МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ГОУ ДПО «Донецкий республиканский институт

дополнительного педагогического образования»

программа

курса по выбору

*«ОСНОВЫ компьютерной безопасности»*

*Для образовательных организаций, осуществляющих образовательную деятельность на освобожденных территориях Донецкой Народной Республики*

*Рекомендовано*

*научно-методическим советом
ГОУ ДПО «Донецкий РИДПО»*

*(протокол № 5 от 22.03.2022 г.)*

Донецк

2022

СОДЕРЖАНИЕ

[**ВВЕДЕНИЕ 4**](#_Toc98862042)

[**I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4**](#_Toc98862043)

[**II. КРИТЕРИИ ОЦЕНИВАНИЯ УРОВНЯ УЧЕБНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ 5**](#_Toc98862044)

[**III. РАСПРЕДЕЛЕНИЕ ЧАСОВ НА ИЗУЧЕНИЕ РАЗДЕЛОВ ПРОГРАММЫ 7**](#_Toc98862045)

[**IV. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА И ТРЕБОВАНИЯ К УЧЕБНЫМ ДОСТИЖЕНИЯМ 8**](#_Toc98862046)

[**V. Тематическое планирование 11**](#_Toc98862047)

[**VI. СПИСОК ЛИТЕРАТУРЫ 13**](#_Toc98862048)

# ВВЕДЕНИЕ

Учебная программа среднего общего образования для курса по выбору «Основы компьютерной безопасности» разработана в соответствии с Государственными образовательными стандартами основного общего и среднего общего образования и направлена на реализацию требований предметной области «Математика и информатика».

**Программа состоит из:**

* пояснительной записки, где описывается цель и задачи курса, особенности организации учебно-воспитательного процесса и перечень программно-технических средств, необходимых для успешного проведения курса;
* содержания учебного материала и требований к учебным достижениям обучающихся;
* критериев оценивания уровня учебных достижений обучающихся и списка рекомендуемой литературы.

# I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью курса «Основы компьютерной безопасности» является формирование у обучающихся знаний и умений, необходимых для квалифицированного использования современных технологий, стандартов, протоколов и средств компьютерной безопасности.

Задачами курса являются формирование у обучающихся теоретической базы, необходимой для безопасной работы с компьютером, развитие умения использовать и самостоятельно осваивать современные программные и технические средства защиты информации, а также предоставить практические рекомендации и другую полезную информацию, необходимую для того, чтобы гарантировать психологическую, моральную и физическую безопасность детей во время работы за компьютером.

Изучение курса планируется на протяжении одного полугодия, по одному часу в неделю. Особенностью курса является то, что он требует наличия Интернет-соединения, а также наличия специального программного обеспечения, которое учителю нужно предварительно установить на все компьютеры обучающихся. Отдельные вопросы курса можно изучать лишь в режиме ознакомления без компьютера.

Программа курса рассчитана на 24 учебных часа и может преподаваться общеобразовательных организациях. Для успешного обучения по тематике курса обучающиеся должны иметь стойкие навыки работы с прикладными программами в среде Windows. После изучения этого курса у обучающихся должен быть сформирован необходимый минимум знаний, умений и навыков, благодаря которым можно успешно использовать технологии и средства защиты информации, которая хранится на компьютере, а также технологии защиты во время доступа к сети Интернет.

Курс имеет практическую направленность. Предусмотрено проведение 9 практических работ. Оценка, полученная обучающимся за выполнение практической работы, может считаться тематической оценкой соответствующей темы курса. Для выполнения практических заданий должно отводиться не меньше половины общего учебного времени.

Для *учебно-методического обеспечения курса, кроме соответствующих учебников и учебных пособий, нужны такие технические и программные средства:*

1. Компьютерный класс с локальной сетью Windows и доступом к Интернету из всех ученических компьютеров.

2. Веб-браузер.

3. Программа для работы с электронной по почте.

4. Антивирусные программы.

5. Программа для шифрования/дешифрования файлов.

6. Брандмауэр.

7. Пакет Norton Internet Security.

# II. КРИТЕРИИ ОЦЕНИВАНИЯ УРОВНЯ УЧЕБНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ

| *Уровень учебных достижений* | *Балл* | *Критерии оценивания уровня учебных достижений обучающегося* |
| --- | --- | --- |
| **Начальный** | 2 | **Обучающийся:*** объясняет основные принципы, которых нужно соблюдаться для безопасной и комфортной работы за компьютером;
* указывает на источники вредного влияния компьютера на пользователя;
* называет основные объекты, которые надо защищать в компьютерных системах и сетях, угрозы и впечатлительности информации;
* указывает на каналы распространения вирусов;
* умеет запустить антивирусную программу и проверить файл на наличие вирусов;
* дает определение конфиденциальности, доступности и целостности информации, приводит примеры их нарушение;
* описывает назначение антивирусных программ и принципы их работы;
* умеет использовать антивирусные программы, средства защиты веб-браузера и программы электронной почты;
* знает отличие между резервным копированием и архивацией файлов;
 |
| **Средний** | 3 | **Обучающийся:*** приводит классификацию угроз безопасности и уязвимости информации;
* дает определение интеллектуальной собственности, коммерческой тайны;
* описывает каналы распространения вирусов и методы предотвращения заражения вирусами;
* умеет настраивать параметры безопасности антивирусных программ и веб-браузера;
* описывает уровне защите информации в компьютерных системах и сетях;
* описывает принципы функционирования брандмауэра;
* описывает технологии поиска вирусов;
* характеризует средства обеспечения безопасности операционных систем, методы идентификации и аутентификации;
* аргументирует необходимость использования цифровой подписи, средств шифрования информации, приводит примеры методов шифрования;
* умеет применять стратегию избегания спаму и антиспамовое программное обеспечение;
* приводит примеры стандартов информационной безопасности;
* дает определение политики безопасности;
* дает сравнительную характеристику антивирусных программ;
* описывает принципы управления доступом в операционной системе Windows;
* характеризует симметричные и асимметрические алгоритмы и системы шифрования;
* умеет использовать функции управления доступом в Windows;
* умеет настраивать параметры безопасности операционной системы Windows и программ электронной почты;
* описывает использование методов социального инжиниринга, деструктивные функции программных закладок;
* дает характеристику стандартов безопасности, приводит примеры симметричных и асимметрических криптосистем и хешувальных функций;
	+ умеет налаживать параметры встроенного брандмауэра Windows;
 |
| **Достаточный** | 4 | **Обучающийся:*** умеет находить в Интернете и загружать необходимую информацию для обновления программных средств защиты, а также использует средства резервного копирования и архивации, понимает принцип работы и умеет применять программу восстановления системы Windows XP;
* объясняет опасность, связанную с сохранением cookie-файлов;
* умеет эффективно обрабатывать системный журнал Windows, использовать программу PGP для общения с другими обучающимися с помощью программ электронной почты;
* умеет налаживать средства защиты персонального компьютера, брандмауэра Zone Alarm, а также использовать пакет утилит Norton Internet Security
 |
| **Высокий** | 5 | **Обучающийся****умеет:** * сформировать политику безопасности во время работы в Internet; осуществлять защиту компьютера с помощью Центра гарантирования безопасности Windows;
* настроить параметры и использовать программу Р6Г для шифрования и дешифровку информации;
* настроить параметры программных средств безопасности персонального компьютера в локальной сети и использовать их;
* активно использует широкий спектр программного обеспечения, предназначенного для защиты информации, в частности антивирусные программы, средства защиты безопасности операционной системы, веб-браузера, почтовой программы, программы шифрования;
* самостоятельно осваивает новые средства защиты и новое программное обеспечение;
* постоянно расширяет и активно применяет знание в области информационной безопасности;
* имеет стойкие системные знания в области теории и практики использования средств информационной безопасности, умеет обеспечить комплексную защиту персонального компьютера от информационных угроз, связанных с Интернетом, в процессе выполнения задач проявляет творческий подход;
 |

# III. РАСПРЕДЕЛЕНИЕ ЧАСОВ НА ИЗУЧЕНИЕ РАЗДЕЛОВ ПРОГРАММЫ

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Раздел** | **Количество часов**  |
| 1 | Безопасная и комфортная работа за компьютером | 1 |
| 2 | Основные понятия информационной безопасности | 3 |
| 3 | Антивирусные программы и комплексы | 3 |
| 4 | Средства безопасности операционной системы Windows | 3 |
| 5 | Интернет и информационная безопасность | 4 |
| 6 | Резервное копирование и восстановление данных | 2 |
| 7 | Криптографические методы защиты информации | 6 |
|  | Резерв часа | 2 |
|  | **Итого:** | **24** |

# IV. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА И ТРЕБОВАНИЯ К УЧЕБНЫМ ДОСТИЖЕНИЯМ

|  |  |
| --- | --- |
| **Содержание учебного материала** | **Учебные достижения обучающихся** |
| **Тема 1. Безопасная и комфортная работа за компьютером (1 час)**Источники вредного влияния компьютера на пользователя. Санитарно-гигиенические требования к персональным компьютерам и к рабочему месту. Организация рабочего места пользователя компьютера ***Практическая работа № 1.*** Организация рабочего места пользователя компьютера | **Обучающийся описывает:** * санитарно-гигиенические требования к персональным компьютерам и к рабочему месту пользователя компьютера;
* источники вредного влияния компьютера на пользователя и способа нейтрализации такого влияния
 |
| **Тема 2. Основные понятия информационной безопасности (3 часа)**Основные объекты и типы информации, которые нужно защищать в компьютерных системах и сетях. Конфиденциальность, доступность и целостность информации. Классификация угроз безопасности и уязвимости информации в компьютерных системах. Этические и правовые основы защиты информации. Интеллектуальная собственность, патенты и коммерческая тайна. Стандарты информационной безопасности. Понятие о социальном инжиниринге. Политика безопасности | **Обучающийся:*** называет объекты, которые нужно защищать в компьютерных системах;
* описывает возможные угрозы безопасности информации, методы защиты информации во время ее хранения и передачи, возможные угрозы, связанные с работой в сети Интернет, критерии и классы безопасности компьютерных систем;
* приводит примеры систем, в которых нужно защищать информацию, использование методов социального инжиниринга, угроз и безопасности, и уязвимости компьютерных систем;
* объясняет особенности стандартов информационной безопасности, необходимость создания политики безопасности
 |
| **Тема 3. Антивирусные программы и комплексы (3 часа)**Классификация компьютерных вирусов. Жизненный цикл вируса. Каналы распространения вирусов и других вредных программ. Технологии поиска вирусов Антивирусные программы. Предотвращение заражения вирусами ***Практическая работа № 2.*** Настройка параметров антивирусных программ, проверка и лечение файлов и дисков | **Обучающийся:*** описывает деструктивные функции программных средств;
* объясняет способы действия вирусов и червей;
* описывает назначение антивирусных программ, основные технологии выявления вредного программного обеспечения, каналы распространения вирусов;
* классифицирует вирусы;
* сравнивает принцип действия троянских программ и червей;
* сравнивает функциональные возможности антивирусных программ;
* приводит примеры вирусов, троянских программ и червей, деструктивных проявлений вирусов, антивирусных программ;
* умеет использовать антивирусное программное обеспечение
 |
| **Тема 4. Средства безопасности операционной системы Windows (3 часа)**Средства гарантирования безопасности операционных систем. Идентификация и аутентификации пользователей. Система аудита. Управление пользователями системы ***Практическая работа № 3.*** Настройка параметров локальной политики безопасности в системе Windows ***Практическая работа № 4.*** Настройка параметров групповой политики безопасности в системе Windows | **Обучающийся:**• описывает принципы управления доступом в операционной системе Windows; • описывает методы идентификации и аутентификации, средства управления доступом и их использование; • использует функции управления доступом к ресурсам системы Windows; • осуществляет защиту компьютера с помощью Центра гарантирования безопасности Windows; • понимает информацию, приведенную в системном журнале Windows, и использует ее |
| **Тема 5. Интернет и информационная безопасность (4 часа)**Угрозы, которые приходят из Интернета. Правила безопасности во время работы в Интернете. Понятие брандмауэра. Использование брандмауэров Windows и Zone Alarm. Управление безопасностью в Internet Explorer. Защита от спама ***Практическая работа № 5.*** Настройка параметров брандмауэра Zone Alarm и брандмауэр; Windows ***Практическая работа № 6.*** Настройка параметров безопасности браузера Internet Explorer и почтовой программы Outlook Express | **Обучающийся:*** описывает распространенные способы проникновения хакеров в информационные системы, распространенные разновидности информационных атак злоумышленников, понятие спама, понятие addware и spyware, понятие брандмауэра, понятие защищенного сайта;
* называет угрозы безопасности детей во время работы в Интернете, семейные правила безопасности во время работы в Интернете, программное обеспечение, предназначенное для блокирования addware и spyware;
* объясняет методы борьбы со спамом, политику безопасности, которая регламентирует использование Интернета, принцип действия брандмауэра на локальном компьютере и в локальной сети, опасность, связанную с сохранением Cookie-Файлов;
* умеет настроить брандмауэры Windows и Zone Alarm, применять стратегию избегания спама и антиспамовое программное обеспечение;
* умеет настроить параметры безопасности браузера Internet Explorer: руководить зонами безопасности, загрузками Cookie-файлов, ограничением доступа и сертификатами
 |
| **Тема 6. Резервное копирование и восстановление данных (2 часа)**Резервное копирование и восстановление данных. Периодичность резервного копирования. Сохранение резервных копий. Программа восстановления системы Windows. Создание точек восстановления и возвращение к ним***Практическая работа № 7.*** Использование программ восстановления Windows | **Обучающийся:*** объясняет цель и процесс резервного копирования данных;
* умеет запускать программу восстановления системы Windows;
* объясняет понятие точки восстановления и называет разновидности точек восстановления;
* умеет создавать точки восстановления пользователя и возвращать систему к состоянию, которое зафиксировано раньше созданной точкой восстановления
 |
| **Тема 7. Криптографические методы защиты информации (6 часов)**Цель и применение шифрования информации. Классические методы шифрования. Симметричные алгоритмы. Поточные и блочные шифры. Асимметрические алгоритмы. Хешированные функции. Электронная цифровая подпись. Распределение ключей шифрования. Функции программы шифрования PGP и ее применение. Утилиты безопасности. Шифрование графических и звуковых файлов ***Практическая работа № 8.*** Получение и использование цифровой подписи ***Практическая работа № 9.*** Использование зашифрованных сообщений во время электронной переписки с одноклассниками | **Обучающийся:*** описывает методы шифрования и дешифрования информации;
* объясняет отличие между симметричными и асимметрическими алгоритмами шифрования, принцип действия и использования хешированных функций, функции цифровой подписи, понятие криптографической стойкости шифра, отличие между поточными и блочными шифрами;
* приводит примеры шифров замены и подстановки, симметричных и асимметрических алгоритмов шифрования;
* умеет настроить параметры и использовать программу PGP для шифрования и дешифрования информации;
* объясняет принцип действия электронной цифровой подписи;
* умеет получать в центре сертификации цифровую подпись и использовать ее для прописывания сообщений и файлов
 |
| **Резерв часа (2 часа)** |  |

# V. Тематическое планирование

| **№** | **Дата** | **Название раздела, темы урока** | **Формы организа-ции занятия** |
| --- | --- | --- | --- |
| **план** | **факт** |
| **Тема 1. Безопасная и комфортная работа за компьютером (1 час)** |
|  |   |  | Источники вредного влияния компьютера на пользователя. Санитарно-гигиенические требования к персональным компьютерам и к рабочему месту. Организация рабочего места пользователя компьютера ***Практическая работа №1.*** Организация рабочего места пользователя компьютера | Индивиду-альные |
| **Тема 2. Основные понятия информационной безопасности (3+1 часа)** |
|  |   |  | Основные объекты и типы информации, которые нужно защищать в компьютерных системах и сетях. Конфиденциальность, доступность и целостность информации.  | Индивиду-альные |
|  |   |  | Классификация угроз безопасности и уязвимости информации в компьютерных системах. | Индивиду-альные |
|  |   |  | Этические и правовые основы защиты информации. Интеллектуальная собственность, патенты и коммерческая тайна. | Подгруп-повые |
|  |  |  | Стандарты информационной безопасности. Понятие о социальном инжиниринге. Политика безопасности | Подгруп-повые |
| **Тема 3. Антивирусные программы и комплексы (3 часа)** |
|  |  |  | Классификация компьютерных вирусов. Жизненный цикл вируса. Каналы распространения вирусов и других вредных программ.  |  |
|  |  |  | Технологии поиска вирусов Антивирусные программы. | Индивиду-альные |
|  |  |  | Предотвращение заражения вирусами ***Практическая работа №2.*** Настройка параметров антивирусных программ, проверка и лечение файлов и дисков | Групповые |
| **Тема 4. Средства безопасности операционной системы Windows (3 часа)** |
|  |  |  | Средства гарантирования безопасности операционных систем. Идентификация и аутентификации пользователей.  | Индивиду-альные |
|  |  |  | Система аудита. ***Практическая работа №3.*** Настройка параметров локальной политики безопасности в системе Windows  | Подгруп-повые |
|  |  |  | Управление пользователями системы ***Практическая работа №4.*** Настройка параметров групповой политики безопасности в системе Windows | Подгруп-повые |
| **Тема 5. Интернет и информационная безопасность (4 часа)** |
|  |   |  | Угрозы, которые приходят из Интернета. Правила безопасности во время работы в Интернете.  | Группо-вые |
|  |   |  | Понятие брандмауэра. | Групповые |
|  |   |  | Использование брандмауэров Windows и Zone Alarm. ***Практическая работа №5.*** Настройка параметров брандмауэра Zone Alarm и брандмауэр; Windows | Индиви-дуальные |
|  |   |  | Управление безопасностью в Internet Explorer. Защита от спама. ***Практическая работа №6.*** Настройка параметров безопасности браузера Internet Explorer и почтовой программы Outlook Express | Индивиду-альные |
| **Тема 6. Резервное копирование и восстановление данных (2 часа)** |
|  |   |  | Резервное копирование и восстановление данных. Периодичность резервного копирования. Сохранение резервных копий.  | Индиви-дуальные |
|  |   |  | Программа восстановления системы Windows. Создание точек восстановления и возвращение к ним***Практическая работа №7.*** Использование программ восстановления Windows | Групповые |
| **Тема 7. Криптографические методы защиты информации (6+1 часов)** |
|  |   |  | Цель и применение шифрования информации. Классические методы шифрования.  | Групповые |
|  |   |  | Симметричные алгоритмы. Поточные и блочные шифры. | Подгруп-повые |
|  |   |  | Асимметрические алгоритмы. Хешированные функции. | Подгруп-повые |
|  |   |  | Электронная цифровая подпись. ***Практическая работа №8.*** Получение и использование цифровой подписи  | Подгруп-повые |
|  |  |  | Распределение ключей шифрования. Функции программы шифрования PGP и ее применение. | Подгруп-повые |
|  |   |  | Утилиты безопасности. ***Практическая работа №9.*** Использование зашифрованных сообщений во время электронной переписки с одноклассниками | Индивиду-альные |
|  |   |  | Шифрование графических и звуковых файлов  | Подгруп-повыеИндивиду-альные |

# VI. СПИСОК ЛИТЕРАТУРЫ

1. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.: ил.
2. Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации; Гелиос АРВ - Москва, 2010.
3. Смирнов С. Н. Безопасность систем баз данных; Гелиос АРВ - Москва, 2007. – 352 с.
4. Тилборг Х. К. ван А. ван Тилборг Основы криптологии. Профессиональное руководство и интерактивный учебник (+ CD-ROM); Мир - Москва, 2009. - 472 c.
5. Хорев П. Б. Программно-аппаратная защита информации; Форум - Москва, 2009. - 352 c.
6. Цирлов В. Л. Основы информационной безопасности. Краткий курс; Феникс - Москва, 2008. - 256 c.
7. Ярочкин В. И. Информационная безопасность. Учебник для вузов; Академический Проект, Мир - Москва, 2008. - 544 c.
8. Романов О. А., Бабин С. А., Жданов С. Г. Организационное обеспечение информационной безопасности; Академия - Москва, 2008. – 192 c.
9. Лапонина О. Р. Межсетевое экранирование; Интернет-университет информационных технологий, Бином. Лаборатория знаний -Москва, 2007. - 344 c.