Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 3 города Каменск-Шахтинский

ПРИНЯТО
Решением методического
объединения
кафедры учителей
естественно-математического цикла
Протокол от «_29_» _августа_2025 г. № _2_

СОГЛАСОВАНО
Заместитель директора по УВР
_____ Яценко Н.А.
«_29_» _августа_2025 г.

РАБОЧАЯ ПРОГРАММА

учебного предмета Информационная безопасность

для обучающихся 5–8 классов

Составитель:
Коновалова Елена Николаевна

2025 год

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа по информационной безопасности на уровне основного общего образования составлена на основе требований к результатам освоения основной образовательной программы основного общего образования, представленных в ФГОС ООО, а также федеральной рабочей программы воспитания.

Программа по информационной безопасности даёт представление о целях, общей стратегии обучения, воспитания и развития обучающихся средствами информационной безопасности на базовом уровне, устанавливает обязательное предметное содержание, предусматривает его структурирование по разделам и темам.

Программа по информационной безопасности определяет количественные и качественные характеристики учебного материала для каждого года изучения, в том числе для содержательного наполнения разного вида контроля (промежуточной аттестации обучающихся, всероссийских проверочных работ, государственной итоговой аттестации).

Программа по информационной безопасности является основой для составления авторских учебных программ, тематического планирования курса учителем.

Целями изучения информатики на уровне основного общего образования являются:

- активную учебно-познавательную деятельность обучающихся;
- построение образовательного процесса с учётом индивидуальных возрастных, психологических и физиологических особенностей обучающихся. Именно этот подход позволяет достичь реализации целей образовательного стандарта и сформировать личностные характеристики ученика, соответствующие «портрету выпускника основной школы». Изучение элективного курса «Информационная безопасность» позволяет гармонично сочетать обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий. 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.

Развитие глобального процесса информатизации общества, захватывающего все развитые и многие развивающиеся страны мира, приводит к

формированию новой информационной среды, информационного уклада и профессиональной деятельности. Однако при этом пропорционально возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств информационно- коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности. Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователей, компетентных в сфере защиты информации. Данный курс преследует следующие цели:

-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.

Перед данным элективным курсом ставятся следующие задачи:

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.

Рабочая программа «Информационная безопасность» предназначена для учащихся 5-6 классов. Курс рассчитан в 5 классе- 34 часа (1 час в неделю), в 6 классе -34 часа (1 час в неделю). Имеет тесную связь с учебной дисциплиной «Информатика».

СОДЕРЖАНИЕ ОБУЧЕНИЯ

1. **Общие проблемы информационной безопасности.**

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. Формы и виды работы: фронтальная беседа, работа за компьютером, демонстрация презентаций и видео – уроков.

2. **Угрозы информационной безопасности.**

Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика. Формы и виды работы: фронтальная беседа, практическая работа, работа с гаджетами (ноутбук, телефон), тестирование.

3. **Вредоносные программы. Методы профилактики и защиты.**

Общие сведения о вредоносных программах. Классификация по среде обитания, поражаемой операционной системе, особенностям алгоритма работы. Принципы функционирования, жизненный цикл и среда обитания компьютерных вирусов. Симптомы заражения и вызываемые вирусами эффекты. Полиморфные и стелс-вирусы. Вирусы макросы для MicrosoftWord и MicrosoftExcel. Вирусы-черви. Профилактика заражения. Программные антивирусные средства. Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Структура антивирусной программы. Виды антивирусных программ. Формы и виды работы: фронтальная беседа, демонстрация фото, видео-презентаций, работа за компьютером, обсуждение материала, выполнение практических работ.

4. **Правовые основы обеспечения информационной безопасности.**

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 нормативно-правовые документы, регламентирующие деятельность организации в области защиты информации. Защита информации ограниченного доступа. Ответственность

за нарушение законодательства в информационной сфере. Информация как объект преступных посягательств. Информация как средство совершения преступлений. Отечественные и зарубежные стандарты в области информационной безопасности. Формы и виды работы: фронтальная беседа, выполнение практических работ, работа за компьютером.

5. **Современные методы защиты информации в автоматизированных системах обработки данных.**

Обзор современных методов защиты информации. Основные сервисы безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит. Криптографическое преобразование информации. История криптографии; простейшие шифры и их свойства. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Электронная цифровая подпись. Контроль целостности; экранирование; анализ защищённости; обеспечение отказоустойчивости; обеспечение безопасного восстановления. Формы и виды работы: фронтальная беседа, выполнение практических работ в группе и самостоятельно, работа с гаджетами (телефон, ноутбук).

6. **Технические и организационные методы защиты информации.**

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 съёму информации по возможным каналам её утечки. Организационные меры защиты. Определение круга лиц, ответственных за информационную безопасность, обеспечение надёжной и экономичной защиты.
Требования к обслуживающему персоналу. Формы и виды работы: фронтальные беседы, выполнение практических работ, работа с гаджетами (компьютер, телефон).

7. **Защита информации в компьютерных сетях.**

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 злоумышленниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д. Формы работы: фронтальная беседа, прохождение тестирований, работа с компьютером.

8. **Проблемы информационно–психологической безопасности личности.** Определение понятия информационно-психологической безопасности. Основные виды информационно-психологических воздействий. Виртуальная реальность и ее 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. Формы и виды работ: фронтальная беседа, демонстрация фото и видео материалов, выполнение практических работ в парах, работа с гаджетами (телефон, компьютер).

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

В соответствии с федеральным государственным стандартом основного общего образования содержание данного предмета определяет достижения личностных, метапредметных и предметных результатов освоения курса внеурочной деятельности

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, эстетические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

1. Развивается 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 коммуникативных технологий.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

1. Сформировать знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформировать умения соблюдать нормы информационной этики;
3. Сформировать умения безопасно работатьс информацией, анализировать и обобщать полученную информацию.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
5 КЛАСС

№ п/п	Наименованиеразделов и темпрограммы	Количествочасов			Электронные (цифровые) образовательныересурсы
		Всего	Контрольныеработы	Практическиеработы	
1	Общиепроблемыинформационнойбезопасности	6			https://lbz.ru/metodist/authors/ib/5-6.php
2	Угрозыинформационнойбезопасности	8			https://lbz.ru/metodist/authors/ib/5-6.php
3	Вредоносные программы. Методы профилактики и защиты	8			https://lbz.ru/metodist/authors/ib/5-6.php
4	Правовые основы обеспечения информационной безопасности	12	1		https://lbz.ru/metodist/authors/ib/5-6.php
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	0	

6 КЛАСС

№ п/п	Наименованиеразделов и темпрограммы	Количествочасов			Электронные (цифровые) образовательныересурсы
		Всего	Контрольныеработы	Практическиеработы	
1	Современные методы защиты информации в автоматизированных системах обработки данных	12			https://lbz.ru/metodist/authors/ib/5-6.php
2	Технические и организационные методы защиты информации	6			https://lbz.ru/metodist/authors/ib/5-6.php
3	Защита информации в компьютерных сетях	8			https://lbz.ru/metodist/authors/ib/5-6.php
4	Проблемы информационно-психологической безопасности личности	8	1		https://lbz.ru/metodist/authors/ib/5-6.php
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	0	

7 КЛАСС

№ п/п	Наименованиеразделов и темпрограммы	Количествочасов			Электронные (цифровые) образовательныересурсы
		Всего	Контрольныеработы	Практическиеработы	
1	Киберпространство	22			https://lbz.ru/metodist/authors/ib/7-9.php
2	Киберкультура	12	1		https://lbz.ru/metodist/authors/ib/7-9.php
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	0	

8 КЛАСС

№ п/п	Наименованиеразделов и темпрограммы	Количествочасов			Электронные (цифровые) образовательныересурсы
		Всего	Контрольныеработы	Практическиеработы	
1	Киберкультура	10			https://lbz.ru/metodist/authors/ib/7-9.php
2	Киберугрозы	24	1		https://lbz.ru/metodist/authors/ib/7-9.php
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	0	

9 КЛАСС

№ п/п	Наименованиеразделов и темпрограммы	Количествочасов			Электронные (цифровые) образовательныересурсы
		Всего	Контрольныеработы	Практическиеработы	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		0	0	0	

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
5 КЛАСС

№ п/п	Темаурока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Чтотакоеинформационноеобщество	1				
2	Историясозданиясетиинтернет	1				
3	Историясозданиясетиинтернет	1				
4	Чтотакоевсемирнаяпаутина	1				
5	Чтотакоевсемирнаяпаутина	1				
6	Путешествие по сети интернет: сайты и электронные сервисы	1				
7	Путешествие по сети интернет: сайты и электронные сервисы	1				
8	Путешествие по сети интернет: сайты и электронные сервисы	1				
9	Путешествие по сети интернет: сайты и электронные сервисы	1				
10	Как стать пользователем сети Интернет	1				
11	Как стать пользователем сети Интернет	1				
12	Опасности для пользователей сети Интернет	1				
13	Опасности для пользователей сети Интернет	1				
14	Чтотакоекибератака	1				

15	Чтотакоекибератака	1				
16	Чтотакоекибератака	1				
17	Чтотакоеинформационнаябезопасность	1				
18	Чтотакоеинформационнаябезопасность	1				
19	Законы о защите личных данных в Интернете	1				
20	Законы о защите личных данных в Интернете	1				
21	Законы о защите личных данных в Интернете	1				
22	Сетевой этикет	1				
23	Сетевой этикет	1				
24	Коллекция сайтов для детей	1				
25	Коллекция сайтов для детей	1				
26	Коллекция сайтов для детей	1				
27	Электронные музеи	1				
28	Электронные музеи	1				
29	Электронные музеи	1				
30	Электронные музеи	1				
31	Электронные музеи	1				
32	Контрольная работа	1	1			
33	Обобщающий урок	1				
34	Резерв учебного времени	1				
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	0		

6 КЛАСС

№ п/п	Темаурока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Правилаработы с СМС	1				
2	Правила работы с СМС	1				
3	Правила работы с электронной почтой	1				
4	Правила работы с электронной почтой	1				
5	Правилаработы с видеосервисами	1				
6	Правилаработы с видеосервисами	1				
7	Правилаработы с видеосервисами	1				
8	Правила работы в социальных сетях	1				
9	Правила работы в социальных сетях	1				
10	Правила работы в социальных сетях	1				
11	Правила защиты от вируса, спама, рекламы и рассылок	1				
12	Правила защиты от негативных сообщений	1				
13	Правила общения в социальной сети	1				
14	Правила общения в социальной сети	1				
15	Правила общения в социальной сети	1				
16	Контрольнаяработаза 1 полугодие	1	1			
17	Правила общения в социальной сети	1				
18	Правила работы с поисковыми системами и анализ информации	1				

19	Правила работы с поисковыми системами и анализ информации	1				
20	Правила ответственности за распространение ложной и негативной информации	1				
21	Правила ответственности за распространение ложной и негативной информации	1				
22	Правила защиты от нежелательных сообщений и контактов	1				
23	Правила защиты от нежелательных сообщений и контактов	1				
24	Правилавызоваэкстреннойпомощи	1				
25	Правила защиты устройств от внешнего вторжения	1				
26	Правила защиты устройств от внешнего вторжения	1				
27	Правила защиты устройств от внешнего вторжения	1				
28	Правила выбора полезных ресурсов в Интернете	1				
29	Правила выбора полезных ресурсов в Интернете	1				
30	Правила выбора полезных ресурсов в Интернете	1				
31	Контрольнаяработаза 2 полугодие	1	1			
32	Средства работы в интернете для людей с особыми потребностями	1				

33	Обобщающийурок	1				
34	Резервучебноговремени	1				
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	2	0		

7 КЛАСС

№ п/п	Темаурока	Количествочасов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Киберпространство	1				
2	Киберпространство	1				
3	Киберпространство	1				
4	Кибермиры	1				
5	Кибермиры	1				
6	Кибермиры	1				
7	Киберфизическаясистема	1				
8	Киберфизическаясистема	1				
9	Киберфизическаясистема	1				
10	Киберобщество	1				
11	Киберобщество	1				
12	Киберобщество	1				
13	Киберобщество	1				
14	Киберденьги	1				
15	Киберденьги	1				
16	Киберденьги	1				
17	Кибермошенничество	1				
18	Кибермошенничество	1				
19	Кибермошенничество	1				
20	Кибермошенничество	1				

21	Практикум к разделу 1	1		1		
22	Практикум к разделу 1	1		1		
23	Тест 1. Киберпространство	1		1		
24	Киберкультура	1				
25	Киберкультура	1				
26	Киберкультура	1				
27	Откниги к гипертексту	1				
28	Откниги к гипертексту	1				
29	Киберкнига	1				
30	Киберкнига	1				
31	Контрольная работа по изученному материалу	1	1			
32	Киберкнига	1				
33	Киберискусство	1				
34	Киберискусство	1				
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	3		

8 КЛАСС

№ п/п	Темаурока	Количествочасов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Социальнаяинженерия	1				
2	Социальнаяинженерия	1				
3	Социальнаяинженерия	1				
4	Классификацияугрозсоциальнойинженерии	1				
5	Классификацияугрозсоциальнойинженерии	1				
6	Классификацияугрозсоциальнойинженерии	1				
7	Практикум к разделу 2	1		1		
8	Практикум к разделу 2	1		1		
9	Практикум к разделу 2	1		1		
10	Тест 2. Киберкультура	1		1		
11	Кибервойны	1				
12	Кибервойны	1				
13	Кибервойны	1				
14	Киберприступность	1				
15	Киберприступность	1				
16	Киберприступность	1				
17	Примерыкиберпреступлений	1				
18	Примерыкиберпреступлений	1				
19	Примерыкиберпреступлений	1				
20	Уязвимостькибербезопасности	1				

21	Уязвимостькибербезопасности	1				
22	Уязвимость кибербезопасности	1				
23	Угрозы информационной безопасности	1				
24	Угрозы информационнойбезопасности	1				
25	Угрозы информационной безопасности	1				
26	Запрещенные и нежелательные сайты	1				
27	Запрещенные и нежелательные сайты	1				
28	Новые профессии в киберобществе	1				
29	Контрольная работа по пройденному материалу	1	1			
30	Новые профессии в киберобществе	1				
31	Практикум к разделу 3	1		1		
32	Практикум к разделу 3	1		1		
33	Тест 3. Киберугрозы	1		1		
34	Новыепрофессии в киберобществе	1				
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	1	7		

9 КЛАСС

№ п/п	Тема урока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		0	0	0		

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 668457944626561634972740990882929036601482128234

Владелец Золотова Ирина Александровна

Действителен С 18.02.2025 по 18.02.2026