Государственное бюджетное образовательное учреждение Самарской области средняя общеобразовательная школа села Мусорка имени Героя Советского Союза Петра Владимировича Лапшова муниципального района Ставропольский Самарской области

РАССМОТРЕНО
МО естественно-научного цикла

_____ Желнина Т.А.

Протокол № __1__

от "26" июля 2022 г.

УТВЕРЖДЕНО
Директор ГБОУ СОШ с.Мусорка

_____Новичкова Г.И.

Приказ №_39-од_

от "26" июля 2022 г.

Рабочая программа по внеурочной деятельности

Наименование **« Основы информационной безопасности»** Класс **8**

Направление внеурочной деятельности: **общеинтеллектуальное**

Рабочую программу составил учитель информатики Макарейкина Светлана Николаевна

Уровень общего образования **основная школа**

Срок реализации программы **2022-2023 учебный год**

Количество часов по учебному плану всего **34 часа в год; в неделю 1 час**

Программа разработана на основе Примерной программы учебной дисциплины **«**Основы информационной безопасности**»,** Москва, 2020 г.

ЭП

C=RU, O=ГБОУ СОШ с.Мусорка, CN=Г.И.Новичкова, E=musor_sch@samara.edu.ru 00d3691c6b8b5413 2022.10.02 12:59:22+04'00'

2022 – 2023 учебный год

Пояснительная записка

Программа по внеурочной деятельности учебной дисциплины «Основы информационной безопасности» является частью примерной основной образовательной программы в соответствии с ФГОС. Примерная программа учебной дисциплины «Основы информационной безопасности» может быть использована для разработки программ.

Место дисциплины

Дисциплина «Основы информационной безопасности» является одной из основных дисциплин базовой части. Методология курса данной дисциплины опирается на системную согласованность с сопутствующими дисциплинами профессионального цикла, а именно Технические средства информатизации, Информатика.

Цели и задачи дисциплины – требования к результатам освоения дисциплины.

Цель дисциплины «Основы информационной безопасности» имеет целью обучить учеников принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем и сетей.

«Основы информационной безопасности» является базовой для изучения дисциплин по программно-аппаратным и организационно-правовым методам обеспечения информационной безопасности.

Знания и практические навыки, полученные из курса «Основы информационной безопасности», используются учениками при изучении других специальных дисциплин.

Основная **задача** базового уровня старшей школы состоит в изучении *общих закономерностей функционирования, создания* и *применения* информационных систем, преимущественно автоматизированных. обеспечения информационной безопасности государства;

- методологии создания систем защиты информации;
- процессов сбора, передачи и накопления информации;
- оценки защищенности и обеспечения информационной безопасности компьютерных систем.

В результате изучения предмета ученик должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

В результате освоения дисциплины ученик должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности.

Планируемые результаты:

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;

3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

4. Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;

2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;

2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Планируемые результаты

В процессе освоения дисциплины у учеников должны сформироваться общие умения

1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения задач, оценивать их эффективность и качество.

3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

8. Самостоятельно определять задачи личностного развития, заниматься самообразованием, осознанно планировать.

9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Процесс изучения дисциплины направлен на формирование компетенций:

- Обеспечивать технику безопасности при проведении организационно-технических мероприятий.
- Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
- Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
- Фиксировать отказы в работе средств защиты.
- Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Планируемые результаты освоения учащимися программы курса «Основы информационной безопасности» уточняют и конкретизируют общее понимание личностных, метапредметных и предметных результатов как с позиции организации их достижения в образовательном процессе, так и с позиции оценки достижения этих результатов.

Личностные образовательные результаты: способность учащихся к саморазвитию, личностному самоопределению; развитость чувства личной ответственности за качество окружающей информационной среды; формирование ответственного отношения к учебной деятельности; формирование потребности к самообразованию, повышение своего образовательного уровня и подготовки к продолжению обучения с использованием обучающих, тестирующих

программ или иных программных продуктов; формирование целостного представления об окружающей действительности; увеличение объема информационных знаний, соответствующих уровню развития науки и общественной практики формирование уважительного и доброжелательного отношения к другому человеку, его мировоззрению; готовность и способность вести диалог с другими людьми и достижение в нём взаимопонимания; формирование нравственных чувств и нравственного поведения, ответственного отношения к собственным поступкам; развитие морального сознания; развитие умения критично относится к своим поступкам и поступкам окружающих; формирование навыков общения и сотрудничества со сверстниками и взрослыми; формирование осознанного выбора будущей профессии и возможности реализации собственных жизненных планов; готовность к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных задач.

Метапредметные образовательные результаты:

формирование умение самостоятельно определять цели своего обучения; развитие мотивов и интересов своей познавательной деятельности; формирование понимания всех этапов решения задачи; умение самостоятельно планировать пути достижения целей, выбирать оптимальные из них; умение соотносить свои действия с планируемыми результатами; умение контролировать свою деятельность в процессе достижения результата; умение корректировать свои действия в соответствии с изменяющейся ситуацией; умение оценивать правильность выполнения учебной задачи; умение правильно оценивать собственные возможности решения задачи; формирование навыков самоконтроля, самооценки своей деятельности; формирование умения давать определения понятиям; умение устанавливать причинно-следственные связи; умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; умение работать индивидуально и в группе; развитие навыков формулировать, аргументировать и отстаивать своё мнение; формирование основных понятий в области использования ИКТ.

Предметные образовательные результаты:

умение применять полученные знания, результаты изучения, методы для решения задач из различных областей; формирование информационной культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств; знание основных компонентов компьютера и их основные функции; владение навыками работы с типовым интерфейсом основного программного обеспечения; знание норм и правил, которым необходимо следовать при общении в Интернет; представление об организации информационной безопасности; умение выбирать способ представления данных в соответствии с поставленной задачей; знание технических и гигиенических требований для безопасной работы с компьютером; владение навыками использования основных средств телекоммуникаций.
После прохождения курса, должен быть достигнут следующий перечень знаний, умений и навыков учащихся.

Учащиеся должны знать:

Основные понятия и определения из области обеспечения информационной безопасности; Методы и средства борьбы с угрозами информационной безопасности; Классификацию вредоносных программ и их влияние на целостность информации; порядок заражения файлов; Методы проведения профилактики, защиты и восстановления пораженных вредоносными программами объектов; Нормативные руководящие документы, касающиеся защиты информации, существующие стандарты информационной безопасности; Принципы выбора пароля, аппаратные и программные средства для аутентификации по паролю; Основные понятия криптографических методов защиты информации, механизмы цифровой электронной подписи; Существующие программные продукты, предназначенные для защиты электронного обмена данными в Интернете, способы отделения интрасети от глобальных сетей; Нормы

информационной этики и права.

Учащиеся должны уметь:

Объяснять необходимость изучения проблемы информационной безопасности; Применять методы профилактики и защиты информационных ресурсов от вредоносного программного обеспечения; Восстанавливать повреждённую информация; Соблюдать права интеллектуальной собственности на информацию; Применять методы ограничения, контроля, разграничения доступа, идентификации и аутентификации; Производить простейшие криптографические преобразования информации; Планировать организационные мероприятия, проводимые при защите информации; Применять методы защиты информации в компьютерных сетях; Различать основные виды информационно-психологических воздействий в виртуальной реальности; Соблюдать требования информационной безопасности, этики и права; Искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества; Интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои суждения по проблемным вопросам; Сравнивать, анализировать и систематизировать имеющийся учебный материал; Участвовать в групповой работе и дискуссиях, решении задач в игровых ситуациях и проектной деятельности; Представлять результаты учебных исследовательских проектов с использованием информационно-коммуникационных технологий. Использовать возможности ОС Windows XP для защиты информации; Пользоваться архиватором и антивирусной программой.

Тематическое планирование 8 класс (1 ч/нед.)

№ урока	Тема, количество часов в неделю	Кол-во часов
1	Введение в понятие информационной безопасности.	1
2	Распространение объектно-ориентированного подхода на информационную безопасность.	1
3	Наиболее распространенные угрозы.	1
4	Законодательный уровень информационной безопасности.	1
5	Стандарты и спецификации в области информационной безопасности.	1
6	Стандарты и спецификации в области информационной безопасности.	1
7	Административный уровень информационной безопасности.	1
8	Управление рисками.	1
9	Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня.	1
10	Основные программно-технические меры. Основные понятия программно-технического уровня информационной безопасности.	1
11	Идентификация и аутентификация, управление доступом.	1
12	Основные программно-технические меры. Основные понятия программно-технического уровня информационной безопасности.	1
13	Основные программно-технические меры. Основные понятия программно-технического уровня информационной безопасности.	1
14	Экранирование, анализ защищенности. Экранирование.	1
15	Туннелирование и управление.	1
16	Виды информационных угроз	1

17	Программные средства защиты персональной информации	1
18	Технические средства защиты и комплексное обеспечение безопасности	1
19	Безопасности в сети Интернет	1
20	Составляющие информационной безопасности	1
21	Система формирования режима информационной безопасности	1
22	Составляющие информационной безопасности	1
23	Нормативно-правовые основы информационной безопасности в РФ	1
24	Стандарты информационной безопасности: "Общие критерии"	1
25	Стандарты информационной безопасности распределенных систем	1
26	Стандарты информационной безопасности	1
27	Стандарты информационной безопасности в РФ	1
28	Административный уровень обеспечения информационной безопасности	1
29	Классификация угроз "информационной безопасности	1
30	Компьютерные вирусы и защита от них	1
31	Вирусы как угроза информационной безопасности	1
32-34	**Характеристика "вирусоподобных" программ**	2
	Итого:	**34**