**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Министерство образования Свердловской области**

**Департамент образования Администрации г. Екатеринбурга**

**МАОУ СОШ № 147**

| РАССМОТРЕНА | СОГЛАСОВАНА | УТВЕРЖДЕНА |
|---|---|---|
| на заседании ШМО | Заместитель директора по УД | Директор МАОУ СОШ № 147 |
| Яковлева И.А. | Белобородова Л.А. | Моисеев А.А. |
| Протокол № 1 от «27» августа 2025 г. | Протокол № 1 от «27» августа 2025 г. | Приказ № 76-о от «28» августа 2025 г. |

# РАБОЧАЯ ПРОГРАММА

## учебного предмета «Информационная безопасность»

для обучающихся 5-7 классов

**Екатеринбург 2025**

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа учебного курса «Информационная безопасность» разработана для организаций, реализующих программы общего образования. В ней учтены приоритеты научно-технологического развития Российской Федерации (Пр-294, п. 2а-16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации.

## Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных

социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах.

Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к

информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых. В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей культуры информационной безопасности при работе в сети Интернет вне школы с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по

возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная **цель** курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого

времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

# ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

**Личностные результаты:**

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

**Метапредметные результаты** - освоенные обучающимися на базе одного, нескольких или всех учебных предметов способы деятельности, применимые как в рамках образовательного процесса, так и в других жизненных ситуациях.

Основными метапредметными результатами, формируемыми при изучении информатики в основной школе, являются:

- владение общепредметными понятиями;
- включаться в диалог, в коллективное обсуждение, проявлять инициативу и активность; обращаться за помощью;
- формулировать свои затруднения; предлагать помощь и сотрудничество;
- договариваться и приходить к общему решению в совместной деятельности, в том числе в ситуации столкновения интересов; слушать собеседника;
- формулировать собственное мнение и позицию;
- адекватно оценивать собственное поведение и поведение окружающих.
- наличие представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества;
- понимание роли информационных процессов в современном мире;
- владение первичными навыками анализа и критичной оценки получаемой информации;
- ответственное отношение к информации с учетом правовых и этических аспектов ее распространения;
- развитие чувства личной ответственности за качество окружающей информационной среды;

- способность увязать учебное содержание с собственным жизненным опытом, понять значимость подготовки в области информатики и ИКТ в условиях развития информационного общества;
- готовность к повышению своего образовательного уровня и продолжению обучения с использованием средств и методов информатики и ИКТ;
- способность и готовность к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественнополезной, учебно-исследовательской, творческой деятельности;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, эргономических и технических условий безопасной эксплуатации средств ИКТ.

**Предметные результаты:**

- научатся 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;
- получат возможность овладеть приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов;
- основами самоконтроля, соблюдения норм информационной этики и права;

- навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети Интернет

# СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

## 5 класс

Информационное общество.

История создания сети Интернет. Что такое Всемирная паутина?

Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета. Сайты, электронные сервисы.

Угрозы в сети Интернет.

Защита личных данных в сети Интернет.

Сетевой этикет.

Коллекции сайтов для детей. Электронные музеи.

Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях.

Что такое информационная безопасность.

Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.

Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.

Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями

## 6 класс

Общение в социальных сетях и мессенджерах.

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

С кем безопасно общаться в интернете.

Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Пароли для аккаунтов социальных сетей

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

Безопасный вход в аккаунты

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

Настройки конфиденциальности в социальных сетях

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфидициальность в месседжерах.

Публикация информации в социальных сетях

Персональные данные. Публикация личной информации.

Кибербуллинг

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

Публичные аккаунты

Настройки приватности публичных страниц. Правила ведения публичных страницы

Фишинг

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

## 7 класс

Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

Методы защиты от вредоносных программ

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

Распространение вредоносного кода для мобильных устройств

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

# ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

# 5 КЛАСС

| № п/п | Наименование разделов и тем программы | Количество часов | | | Электронные (цифровые) образовательные ресурсы |
|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | |
| 1 | Информационное общество | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 2 | Интернет как глобальная компьютерная сеть. Сайты, электронные сервисы. Коллекции сайтов для учебной и познавательной деятельности | 4 | | 1 | https://lib.myschool.edu.ru/ |
| 3 | Угрозы в сети Интернет. Защита личных данных в сети Интернет | 6 | | 3 | https://lib.myschool.edu.ru/ |
| 4 | Сетевой этикет. Коллекции сайтов для детей. Электронные музеи | 2 | | 1 | https://lib.myschool.edu.ru/ |
| 5 | Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 6 | Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения | 3 | | 2 | https://lib.myschool.edu.ru/ |
| 7 | Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи | 6 | | 3 | https://lib.myschool.edu.ru/ |
| 8 | Использование полезных ресурсов в сети. Интернет, работа в сети. Интернет для людей с особыми потребностями | 3 | | 2 | https://lib.myschool.edu.ru/ |
| | Резерв | 4 | | | https://lib.myschool.edu.ru/ |
| | Всего: | 34 | 0 | 14 | |

# 6 КЛАСС

| № п/п | Наименование разделов и тем программы | Количество часов | | | Электронные (цифровые) образовательные ресурсы |
|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | |
| 1 | Общение в социальных сетях и мессенджерах | 5 | | 1 | https://lib.myschool.edu.ru/ |
| 2 | С кем безопасно общаться в интернете | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 3 | Пароли для аккаунтов социальных сетей | 4 | | 1 | https://lib.myschool.edu.ru/ |
| 4 | Безопасный вход в аккаунты | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 5 | Настройка конфиденциальности в социальных сетях | 3 | | 2 | https://lib.myschool.edu.ru/ |
| 6 | Публикация информации в социальных сетях | 2 | | 2 | https://lib.myschool.edu.ru/ |
| 7 | Кибербуллинг | 4 | | 2 | https://lib.myschool.edu.ru/ |
| 8 | Публичные аккаунты | 2 | | 2 | https://lib.myschool.edu.ru/ |
| 9 | Фишинг | 4 | | 0 | https://lib.myschool.edu.ru/ |
| | Резерв | 4 | | | https://lib.myschool.edu.ru/ |
| | Всего: | 34 | | 12 | |

# 7 КЛАСС

| № п/п | Наименование разделов и тем программы | Количество часов | | | Электронные (цифровые) образовательные ресурсы |
|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | |
| 1 | Общение в социальных сетях и мессенджерах | 5 | | 1 | https://lib.myschool.edu.ru/ |
| 2 | С кем безопасно общаться в интернете | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 3 | Пароли для аккаунтов социальных сетей | 4 | | 2 | https://lib.myschool.edu.ru/ |
| 4 | Безопасный вход в аккаунты | 3 | | 1 | https://lib.myschool.edu.ru/ |
| 5 | Настройка конфиденциальности в социальных сетях | 3 | | 2 | https://lib.myschool.edu.ru/ |
| 6 | Публикация информации в социальных сетях | 2 | | 1 | https://lib.myschool.edu.ru/ |
| 7 | Кибербуллинг | 4 | | 1 | https://lib.myschool.edu.ru/ |
| 8 | Публичные аккаунты | 2 | | 1 | https://lib.myschool.edu.ru/ |
| 9 | Фишинг | 4 | | 1 | https://lib.myschool.edu.ru/ |
| | Резерв | 4 | | | https://lib.myschool.edu.ru/ |
| | Всего: | 34 | | 11 | |

# ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

# 5 КЛАСС

| № п/п | Тема урока | Количество часов | | | Дата изучения | Электронные цифровые образовательные ресурсы |
|---|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | | |
| 1 | Введение. Что такое информационное общество? | 1 | | | | https://lib.myschool.edu.ru/ |
| 2 | История создания сети Интернет | 1 | | | | https://lib.myschool.edu.ru/ |
| 3 | Что такое Всемирная паутина? | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 4 | Путешествие по сети Интернет: сайты и электронные сервисы | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 5 | Как стать пользователем Интернета? | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 6 | Опасности для пользователей Интернета | 1 | | | | https://lib.myschool.edu.ru/ |
| 7 | Что такое кибератака? | 1 | | | | https://lib.myschool.edu.ru/ |
| 8 | Что такое информационная безопасность? | 1 | | | | https://lib.myschool.edu.ru/ |
| 9 | Законы о защите личных данных в Интернете | 1 | | | | https://lib.myschool.edu.ru/ |
| 10 | Коллекции сайтов для детей | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 11 | Электронные музеи | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 12 | Контрольный урок | 1 | 1 | | | https://lib.myschool.edu.ru/ |
| 13 | Правила работы с СМС | 1 | | | | https://lib.myschool.edu.ru/ |
| 14 | Правила работы с электронной почтой | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 15 | Правила работы с видеосервисами | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 16 | Правила работы в социальных сетях | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 17 | Правила защиты от вирусов, спама, рекламы и рассылок | 1 | | | | https://lib.myschool.edu.ru/ |
| 18 | Практическое занятие | | | 1 | | https://lib.myschool.edu.ru/ |
| 19 | Правила защиты от негативных сообщений | 1 | | | | https://lib.myschool.edu.ru/ |

| | | | | | | |
|---|---|---|---|---|---|---|
| 20 | Правила общения в социальной сети | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 21 | Правила работы с поисковыми системами и анализ информации | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 22 | Практическое занятие | | | 1 | | https://lib.myschool.edu.ru/ |
| 23 | Правила ответственности за распространение ложной и негативной информации | 1 | | | | https://lib.myschool.edu.ru/ |
| 24 | Правила защиты от нежелательных сообщений и контактов | 1 | | | | https://lib.myschool.edu.ru/ |
| 25 | Практическое занятие | | | 1 | | https://lib.myschool.edu.ru/ |
| 26 | Правила вызова экстренной помощи | 1 | | | | https://lib.myschool.edu.ru/ |
| 27 | Правила защиты устройств от внешнего вторжения | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 28 | Правила выбора полезных ресурсов в Интернете | 1 | | | | https://lib.myschool.edu.ru/ |
| 29 | Средства работы в Интернете для людей с особыми потребностями | 1 | | | | https://lib.myschool.edu.ru/ |
| 30 | Контрольный урок | 1 | 1 | | | https://lib.myschool.edu.ru/ |
| 31-34 | Резерв | 4 | | | | https://lib.myschool.edu.ru/ |
| | **Всего:** | 34 | 2 | 14 | | |

# 6 КЛАСС

| № п/п | Тема урока | Количество часов | | | Дата изучения | Электронные цифровые образовательные ресурсы |
|---|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | | |
| 1 | Что такое «социальная сеть»? | 1 | | | | https://lib.myschool.edu.ru/ |
| 2 | История социальных сетей и мессенджеров | 1 | | | | https://lib.myschool.edu.ru/ |
| 3 | Назначение социальных сетей и мессенджеров | 1 | | | | https://lib.myschool.edu.ru/ |
| 4 | Продвижение и реклама в социальных сетях | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 5 | Почему социальные сети стали настолько популярными? | 1 | | | | https://lib.myschool.edu.ru/ |
| 6 | Анонимность в социальных сетях | 1 | | | | https://lib.myschool.edu.ru/ |
| 7 | Профиль пользователя в социальной сети | 1 | | | | https://lib.myschool.edu.ru/ |
| 8 | Правила добавления друзей в социальных сетях | 1 | | | | https://lib.myschool.edu.ru/ |
| 9 | Как правильно создавать пароли для безопасного использования в Интернете? | 1 | | | | https://lib.myschool.edu.ru/ |
| 10 | Какой пароль считается хорошим и безопасным? | 1 | | | | https://lib.myschool.edu.ru/ |
| 11 | Основные правила по безопасному использованию паролей | 1 | | | | https://lib.myschool.edu.ru/ |
| 12 | Как запомнить все пароли или где их хранить? | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 13 | Виды аутентификации | 1 | | | | https://lib.myschool.edu.ru/ |
| 14 | Настройка безопасности аккаунта | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 15 | Работа на чужом компьютере с точки зрения безопасности личного аккаунта | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 16 | Безопасность в социальных сетях и мессенджерах – приватность и конфиденциальность информации | 1 | | | | https://lib.myschool.edu.ru/ |
| 17 | Ограничение доступа к выложенной информации в социальных сетях | 1 | | 1 | | https://lib.myschool.edu.ru/ |

| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | Настройка приватности и конфиденциальности в разных социальных сетях | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 19 | Основные требования к выкладываемой информации в социальных сетях | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 20 | Ответственность за публикацию, распространение и репост информации | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 21 | Что такое «кибербуллинг»? | 1 | | | | https://lib.myschool.edu.ru/ |
| 22 | Возможные причины кибербуллинга | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 23 | Как не стать жертвой кибербуллинга? | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 24 | Методы борьбы с кибербуллингом | 1 | | | | https://lib.myschool.edu.ru/ |
| 25 | Настройка приватности публичных страниц | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 26 | Правила ведения публичных страниц | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 27 | Фишинг как мошеннический прием | 1 | | | | https://lib.myschool.edu.ru/ |
| 28 | Варианты распространения фишинга | 1 | | | | https://lib.myschool.edu.ru/ |
| 29 | Отличие настоящих и фишинговых сайтов | 1 | | | | https://lib.myschool.edu.ru/ |
| 30 | Как защититься от фишеров в социальных сетях и мессенджерах? | 1 | | | | https://lib.myschool.edu.ru/ |
| 31-34 | Резерв | 4 | | | | |
| | Всего: | 34 | | 12 | | |

# 7 КЛАСС

| № п/п | Тема урока | Количество часов | | | Дата изучения | Электронные цифровые образовательные ресурсы |
|---|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | | |
| 1 | Понятие «вредоносный код» | 1 | | | | https://lib.myschool.edu.ru/ |
| 2 | Виды вредоносных кодов | 1 | | | | https://lib.myschool.edu.ru/ |
| 3 | Возможности и функции вредоносных кодов | 1 | | | | https://lib.myschool.edu.ru/ |
| 4 | Чем опасен вредоносный код? | 1 | | | | https://lib.myschool.edu.ru/ |
| 5 | Как защититься от вредоносного кода? | 1 | | | | https://lib.myschool.edu.ru/ |
| 6 | Отличие вредоносного кода от ошибочного кода | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 7 | Отличие вредоносного кода от вредоносного программного обеспечения | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 8 | Вредоносное программное обеспечение, вошедшее в историю | 1 | | | | https://lib.myschool.edu.ru/ |
| 9 | Цель внедрения вредоносного кода | 1 | | | | https://lib.myschool.edu.ru/ |
| 10 | Схемы внедрения вредоносного кода | 1 | | | | https://lib.myschool.edu.ru/ |
| 11 | Способы доставки вредоносного кода | 1 | | | | https://lib.myschool.edu.ru/ |
| 12 | Исполняемые файлы и расширения вредоносного кода | 1 | | | | https://lib.myschool.edu.ru/ |
| 13 | Вредоносная рассылка | 1 | | | | https://lib.myschool.edu.ru/ |
| 14 | Вредоносные скрипты | 1 | | | | https://lib.myschool.edu.ru/ |
| 15 - 16 | Как искать вредоносный код без антивирусов и сканеров? | 2 | | 1 | | https://lib.myschool.edu.ru/ |

| | | | | | | |
|---|---|---|---|---|---|---|
| 17 | Способы выявления наличия вредоносного кода на устройствах | 1 | | | | https://lib.myschool.edu.ru/ |
| 18 | Действия при обнаружении вредоносного кода на устройствах | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 19 | Как не разместить вредоносный код случайно? | 1 | | | | https://lib.myschool.edu.ru/ |
| 20 | Что такое «комплексная защита» устройства? | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 21 | Профилактические меры для предупреждения появления вредоносного кода | 1 | | | | https://lib.myschool.edu.ru/ |
| 22 | Способы защиты устройств от вредоносного кода | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 23 | Правила защиты от вредоносных кодов | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 24 | Антивирусные программы и их характеристики | 1 | | | | https://lib.myschool.edu.ru/ |
| 25 | Правила для выбора антивирусного продукта | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 26 | Преимущества и недостатки антивирусных программ | 1 | | | | https://lib.myschool.edu.ru/ |
| 27 | Типы вредоносного мобильного программного обеспечения | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 28 | Расширение вредоносных кодов для мобильных устройств | 1 | | | | https://lib.myschool.edu.ru/ |
| 29 | Меры по защите мобильных устройств от вредоносного кода | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 30 | Правила безопасности при установке приложений на мобильные устройства | 1 | | 1 | | https://lib.myschool.edu.ru/ |
| 31-34 | Резерв | 1 | | | | https://lib.myschool.edu.ru/ |
| | Всего: | 34 | | 11 | | |

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 647030360437668574821219143876024766403350371137

Владелец Моисеев Александр Анатольевич

Действителен С 27.01.2026 по 27.01.2027