доступа к файловым объектам. Основные права доступа к файловым объектам. Элементы разрешений на доступ. «Владелец» файла. Наследование прав доступа.	Применять средства защиты информации: брандмауэры, антивирусные программы, паролирование и архивирование, шифрование. Предотвращать несанкционированный доступ к личной конфиденциальной информации, хранящейся на персональном компьютере, мобильных устройствах. Практические работы: Настройка учетных записей». «Разграничение доступа к файлам «Разграничение доступа к запуску программного обеспечения». «Аудит событий безопасности». «Защита документов MS Office». «Защита

	Разграничение доступа к принтерам. Выполнение практической работы «Разграничение доступа к файлам». Разграничение доступа к запуску программного обеспечения. Ограниченное использование программ. Настройки ограничения доступа к программам. Выполнение практической работы «Разграничение доступа к запуску программного обеспечения». Аудит событий безопасности операционной системы. Политика аудита. Аудит входа/выхода пользователей. Аудит событий, связанных с администрированием. Аудит событий, связанных с работой операционной системы. Аудит доступа пользователей к ресурсам. Управление журналом аудита. Выполнение практической работы «Аудит событий безопасности». «Защита документов MS Office». Шифрование документа и задание пароля для его открытия. Создание надёжных паролей. Выполнение практической работы «Защита документов MS Office». «Работа с программой вскрытия паролей AZPR». Проблема: забытые пароли. Методы восстановления пароля. Установка пароля на архивы ZIP и RAR. Работа с программами взлома на примере AZPR. Выполнение практической работы «Работа с программой вскрытия паролей». Настройка межсетевого экрана. Теоретические сведения. Архитектура firewall. Использование Outpost. Выполнение практической работы «Настройка межсетевого экрана». Резервное копирование программ, системных параметров и файлов. Панели управления Архивация и восстановление. Настройка параметров регулярного резервного копирования. Создание образа системы. Рекомендации по резервному копированию. Выполнение практической работы «Резервное копирование». Использование методов замены для шифрования данных. Примеры классических шифров замены. Шифр Цезаря. Шифр	документов MS Office». «Работа с программой вскрытия паролей AZPR». «Работа с программой вскрытия паролей». «Настройка межсетевого экрана». «Резервное копирование». «Шифрование. Методы замены». «Шифрование. Методы перестановки».

	Тритемиуса. Шифр Вижинера. Выполнение практической работы «Шифрование. Методы замены». Использование методов перестановки для шифрования данных. Классические шифры перестановки. Перестановки с ключом. Шифрование методом перестановки по маршрутам. Выполнение практической работы «Шифрование. Методы перестановки».	

Форма проведения занятий

Обучение предусматривает групповую форму занятий в классе с учителем. Тематическое планирование состоит из семи модулей, где седьмой модуль включает практические методы защиты информации. Проводится 1 академический час в неделю. Итого 34 часа.

Занятия предусматривают индивидуальную и групповую работу школьников, а также предоставляют им возможность проявить и развить самостоятельность. В курсе наиболее распространены следующие формы работы: обсуждения, дискуссии, работа с ЭВМ, решения кейсов, эксперименты, выполнение интерактивных заданий на образовательной платформе.

Учебно-методическое обеспечение образовательного процесса

• Информатика (в 2 частях), 10 класс/ Поляков К.Ю., Еремин Е.А., Общество с ограниченной ответственностью «БИНОМ. Лаборатория знаний»; Акционерное общество «Издательство «Просвещение», Помодульные дидактические материалы, представленные на образовательной платформе (в том числе раздаточный материал и т. д.).

Методические материалы для ученика

Помодульные дидактические материалы, представленные на

образовательной платформе (в том числе раздаточный материал и т. д.).

Методические материалы для учителя

Методические материалы.

Демонстрационные материалы по теме занятия.

Методическое видео с подробным разбором материалов, рекомендуемых для использования на занятии.

Цифровые образовательные ресурсы и ресурсы интернета

Образовательная платформа.

Учебное оборудование

Компьютер (стационарный компьютер, ноутбук, планшет).

Компьютерные мыши.

Клавиатуры.

Учебное оборудование для проведения лабораторных работ, практических работ и демонстраций

Мультимедийный проектор с экраном (интерактивной доской) или интерактивная панель.

Компьютер (стационарный компьютер, ноутбук, планшет).

Компьютерные мыши.

Клавиатуры.