#### **УТВЕРЖДЕНО**

приказ № 151 от 30.08.2023 г эффектор МБОУ «Волочастский лицей»

С.В. Якушенко

#### **ОТ**РИИЧП

на заседании

подагогического совета протокол № 1 от 30 августа 2023 г

#### РАССМОТРЕНО

на заседании ППМО протокол № 1 от « 29» августа 2023 г.

# РАБОЧАЯ ПРОГРАММА И КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ ЭЛЕКТИВНОГО КУРСА

		bezon	асно	onnas emb	2007	
1800	11_			**	n ,	
o -1810/	OTRO FROMB	. и палето	_ 1 =	; за год <u></u>	<i>34</i> u	

#### Пояснительная записка

Рабочая программа элективного курса «Информационная безопасность» разработана для обучающихся 11 класса на основании ООП СОО МБОУ «Волочаевский лицей», учебного плана МБОУ «Волочаевский лицей», с использованием УМК учебной области «Информатика».

## Актуальность программы:

Курс ориентирован на подготовку подрастающего поколения к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопросы обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны.

Курс служит средством внутри профильной специализации в области информатики и информационных технологий, что способствует созданию дополнительных условий для построения индивидуальных образовательных траекторий учащихся классов информационно-технологического профиля.

Курс рассчитан на 34 часа и изучается в течении одного учебного года по 1 часу в неделю в 11 классе.

Данный курс может с успехом использоваться не только в информационнотехнологическом, но и в других профилях старшей школы, поскольку проблема информационной безопасности сегодня актуальна во всех сферах современного общества - гуманитарной, социальной, экономической и др.

Для успешного изучения курса «Компьютерная и информационная безопасность» необходимы базовые знания, полученные учащимися при изучении информатики и информационных технологий.

# Цель курса:

- · Овладение учащимися умениями: профилактики, защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.
- · Приобретение учащимися опыта по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программно-технические комплексы; опыта информационной деятельности в сферах обеспечения защиты информации, актуальных на рынке труда.
- · Приобретения учащимися опыта создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств; коллективной реализации информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебных проектов.

# Задачи курса:

Образовательные:

- · освоение учащимися знаний, относящихся к основам обеспечения информационной безопасности, и их систематизация;
- · изучение учащимися мер законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в системах связи;

#### развивающие:

- повышение интереса учащихся к изучению информатики;
- приобретение учащимися навыков самостоятельной работы с учебной, научно-

популярной литературой и материалами сети Интернет;

- · развитие у учащихся способностей к исследовательской деятельности; воспитательные:
- · воспитание у учащихся культуры в области применения ИКТ в различных сферах современной жизни;
- · воспитание у учащихся чувства ответственности за результаты своего труда, используемые другими людьми;
  - воспитание у учащихся умения планировать, работать в коллективе;
- · воспитание у учащихся нравственных качеств, негативного отношения к нарушителям информационной безопасности;
- · воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

# Контроль:

- 1. Текущий контроль: практическая работа, самостоятельная работа.
- 2. Тематический контроль: тест.
- 3. Промежуточная аттестация: контрольная работа

# Требования к уровню подготовкиучащихся:

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 вредоноснымипрограммами объектов;
- · нормативные руководящие документы, касающиеся защиты информации, существующиестандарты информационной безопасности;
- · принципы выбора пароля, аппаратные и программные средства для аутентификации попаролю;
- · основные понятия криптографических методов защиты информации, механизмыцифровой электронной подписи;
- · существующие программные продукты, предназначенные для защиты электронногообмена 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 вредоносногопрограммного обеспечения;
  - восстанавливать поврежденную информация;
  - · соблюдать права интеллектуальной собственности на информацию;
- · применять методы ограничения, контроля, разграничения доступа, идентификации иаутентификации;
- · использовать современные методы программирования для разработки сервисовбезопасности;
  - · 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 ипроектной деятельности;
- · представлять результаты учебных исследовательских проектов с использованиеминформационно-коммуникационных технологий.

#### Содержание курса

#### 1. Общие проблемы информационной безопасности (2 часа)

Информация и информационные технологии. Актуальность проблемы обеспечения безопасности информационных технологий. Основные термины и определения. Субъекты информационных отношений, их интересы и безопасность. Конфиденциальность, целостность, доступность. Пути нанесения ущерба. Цели и объекты защиты.

## 2. Угрозы информационной безопасности (6 часов)

Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика.

#### 3. Правовые основы обеспечения информационной безопасности (5 часов)

Законодательство в информационной сфере. Виды защищаемой информации. Государственная тайна как особый вид защищаемой информации; система защиты государственной тайны; правовой режим защиты государственной тайны. Конфиденциальная информация. Лицензионная и сертификационная деятельность в области защиты информации. Основные законы и другие регламентирующие деятельность нормативно-правовые документы, информации. Защита организации области информации защиты ограниченного доступа. Ответственность за нарушение законодательства в информационной сфере. Информация как объект преступных посягательств. Информация как средство совершения преступлений. Отечественные зарубежные стандарты в области информационной безопасности.

# 4. Современные методы защиты информации в автоматизированных системах обработкиданных (8 часов)

Обзор современных методов защиты информации. Основные сервисы аутентификация, управление доступом, безопасности: идентификация и протоколирование и аудит. Криптографическое преобразование информации. История криптографии; простейшие шифры и их свойства. Принципы построения криптографических алгоритмов симметричными c несимметричными ключами. Электронная цифровая подпись. Контроль целостности; экранирование; защищенности; обеспечение анализ отказоустойчивости; обеспечение безопасного восстановления.

5. Технические и организационные методы защиты информации (2 часа)

Технические средства охраны объектов (физическая защита доступа, противопожарные меры). Защита от утечки информации (перехвата данных, электростатических и электромагнитных излучений и др.). Технические средства противодействия несанкционированному съему информации по возможным каналам ее утечки. Организационные меры защиты. Определение круга лиц, ответственных за информационную безопасность, обеспечение надежной и экономичной защиты. Требования к обслуживающемуперсоналу.

6. Защита информации в компьютерных сетях (5 часов)

Примеры взломов сетей и веб-сайтов. Причины уязвимости сети Интернет. Цели, функции и задачи защиты информации в компьютерных сетях. Безопасность в сети Интернет. Методы атак, используемые злоумышлиниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д.

7. Проблемы информационно-психологической безопасности личности (5 часов)

Определение понятия информационно-психологической безопасности. Основные виды информационно-психологических воздействий. Виртуальная реальность и еè воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников. Игромания, компьютерные манипуляции, фишинг, киберугрозы и пропаганда других опасных явлений в Интернете. Способы Защиты от нежелательной информации в Интернете. Нравственно-этические проблемы информационного общества.

#### Тематический план

	Наименование разделов и	Количест
	поурочных тем	вочасов
1.	Общие проблемы информационной безопасности	2
2.	Угрозы информационной безопасности	6
3.	Правовые основы обеспечения информационной	5
	безопасности	
4.	Современные методы защиты информации	8
	вавтоматизированных системах	
	обработки данных	
5.	Технические и организационные методы защиты	2
	информации	
6.	Защита информации в компьютерных сетях	5

7.	Проблемы информационно-психологической безопасности	5
	личности	
8.	Промежуточная аттестация	1
	Всего часов:	

# Перечень учебно-методического обеспечения.

#### Дополнительная литература:

- 1. Гостехкомиссия России. Руководящий документ: Защита от несанкционированногодоступа к информации. Термины и определения. М.: ГТК 1992.
- 2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.:Издательство Агентства «Яхтсмен», 1996.
- 3. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основыкомпьютерной безопасности. М.: Радио и связь, 2000.
  - 4. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. М.: МГУЛ, 2003. 212 с.
- 5. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. М. «Радио и связь» 2003.
  - 6. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. -МЦНМО, 2003.
  - 7. Введение в криптографию. Сб. под ред. В.В.Ященко. МЦНМО, 1999.
- 8. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. М. «Радио и связь», Веста, 1992.

# Календарно – тематическое планирование

Номер	Тема	Вид урока		
урока	урока			
	Общие проблемы информационной безопасности - 2 часа			
1	Основные понятия информационной безопасности.	Лекция		
2	Актуальность проблемы обеспечения безопасности ИТ.	лекция		
	Угрозы информационной безопасности - 6 часов			
3	Понятие угрозы информационной безопасности.	Лекция		
4	Классификация видов угроз информационной безопасности по	Лекция		
_	различным признакам.	п		
5	Каналы утечки информации	Лекция		
6	Общие сведения о вредоносных программах. Компьютерные	Лекция		
7	вирусы			
7	Профилактика заражения. Методы защиты	лекция		
	компьютеров отвредоносных программ.			
	Восстановление информации	+		
		практическа		
		Я		
		работа		
8	Программные антивирусные средства.	лекция		
	Антивирусные программы.			
		+		
		практическа		
		Я		
		работа		
	равовые основы обеспечения информационной безопа асов	сности - 5		
9	Законодательство в области защиты информации.	лекция		
10	Защита информации ограниченного доступа.	лекция		
	Государственная тайна как особый вид защищаемой			
	информации; система защиты государственной тайны;	+		
	правовой режим защиты	практическа		
	государственной тайны.	я работа		
11	Конфиденциальная информация и еѐ защита.	лекция		
12	Преступление и наказание в сфере	лекция		
	информационных			
	технологий.			

13	Отечественные и зарубежные стандарты в области	лекция		
	информационных технологий.			
	Современные методы защиты информации в			
автоматизированных системах обработки данных - 8 часов.				
14	Основные сервисы безопасности. Правила создания и	лекция		
	замены			
	паролей.			
15	Идентификация и аутентификация.	лекция		
16	Управление доступом. Протоколирование и аудит.	лекция +		
		практическа		
		Я		

		работа
17	Криптография. Криптографическая защита. История	лекция
	криптографии	
18	Принципы построения криптографических	лекция
	алгоритмов ссимметричными и	
	несимметричными ключами. Электронная	+
	цифровая подпись.	практическа
		Я
		работа
19	Криптографические методы защиты информации.	практическа
		Я
	74	работа
20	Контроль целостности; экранирование; анализ защищенности.	лекция
21	Обеспечение отказоустойчивости и безопасного	лекция +
	восстановления.	практическ
		аяработа
	Технические и организационные методы хранения инфо	ормации - 2
22	часа.	лекция
23	Организационные меры защиты.	лекция +
23	организационные меры защиты.	практическ
		аяработа
	Защита информации в компьютерных сетях - 5 часо	-
24	Защита информации в компьютерных сетях.	лекция
25	Безопасность в сети Интернет	лекция
26	Защита электронного обмена данных в Интернете.	лекция
		,
		+
		практическа
		Я
		работа
27	Способы отделения интрасети от глобальных сетей.	лекция
28	Фильтрующий маршрутизатор, программный фильтр,	лекция
20	системы	
	типа FireWall (брандмауэр, экранирующий фильтр) и	
	Т.Д.	
111	Промежуточная аттестация. Тест	
	роблемы информационно-психологической безопасност сов	и личности -5
30	Информационно-психологическая	лекция
	безопасность личности в	

	информационном обществе	
31	Виртуальная реальность и еѐ воздействие на нравственное,	лекция
	духовное, эмоциональное и физическое здоровье	
	школьников.	
32	Нравственно-этические проблемы информационного общества.	лекция
33	Работа над проектом «Перспективные направления в области	практическа я
	обеспечения информационной безопасности».	работа
34	Итоговое занятие. Защита проектов.	практическа
		Я
		работа