МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Московской области
Администрация Одинцовского городского округа
МБОУ Одинцовская лингвистическая гимназия

РАССМОТРЕНО

руководитель ШМО

_____
Лазарева И.М.
Протокол заседания
кафедры № 1
от «27» августа 2025 г.

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Основы информационной безопасности
для обучающихся 11 классов

Данные электронной подписи
Владелец: Кобзенко Ирина Константиновна Директор
Организация: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ОДИНЦОВСКАЯ ЛИНГВИСТИЧЕСКАЯ ГИМНАЗИЯ 281100405009

Данные сертификата
Серийный номер:
008C E0FE 4362 1BF0 FBB9 8B84 32BA B9AB 7C
Срок действия: 20.08.2025 - 13.11.2026

Одинцово 2025

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Сегодня уже ни у кого не вызывает сомнения тот факт, что XXI век - век информации и научных знаний. Развитие глобального процесса информатизации общества, охватывающего 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. Под информационной безопасностью понимается область науки и техники, охватывающая совокупность программных, аппаратных и организационно-правовых методов и средств обеспечения безопасности информации при обработке, хранении и передаче с использованием современных информационных технологий. А так же под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Под угрозой информационной безопасности понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

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. Задача подготовки таких специалистов является особенно актуальной ещё и потому, что одной из важнейших задач современности является борьба с компьютерной преступностью и кибертерроризмом. Спектр преступлений в сфере информационных технологий весьма широк, он варьируется от интернет-мошенничества и до такой потенциально опасной деятельности, как электронный шпионаж и подготовка к террористическим актам.

В настоящее время достаточно свободно распространяются различные печатные издания, где описываются технологии совершения компьютерных преступлений; публикуются книги, освещающие приёмы атак на

информационные системы. В Интернете представлено огромное количество сайтов, обучающих компьютерному взлому, проводятся форумы, виртуальные конференции и семинары по «повышению квалификации» и «обмену опытом» совершения компьютерных преступлений. Среди выявленных преступников, в отношении которых возбуждены дела за противоправные действия в сфере информационных технологий, свыше 75% составляет молодёжь. Всё это подчёркивает важность ещё одной задачи - активного противодействия вовлечению молодёжи в преступную среду и разработки активных методов проведения воспитательной работы среди молодёжи. Очевидно, что насущной задачей современного образования становится разработка таких методов учебно-воспитательной работы, которые гармонично сочетают обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий.

Таким образом, можно считать актуальным и значительным старших классов изучение внеурочного курса «Информационная безопасность». 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 рассчитан на 34 часа и изучается в течении одного учебного года по 1 часу в неделю в 11 классе.

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

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСТЬ

Программа курса по информационной безопасности для старших школьников предназначен для ознакомления учащихся с основами защиты информации в условиях современного цифрового мира. Он включает изучение законодательных актов, этических норм, технических средств обеспечения информационной безопасности, а также социальных аспектов информационной безопасности. Особое внимание уделяется практическим навыкам, таким как использование антивирусных программ, настройка межсетевых экранов, а также основам шифрования данных. В рамках курса

проводятся практические занятия, направленные на развитие умений и навыков работы с различными инструментами защиты информации.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСТЬ

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.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСТЬ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Особенностью программы курса является ее включение в контекст не только обучения, но и воспитания в условиях быстро нарастающих новых видов информационных угроз и развития средств противодействия им, отраженных в законодательстве Российской Федерации.

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСТЬ

- познавательная беседа;

- изучение терминов;
- практические занятия;
- проектная деятельность;
- лекции.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСТЬ

Основы информационной безопасности

Введение в информационную безопасность: понятие информации и ее значение в современном мире, основные угрозы информационной безопасности, а также значение защиты информации для личности, общества и государства.

Основные законодательные акты РФ в области информационной безопасности и ответственность за нарушение законодательства в сфере информационной безопасности. Этические аспекты информационной безопасности, принципы поведения при работе с информацией.

Вопросы безопасности информационных систем

Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД. Защита государственных информационных систем

Проблемы безопасности банковских и платежных систем. Безопасность геоинформационных систем. Безопасность корпоративных баз данных.

Хакерские атаки и их классификация. Виды атак. Кибербезопасность и киберпространство. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств. Рост числа атак на инфраструктуру. Кибершпионаж. Кибероружие.

Технические средства обеспечения информационной безопасности

Антивирусные программы. Функции антивирусного программного обеспечения, правила использования антивирусных программ. Установка и настройка антивирусной программы. Проведение сканирования системы на наличие вирусов

Роль межсетевых экранов в защите информации, принцип их работы. Установка и настройка межсетевых экранов.

Шифрование данных. Методы шифрования данных, использование шифрования в различных ситуациях. Шифрование файлов и папок. Дешифровка защищенных данных.

Социальные аспекты информационной безопасности

Социальные сети и интернет-мемы. Влияние социальных сетей на общество. Безопасность личных данных в социальных сетях.

Понятия кибербуллинга и киберпреступлений. Меры по предотвращению и борьбе с кибербуллингом и киберпреступлениями.

Сущность фишинговых атак и спама. Способы защиты от фишинговых атак и спама.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Планируемые результаты по программе соотнесены с задачами и содержанием программы. Обучающиеся к концу обучения должны иметь следующие результаты:

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Личностными результатами обучающихся являются:

– готовность к самоидентификации в окружающем мире на основе критического анализа информации, отражающей различные точки зрения на смысл и ценности жизни;

– владение навыками соотношения получаемой информации с принятыми в обществе моделями, например, морально-этическими нормами, критическая оценка информации в СМИ;

– умение создавать и поддерживать индивидуальную информационную среду, обеспечивать защиту значимой информации и личную информационную безопасность, развитие чувства личной ответственности за качество окружающей информационной среды;

– приобретение опыта использования информационных ресурсов общества и электронных средств связи в учебной и практической деятельности; освоение типичных ситуаций по настройке и управлению персональных средств ИКТ, включая цифровую бытовую технику;

– умение осуществлять совместную информационную деятельность, в частности при выполнении учебных проектов;

– повышение своего образовательного уровня и уровня готовности к продолжению обучения с использованием ИКТ;

– формирование ответственного отношения к учению, готовности и способности, обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;

– формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;

– развитие осознанного и ответственного отношения к собственным поступкам;

– формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Метапредметными результатами обучающихся являются:

– умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

– владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;

– умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;

– умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

– смысловое чтение; умение осознанно использовать речевые средства в соответствии с задачей коммуникации;

– формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ - компетенции).

– владение навыками постановки задачи на основе известной и усвоенной информации и того, что ещё неизвестно;

– планирование деятельности: определение последовательности промежуточных целей с учётом конечного результата, составление плана и последовательности действий;

– прогнозирование результата деятельности и его характеристики;

– контроль в форме сличения результата действия с заданным эталоном; коррекция деятельности: внесение необходимых дополнений и корректив в план действий;

– умение выбирать источники информации, необходимые для решения задачи (средства массовой информации, электронные базы данных, информационно-телекоммуникационные системы, Интернет, словари, справочники, энциклопедии и др.);

– умение выбирать средства ИКТ для решения задач из разных сфер человеческой деятельности;

– выбор языка представления информации в модели в зависимости от поставленной задачи.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Предметными результатами обучающихся являются:

– понимание основных проблем защиты информации;

– следование нормам жизни и труда в условиях информационной цивилизации;

– приобретение опыта выявления информационных технологий, разработанных со скрытыми целями;

– соблюдение норм этикета, российских и международных законов при передаче информации по телекоммуникационным каналам;

– расширение представления о правовых и морально-этических нормах в информационной сфере, законодательстве Российской федерации в области защиты информации и авторского права;

– формирование чувства ответственности за производство и распространение информации;

– понимание роли информационных процессов как фундаментальной реальности окружающего мира и определяющего компонента современной информационной цивилизации;

– определение средств информационных технологий, реализующих основные информационные процессы;

– понимание принципов действия различных средств информатизации, их возможностей и технических и экономических ограничений;

– выбор средств информационных технологий для решения поставленной задачи;

– приобретение опыта создания и преобразования информации различного вида, в том числе с помощью компьютера;

– приобретение опыта создания эстетически значимых объектов с помощью возможностей средств информационных технологий (графических, цветовых, звуковых, анимационных);

– понимание особенностей работы со средствами информатизации, их влияния на здоровье человека, владение профилактическими мерами при работе с этими средствами;

– приобретение навыков защиты информации;

– соблюдение требований безопасности и гигиены в работе с компьютером и другими средствами информационных технологий.

11 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
Раздел 1. Основы информационной безопасности					
	Введение в информационную безопасность	4	Общие сведения об информации и информационной безопасности.	познавательная беседа; изучение терминов; лекции	
	Законодательство в области информационной безопасности	2	Защита персональных данных, кибербезопасность, ответственность за нарушения, сообщение о нарушениях и международное сотрудничество.	познавательная беседа; изучение терминов; проектная деятельность; лекции	
	Этические аспекты информационной безопасности	2	Моральные принципы и нормы, которые необходимо соблюдать при работе с данными и информационными системами.	познавательная беседа; лекции	
Итого по разделу		8			
Раздел 2. Вопросы безопасности информационных систем					

	Безопасность информационных систем	6	Комплекс мер и технологий, направленных на защиту информации и информационных ресурсов от несанкционированного доступа, утраты, повреждения или изменения.	познавательная беседа; изучение терминов; лекции	
	Основные виды угроз информационной безопасности	3	Основные виды угроз информационной безопасности включают несанкционированный доступ, утечку данных, вирусные атаки, фишинговые атаки, DDoS-атаки, взлом учетных записей, шпионское ПО.	изучение терминов; проектная деятельность; лекции	
Итого по разделу		9			
Раздел 3. Технические средства обеспечения информационной безопасности					
	Антивирусные программы	4	Антивирусные программы, их виды и функции. Установка и настройка антивирусных	изучение терминов; лекции практические занятия;	

			программ.		
	Межсетевые экраны	3	Роль и принципы работы межсетевых экранов. Установка и настройка межсетевых экранов.	изучение терминов; лекции практические занятия;	
	Шифрование данных	4	История возникновения шифров. Симметричное и ассиметричное шифрование. Применения алгоритмов шифрования на практике.	изучение терминов; лекции практические занятия;	
Итого по разделу		11			
Раздел 4. Социальные аспекты информационной безопасности					
	Социальные сети и интернет-мемы	2	Влияние социальный сетей на общество и защита личных данных в социальных сетях.	познавательная беседа; изучение терминов; лекции	
	Кибербуллинг и киберпреступления	2	Что такое кибербуллинг и киберпреступления. Меры борьбы с ними.	познавательная беседа; изучение терминов; лекции	
	Фишинговые атаки и спам	2	Фишинговые атаки и	познавательная	

			спам, меры борьбы с ними.	беседа; изучение терминов; лекции	
Итого по разделу		6			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		**34**			

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
11 КЛАСС

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Вводное занятие	1			
2	Понятие информации и ее значение в современном мире	1			
3	Основные угрозы информационной безопасности	1			
4	Значение защиты информации для личности, общества и государства	1			
5	Основные законодательные акты РФ в области информационной безопасности	1			
6	Ответственность за нарушение законодательства в сфере информационной безопасности	1			
7	Этика и профессиональная этика в информационной среде	1			
8	Принципы поведения при работе с информацией	1			
9	Проблемы безопасности информационных систем	1			
10	Защита государственных информационных систем	1			
11	Проблемы безопасности банковских систем	1			
12	Безопасность платежных систем	1			
13	Безопасность геоинформационных систем	1			
14	Безопасность корпоративных баз данных	1			
15	Хакерские атаки. Виды атак	1			

16	Кибербезопасность и киберпространство	1			
17	Новые технологии и новые угрозы информационной безопасности	1			
18	Функции антивирусного программного обеспечения	1			
19	Правила использования антивирусных программ	1			
20	Установка и настройка антивирусной программы	1		1	
21	Проведение сканирования системы на наличие вирусов	1		1	
22	Роль межсетевых экранов в защите информации	1			
23	Принцип работы межсетевых экранов	1			
24	Установка и настройка межсетевых экранов	1		1	
25	Методы шифрования данных	1			
26	Использование шифрования в различных ситуациях	1			
27	Шифрование файлов и папок	1		1	
28	Дешифровка защищенных данных	1		1	
29	Влияние социальных сетей на общество	1			
30	Безопасность личных данных в социальных сетях	1			
31	Понятия кибербуллинга и киберпреступлений	1			
32	Меры по предотвращению и борьбе с кибербуллингом и киберпреступлениями	1			
33	Сущность фишинговых атак и спама	1			
34	Способы защиты от фишинговых атак и спама	1			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	5	