МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Комитет по образованию Санкт-Петербурга
Администрация Приморского района Санкт-Петербурга
Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 320

Принято
решением
Педагогического совета
от 30.08.2023
протокол № 1

«Утверждаю»
Директор ГБОУ школы № 320

_____ И.Б.Черноус

Приказ № 227-Д от 30.08.2023

Документ подписан электронной подписью
Сертификат: 14e37f57a1217b6fc965c72e488707db
Кому выдан: Черноус Ирина Борисовна
Действителен: с 10.05.2023 по 02.08.2024

Принято
с учетом
мотивированного
мнения совета родителей
протокол № 1 от 29.08.2023

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

«Информационная безопасность»

для обучающихся 10 классов

Санкт-Петербург
2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Характеристика курса внеурочной деятельности:

Курс внеурочной деятельности «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Правовая грамотность приобретает новый ракурс в связи с процессом информатизации всех сфер деятельности человека, включая и школьное образование. Роль информации в данном процессе достаточно велика, и, по мнению ведущих специалистов в области информационной безопасности, она на сегодняшний день занимает уровень главного ресурса развития человеческой цивилизации. Более того, информация наряду с веществом и энергией стала основой всего научного знания и жизни человека. В этой связи вопросы, касающиеся информационной безопасности, являются составной частью правовой культуры и совершенно очевидно, что они должны занимать значительное место в содержании школьного курса информатики.

Программа курса «Информационной безопасности» ориентирована на учащихся, проявляющих интерес к различным аспектам защиты информации, желающих углубленно изучить правовые аспекты информационной безопасности, и рассчитана на учеников, имеющих подготовку по информатике в объеме, соответствующем требованиям стандарта среднего общего образования по информатике и информационным технологиям.

Курс включает в себя как теорию, так и практику. Теория дает знания о предмете безопасности, проблемах ее обеспечения и принципах их решения. В результате практических занятий формируются умения оформления информационных объектов с целью обеспечения их безопасного состояния.

Особый характер тематики обучения требует дискуссионной формы организации занятий, когда ученики вовлекаются в круг проблем, смело высказывают свои мнения и суждения по каждому вопросу. Практическая работа осуществляется учеником на персональном компьютере, где в отдельной папке он формирует файлы-документы и производит над ними соответствующие действия.

Содержание обучения, формы занятий, проектная деятельность предусматривают развитие межпредметных связей - опору на знания других разделов информатики, истории, обществознания, естествознания и др.

Цель изучения курса внеурочной деятельности:

дать понятие информационной безопасности, целей и задач информационной безопасности, структуры предмета информационной безопасности и ее обеспечения; представление о защите информации, ее формах, структуре, функциях и задачах; сформировать у учащихся представление об основных проблемах информационной безопасности, принципах и подходах к их решению; сформировать у учащихся компетенций в следующих областях:

○ обеспечение информационной безопасности;
○ правовые аспекты информационной безопасности;
○ криптография;
○ сетевая безопасность;

○ безопасность личного информационного пространства.

обеспечение условий для профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера).

Задачи изучения курса внеурочной деятельности:

Сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео); создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде; сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.; сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей; сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Место курса внеурочной деятельности в структуре учебного плана

Программа курса внеурочной деятельности «Информационная безопасность» предназначена для реализации на уровне среднего общего образования.

Реализация Программы курса рассчитана на один год обучения, предназначена для использования во внеурочной деятельности, предполагает разные варианты формирования календарно-тематического планирования.

Курс внеурочной деятельности «Информационная безопасность» составлен на основе требований к предметным результатам освоения основной образовательной программы, представленной в федеральном государственном образовательном стандарте основного общего образования, и рассчитан на общую учебную нагрузку в объеме 34 часа (1 ч в неделю в течение одного года).

УМК курса внеурочной деятельности для педагога:

1. Федеральный закон от 29.12.2012 года № 273 – ФЗ «Об образовании в Российской Федерации»;
2. Примерная программа основного общего образования по информатике и информационным технологиям Федерального государственного образовательного стандарта среднего общего образования;
3. Профессиональный стандарт:

3.1. 06.026 «Системный администратор информационно-коммуникационных систем», утв. приказом Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 года N 680 (зарегистрирован Министерством юстиции Российской Федерации 26 октября 2020 года, регистрационный № 60580).
3.2. 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утв. приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449).
3.3. 06.032 «Специалист по безопасности компьютерных систем и сетей», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464), (с изменениями и дополнениями).
3.4. 06.033 «Специалист по защите информации в автоматизированных системах», утв. приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).
3.5. 06.034 «Специалист по технической защите информации», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 года, регистрационный № 44443).
4. Курсы по информационной безопасности (sbersova.ru);
5. Урок Цифры — всероссийский образовательный проект в сфере цифровой экономики (xn--h1adlhdnlo2c.xn--p1ai).
6. Khttps://resh.edu.ru/page/cyber-project.

УМК курса внеурочной деятельности для обучающихся:

1. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие– Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017.
2. Основы информационной безопасности : учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019.
3. Цифровой ликбез — просветительский проект, который поможет повысить цифровую грамотность и узнать больше о кибербезопасности в сети (datalesson.ru);
4. Кибербезопасность для детей и подростков (sberbank.ru).
5. Урок Цифры — всероссийский образовательный проект в сфере цифровой экономики (xn--h1adlhdnlo2c.xn--p1ai).
6. Курсы по информационной безопасности (sbersova.ru).
7. Khttps://resh.edu.ru/page/cyber-project.

Содержание обучения

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации». Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Безопасность информации (15 часов).

Социальная инженерия: распознать и избежать (2 часа).

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете (2 часа).

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Безопасность при использовании платежных карт в Интернете (2 часа).

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Беспроводная технология связи (2 часа).

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Резервное копирование данных (2 часа).

Безопасность личной информации. Создание резервных копий на различных устройствах.

Основы государственной политики в области формирования культуры информационной безопасности (4 часа).

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов (1 час).

Безопасность устройств (12 часов).

Что такое вредоносный код? (2 часа).

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Распространение вредоносного кода (2 часа).

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Методы защиты от вредоносных программ (4 часа).

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Распространение вредоносного кода для мобильных устройств (2 часа).

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. (2 часа).

Безопасность общения (7 часов).

Общение в социальных сетях и мессенджерах (2 часа).

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

С кем безопасно общаться в интернете (1 час).

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Пароли для аккаунтов социальных сетей (1 час).

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты (1 час).

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Настройки конфиденциальности в социальных сетях (1 час).

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Публикация информации в социальных сетях (1 час).

Персональные данные. Публикация личной информации. Фиппинг.

Планируемые результаты освоения программы

Личностные:

Выработать у обучающегося осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;

понимание социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;

сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные:

В результате освоения учебного курса обучающийся сможет идентифицировать собственные проблемы и определять главную проблему; выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; ставить цель деятельности на основе определенной проблемы и существующих возможностей; выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; составлять план решения проблемы (выполнения проекта, проведения исследования); описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса; оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата; работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата; принимать решение в учебной ситуации и нести за него ответственность; выделять явление из общего ряда других явлений; определять обстоятельства, которые предшествовали возникновению связи между

явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений; строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; излагать полученную информацию, интерпретируя ее в контексте решаемой задачи; самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; критически оценивать содержание и форму текста; определять необходимые ключевые поисковые слова и запросы;. строить позитивные отношения в процессе учебной и познавательной деятельности; критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его; договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его. целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.; использовать информацию с учетом этических и правовых норм; создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Обучающийся научится анализировать доменные имена компьютеров и адреса документов в интернете; безопасно использовать средства коммуникации, безопасно вести и применять способы самозащиты при попытке мошенничества, безопасно использовать ресурсы интернета.

Овладеет приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Получит возможность овладеть основами соблюдения норм информационной этики и права; основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Тематическое планирование

№ п/п	Наименование разделов и тем программы	Количество часов	Электронные (цифровые) образовательные ресурсы
1.	**Безопасность информации**.	**15**	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.

1.1.	Основы информационной безопасности. Введение.	1	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.2.	Социальная инженерия: распознать и избежать	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.3.	Ложная информация в Интернете,	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.4.	Безопасность при использовании платежных карт в Интернете	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.5.	Беспроводная технология связи	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.6.	Резервное копирование данных	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.7.	Основы государственной политики в области формирования культуры информационной безопасности	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
1.8.	Выполнение и защита индивидуальных и групповых проектов	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.	**Безопасность устройств**	**12**	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.1.	Что такое вредоносный код?	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.2.	Распространение вредоносного кода	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.3.	Методы защиты от вредоносных программ	4	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.4.	Распространение вредоносного кода для мобильных устройств	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
2.5.	Выполнение и защита индивидуальных и групповых проектов	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
3.	**Безопасность общения**	**7**	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
3.1.	Общение в социальных сетях и мессенджерах	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
3.2.	Публикация информации в социальных сетях	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.

3.3.	Фишинг	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655.
3.4.	Практическая работа	1	

Поурочное планирование

№ п/п	Тема урока	Количество часов	Электронные (цифровые) образовательные ресурсы
1	Основы информационной безопасности. Введение.	1	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
2-3	Социальная инженерия: распознать и избежать	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
4-5	Ложная информация в Интернете,	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
6-7	Безопасность при использовании платежных карт в Интернете	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
8-9	Беспроводная технология связи	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
10-11	Резервное копирование данных	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
12-13	Основы государственной политики в области формирования культуры информационной безопасности	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
14-15	Выполнение и защита индивидуальных и групповых проектов	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
16-17	Что такое вредоносный код?	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
18-19	Распространение вредоносного кода	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.

20-23	Методы защиты от вредоносных программ	4	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
24-25	Распространение вредоносного кода для мобильных устройств	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
26-27	Выполнение и защита индивидуальных и групповых проектов	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
28-29	Общение в социальных сетях и мессенджерах	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
30-31	Публикация информации в социальных сетях	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
32-33	Фишинг	2	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.
34	Практическая работа	1	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti?ysclid=lonb9bf723565521655. Khttps://resh.edu.ru/page/cyber-project.