**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**‌****Министерство образования Ярославской области‌‌**

**‌****Управление образования Администрации г. Переславля-Залесского ‌**​

**МОУ Дмитриевская ОШ**

****

**Рабочая программа внеурочной деятельности**

**социальной направленности**

 **9 класс**

**«Информационная безопасность»**

с.Дмитриевское,2023

**ХАРАКТЕРИСТИКА ПРОГРАММЫ**Дополнительная общеобразовательная общеразвивающая программа – «Защита информации»
*Направленность программы* – техническая
*Возраст обучающихся* –9 класс
*Срок обучения* – 17 часов
Форма обучения – очная, применением дистанционных образовательных технологий
**Программа создана на основании**1. Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ».
2. Распоряжение Правительства РФ от 04.09.2014 N 1726-р «Об утверждении Концепции развития дополнительного
образования детей».
3. Постановление Главного государственного санитарного врача РФ от 04.07.2014 № 41 «Об утверждении СанПиН
2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы
образовательных организаций дополнительного образования детей».
4. Приказ Министерства просвещения РФ от 9 ноября 2018 г. N 196 «Об утверждении Порядка организации и
осуществления образовательной деятельности по дополнительным общеобразовательным программам».
5. Письмо Минобрнауки России от 18.11.2015 № 09-3242 «О направлении информации» (вместе с «Методическими
рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые
программы)».
**Пояснительная записка
Актуальность проблемы обеспечения безопасности информации.**Проблемы защиты информации от постороннего доступа и нежелательного воздействия на нее возникло с той поры,
когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком.
Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам
получить какой-либо выигрыш.
С переходом на использование технических средств связи, информация подвергается воздействию случайных
процессов (неисправностям и сбоям оборудования, ошибкам операторов и т.д.), которые могут привести к ее
разрушению, изменению на ложную, а также создать предпосылки к доступу к ней посторонних лиц. С появлением
сложных автоматизированных систем управления, связанных с автоматизированным вводом, хранением, обработкой
и выводом информации, проблемы ее защиты приобретают еще большее значение.
**Этому способствует:**1. Увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств
вычислительной техники.
2. Сосредоточение в единых базах данных информации различного назначения и принадлежности.
3. Расширение круга пользователей, имеющих доступ к ресурсам вычислительной системы, и находящимся в ней
массивам данных.
4. Усложнение режима функционирования технических средств, вычислительной системы (широкое внедрение
многопрограммного режима разделения времени и реального времени).
5. Автоматизация межмашинного обмена информацией, в т.ч. и на больших расстояниях.
6. Увеличение количества технических средств и связей в автоматизированных системах управления (АСУ) и обработки
данных.
7. Появление ПЭВМ, расширяющих возможности не только пользователя, но и нарушителя.
8. Индустрия переработки информации достигла глобального уровня.
9. Появление электронных денег. Создало предпосылки для хищения крупных сумм.
10.Появилось удивительное порождение научно-технических работников. **Хакеры** - прекрасные знатоки
информационной техники. Кракеры. Фракеры - приверженцы электронного журнала Phrack.
11.В последнее время широкое распространение получило новое компьютерное преступление - создание компьютерных
вирусов.
Образовательная программа технической направленности, ориентированная на развитие творческого и
креативного мышления, способного принимать решения связанные с безопасностью и защитой данных. Способность
решать проблемы, связанные с защитой информации.
Активизация познавательного процесса позволяет учащимся более полно и на практике развивать исследовательские,
прикладные способности обучающихся в области защиты информации.
**Формы и режим обучения**Основная методическая установка — деятельностный характер обучения, ориентация учебного процесса на развитие
самостоятельности и ответственности обучающихся за результаты своей деятельности.
Программа реализуется в очном и дистанционном формате, обучение подразумевает использование такого режима,
при котором обучающиеся осваивают курс дистанционно на онлайн ресурсах.
Рекомендуемый режим занятий — 2 часа в неделю.
Основная форма занятий — чередование деятельности обучающегося: работа над проектами, практические занятия с
использованием дополнительных материалов, онлайн порталах.
**Адресат программы**Программа предназначена для обучающихся в возрасте 9 класс).
Для качественного обучения необходимо, чтобы обучающиеся обладали
элементарными навыками работы с файлами в операционной системе, навыками работы в Интернете. Также
необходимы готовность к индивидуальному обучению, умение учиться независимо от других, планировать и
организовывать свою деятельность.
**Объём и срок освоения программы**Программа рассчитана на 17 часов (1 раз в 2 недели).
**Цель и задачи программы**Основной **целью программы** является формирование и раскрытие творческой индивидуальности обучающихся через
расширение опыта творческой активности в разных сферах жизнедеятельности.
Следствием достижения этой цели видится адаптация обучающихся к изменяющимся условиям техническим
новинкам программному обеспечению
**Задачи программы
*Обучающие:***• усовершенствовать навыки владения техникой и технологиями и программными средствами, позволяющими
осуществлять защиту данных.
***Развивающие:***• включить обучающихся в разнообразные виды деятельности;
• создать условия для формирования осознанного интереса к данному направлению деятельности;
• создать условия для повышения активности обучающихся в познавательной и исследовательской деятельности.
***Воспитательные:***• развить инициативность и самостоятельность.

**Содержание программы**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование разделов и тем** | **Дата** |
| **1.**  | **Актуальность проблемы обеспечения безопасности информации**Введение. Угрозы информационной безопасности: классификация, источникивозникновения и пути реализации. Определение требований к уровнюобеспечения информационной безопасности |  |
| **2.**  | **Видео лекция Компании, которые следят за нами**https://www.youtube.com/watch?v=WW1SFdivho8 |  |
| **3.**  | **Виды мер обеспечения информационной безопасности**Виды мер обеспечения информационной безопасности: законодательные,морально-этические, организационные, технические, программноматематические.Специфические приемы управления техническими средствами. Методызащиты от копирования. Не копируемые метки. |  |
| **4.**  | **Видео лекция Цифровая эпидемия. Кибербезопасность | Основной элемент** https://www.youtube.com/watch?v=yR8nEvzcPxcЗащита информации от копирования: Создание защищенных документов иархивов |  |

|  |  |
| --- | --- |
| **5.**  | **Биометрия на защите персональных данныхВидео лекция О блокчейне и биометрии**https://www.youtube.com/watch?time\_continue=140&v=jqym2KUri5o**Видео лекция Как и на кого работает биометрия**https://www.youtube.com/watch?time\_continue=10&v=ktZamo4iS\_M |
| **6.**  | **Безопасность в интернете (яндекс академия)Защита от вредоносных программ** |
| **7.**  | **1. Безопасный аккаунт** |
| **8.**  | **2. Безопасные онлайн платежи3.** https://stepik.org/course/191/promo#toc |
| **9.**  | **4. Антивирусные программы**Рейтинг антивирусов на 2019 год. |
| **10.**  | **Работа с ресурсом Нод 32 для пользователей**Изучение материалов получение сертификатовhttps://academy.esetnod32.ru/home/ |
| **11.**  | **Работа с ресурсом Доктор веб для пользователей**Изучение материалов получение сертификатовhttps://free.drweb.ru/cureit/ |
| **12.**  | **Работа с браузерами**Настройка браузера. |
| **13.**  | Антивирусная защита |
| **14.**  | **Работа с файлообменниками**Файлообменник. |
| **15.**  | **Антивирусные сканеры** |
| **16.**  | **Проверок флешек на вирусы** |
| **17.**  | **Защита портфолио и работ** |
| **всего** |  |

**Актуальность проблемы обеспечения безопасности информации***Содержание темы*
Введение. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации.
Определение требований к уровню обеспечения информационной безопасности
**Видео лекция Компании, которые следят за нами**https://www.youtube.com/watch?v=WW1SFdivho8
**Виды мер обеспечения информационной безопасности***Содержание темы*Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные,
технические, программно-математические.
Специфические приемы управления техническими средствами. Методы защиты от копирования. Не копируемые
метки.
**Видео лекция Цифровая эпидемия. Кибербезопасность Основной элемент**https://www.youtube.com/watch?v=yR8nEvzcPxc
Защита информации от копирования: Создание защищенных документов и архиво
**Биометрия на защите персональных данных***Содержание темы***Видео лекция О блокчейне и биометрии**https://www.youtube.com/watch?time\_continue=140&v=jqym2KUri5o
**Видео лекция Как и на кого работает биометрия**https://www.youtube.com/watch?time\_continue=10&v=ktZamo4iS\_M
**Безопасность в интернете (яндекс академия)***Содержание темы***1. Что такое вредоносная программа**Типы вредоносных программ. Как защитить свой компьютер**.** Безопасный браузер**.** Правила безопасного поведения
**2. Безопасный аккаунт**Что такое аккаунт. Как взламывают аккаунты. Как защитить аккаунт.Что делать, если вас взломали
**3. Безопасные онлайн платежи**Вступительное видео. Выманивание смс. Выманивание денег
«Официальные» письма. Спам с выгодными предложениями. Поддельные магазины
Выманивание телефонного номера. Работа, которой нет. Обман под видом благотворительности. Что нужно знать о
банковской карте. Безопасные покупки с онлайн-кошельком. Если со счётом проблемы
https://stepik.org/course/191/promo#toc
**Получение сертификата
Тема 5. Антивирусные программы**Рейтинг антивирусов на 2019 год.
**Тема 6. Работа с ресурсом Нод 32 для пользователей**Изучение материалов получение сертификатов
https://academy.esetnod32.ru/home/
**Работа с ресурсом Доктор веб для пользователей**Изучение материалов получение сертификатов
https://free.drweb.ru/cureit/
**Работа с браузерами**Настройка браузера. Антивирусная защита
**Работа с файлообменниками**Файлообменник.
**Антивирусные сканеры**Проверок флешек на вирусы
**Защита портфолио и работ
Планируемые результаты
Умения:**−применять организационные, технические и программные средства защиты информации
**Знания:**−источников возникновения информационных угроз
−моделей и принципов защиты информации от несанкционированного доступа
−методов антивирусной защиты информации
−состава и методов организационно-правовой защиты информации
**Материально-техническое обеспечение**−Кабинет для занятий должен быть оснащён компьютерами с выходом в Интернет, интерактивной доской или
проектором.
−Для выполнения некоторых заданий могут потребоваться флеш носители.
−Ссылки на необходимое программное обеспечение и материалы, необходимые на занятиях, размещены в
навигаторах и онлайн-курсах.
−Список другого оборудования, необходимого для проведения занятий, прописывается непосредственно в
навигаторе проведения занятий по соответствующей теме.
**Учебно-методическое обеспечение**Комплект дидактических материалов для организации занятий по курсу
Находиться на следующих порталах
https://stepik.org/course/191/promo#toc
https://academy.esetnod32.ru/home/
https://free.drweb.ru/cureit/
**Список литературы
*Основные источники:***1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. //Российская
газета. 1993. 25 декабря.
2. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите
информации" (с изменениями и дополнениями).
3. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне"(с изменениями и дополнениями).
***Основная литература:***
1. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. 6-е
издание.- М.: Академия, 2012.
2. Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. - СПб.: Изд-во
Политехн. ун-та, 2009. - 126 с.
3. Цирлов Валентин, Основы информационной безопасности. Краткий курс. – М.: Феникс, 2008 . - 256 с.
***Интернет – ресурсы:***1. http://nsecurity.ru/sitemap.html
2. http://ab-solut.net/ru/articles/problemi\_zashiti/
3. http://nsecurity.ru/metody-zashity-informacii.html