Приложение 3.18
Основной образовательной программы среднего общего образования МАОУ СОШ п. Цементный, утвержденной приказом
№ 216-Д от 29 августа 2025 г.

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования и молодежной политики Свердловской области

Управление образования Невьянского городского округа

МАОУ СОШ п. Цементный

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
ШМО учителей математики и информатики	Заместитель директора по УВР	Директор МАОУ СОШ п. Цементный
Курылева Н.А.	Откидач Ю.Н.	Арапова О.В.
Протокол № 1 от «29» августа 2025 г.	«29» августа 2025 г.	Приказ № 216-Д от «29» августа 2025 г.

РАБОЧАЯ ПРОГРАММА

факультативного курса

«Информационная безопасность»

для обучающихся 11 класса

Составитель: Томм Ольга Александровна,
учитель информатики МАОУ СОШ п. Цементный

п. Цементный, 2025 г

Пояснительная записка
к рабочей программе факультативного курса «информационная безопасность» для уровня среднего общего образования

Рабочая программа факультативного курса «Информационная безопасность» для 11 класса составлена на основе Федерального государственного образовательного стандарта среднего общего образования, Основной образовательной программы среднего общего образования МАОУ СОШ п. Цементный.

Цели и задачи 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:

- освоить знания, относящихся к основам обеспечения информационной безопасности, и их систематизация;
-изучить меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в системах связи;
- повышать интерес учащихся к изучению информатики;
- приобрести навыки самостоятельной работы с учебной, научно-популярной литературой и материалами сети Интернет;
- развивать способности к исследовательской деятельности;
- воспитывать культуру в области применения ИКТ в различных сферах современной жизни;
- воспитывать нравственные качества, негативное отношение к нарушителям информационной безопасности;
- настраивать на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

Факультативный курс «Информационная безопасность» направлен на

продолжение формирования знаний учащихся старших классов о системах искусственного интеллекта как одной из наиболее перспективной и развивающейся областей научного и технологического знания. Данный курс развивает интерес к исследовательской деятельности, способствует развитию профессиональной ориентации учащихся, ориентирован на подготовку подрастающего поколения к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопрос обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны.

Данный 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.

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

Тематическое планирование данной рабочей программы предполагает учет и использование целевых установок рабочей программы воспитания, которая реализуется в единстве урочной и внеурочной деятельности. Факультативный курс «Информационная безопасность» является дополнительным курсом по выбору учебного плана МАОУ СОШ п. Цементный и на уровне среднего общего образования изучается в 11 классе. Общее количество времени в рамках программы составляет 34 часа (1 час в неделю).

Планируемые результаты освоения факультативного курса «Информационная безопасность»

Занятия в рамках программы направлены на обеспечение достижений обучающимися следующих личностных, метапредметных и предметных образовательных результатов. Они формируются во всех направлениях функциональной грамотности, при этом направление формирования имеет приоритетное значение.

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Формирование у учащегося мировоззрения, соответствующего современному уровню развития науки и общества. Формирование у учащегося интереса к достижениям науки и технологии в области информационной безопасности. Формирование у учащегося установки на осмысленное и безопасное взаимодействие с технологиями и устройствами, реализованными на основе принципов информационной безопасности. Приобретение опыта творческой деятельности, опирающейся на использование современных информационных технологий.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Познавательные УУД:
Умение работать с информацией, анализировать и структурировать полученные знания и синтезировать новые, устанавливать причинно-следственные связи. Умения объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности. Умение делать выводы на основе критического анализа разных точек зрения, подтверждать их собственной аргументацией или самостоятельно полученными данными. Умение анализировать/рефлексировать опыт исследования (теоретического, эмпирического) на основе предложенной ситуации, поставленной цели; Умение строить рассуждение на основе сравнения предметов и явлений.
Регулятивные УУД:
Умение обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логику. Умение планировать необходимые действия в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения. Умение описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса. Умение выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели в ходе исследовательской деятельности. Умение принимать решение в игровой и учебной ситуации и нести за него ответственность. **Коммуникативные УУД**
Умение взаимодействовать в команде, умением вступать в диалог и вести его. Умение соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей. Умение определять свои действия и действия партнеров для продуктивной коммуникации. Умение приходить к консенсусу в дискуссии или командной работе.
ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ
Иметь представления об информационной безопасности, ее возможностях и ограничениях; и сферах его применения; выявлять и формулировать задачи информационной безопасности для различных сфер жизни человека и в соответствии с реальными потребностями.

Содержание факультативного курса «Информационная безопасность»

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 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.

4. **Современные методы защиты информации в автоматизированных системах обработки данных (8 часов)**

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 защищѐнности; обеспечение 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 съѐму информации по возможным каналам еѐ утечки. Организационные меры защиты. Определение круга лиц, ответственных за информационную безопасность, обеспечение надѐжной и экономичной защиты. Требования к обслуживающему персоналу.

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 еѐ 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.

Тематическое планирование

№	Тема	Кол-во часов	Цифровые образовательные ресурсы
1.	Общие проблемы информационной безопасности	2	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
2.	Угрозы информационной безопасности	6	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
3.	Правовые основы обеспечения информационной безопасности	5	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
4.	Современные методы защиты информации в автоматизированных системах обработки данных	8	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
5.	Технические и организационные методы защиты информации	2	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
6.	Защита информации в компьютерных сетях	5	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
7.	Проблемы информационно-психологической личности	5	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
8.	Промежуточная аттестация	1	Библиотека ЦОК. РЭШ. https://fipi.ru/oge/otkrytyy-bank-zadaniyoge#!/tab/173942232-3
	Всего часов:	34	

Календарно-тематическое планирование

№ п / п	Тема занятия	Форма
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 различным признакам.	Лекция
5	Каналы утечки информации	Лекция
6	Общие сведения о вредоносных программах. Компьютерные вирусы	Лекция
7	Профилактика заражения. Методы защиты компьютеров от вредоносных программ. Восстановление информации	лекция+ практическая работа
8	Программные антивирусные средства. Антивирусные программы.	лекция+ практическая работа
Правовые основы обеспечения информационной безопасности - 5 часов		
9	Законодательство в области защиты информации.	лекция
10	Защита информации ограниченного доступа. Государственная тайна как особый вид защищаемой информации; система защиты государственной тайны; правовой режим защиты государственной тайны.	лекция+ практическая работа
11	Конфиденциальная информация и еѐ защита.	лекция
12	Преступление и наказание в сфере информационных технологий.	лекция
13	Отечественные и зарубежные стандарты в области информационных технологий.	лекция
Современные методы защиты информации в автоматизированных системах обработки данных - 8 часов.		

14	Основные сервисы безопасности. Правила создания и замены паролей.	лекция
15	Идентификация и аутентификация.	лекция
16	Управление доступом. Протоколирование и аудит.	лекция+практическая работа
17	Криптография. Криптографическая защита. История криптографии	лекция
18	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Электронная цифровая подпись.	лекция+ практическая работа
19	Криптографические методы защиты информации.	Практическая работа
20	Контроль целостности; экранирование; анализ защищѐнности.	лекция
21	Обеспечение отказоустойчивости и безопасного восстановления.	лекция+практическая работа
Технические и организационные методы хранения информации - 2 часа. лекция		
22	Технические средства защиты информации.	лекция+практическая работа
23	Организационные меры защиты.	
Защита информации в компьютерных сетях - 5 часов.		
24	Защита информации в компьютерных сетях.	лекция
25	Безопасность в сети Интернет	лекция
26	Защита электронного обмена данных в Интернете.	лекция+ практическаяработа

27	Способы отделения интрасети от глобальных сетей.	лекция
28	Фильтрующий маршрутизатор, программный фильтр, системы типа FireWall (брандмауэр, экранирующий фильтр) и т.д.	лекция
29	Промежуточная аттестация. Тест	
Проблемы информационно-психологической безопасности личности -5 часов		
30	Информационно-психологическая безопасность личности в информационном обществе	лекция
31	Виртуальная реальность и еѐ воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников.	лекция
32	Нравственно-этические проблемы информационного общества.	лекция
33	Работа над проектом «Перспективные направления в области обеспечения информационной безопасности».	Практическая работа
34	Итоговое занятие. Защита проектов.	Практическая работа

Используемая литература:

1. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа 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 основы компьютерной 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.