МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Комитет по образованию Санкт-Петербурга

Администрация Выборгского района Санкт-Петербурга

ГБОУ СОШ №463

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель МО	Зам. директора УВР	Директор школы
_____	_____	_____
Белостоцкая Л.А.	Фёдорова М.Б.	Лунева Г.Ю.
Приказ №60 от «26» мая 2023 г.	Приказ №60 от «26» мая 2023 г.	Приказ №60 от «26» мая 2023 г.

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности

учебного предмета «Цифровая среда »

для обучающихся 11-х классов

Санкт-Петербург
2023

Пояснительная записка

Нормативно правовые документы,
на основе которых разработана данная программа

- Федерального закона от 29.12.12 N273-ОЗ (ред. 13.07.2015) Об образовании в Российской Федерации»;
- Федерального государственного образовательного стандарта основного общего образования (Утвержден приказом Минобрнауки России от 17.12.2010 г. №1897);
- Приказа Министерства образования и науки Российской федерации от 17.12.2010 № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования»;
- Приказа Министерства образования и науки Российской Федерациит от 31.12.2015 № 1577 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17.12.2010 г. №1577»;

Курс ориентирован на проведение уроков по информационной безопасности школьников и безопасному поведению в сети Интернет и отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах.

Задачи курса по информационной безопасности детей:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей,

как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

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. Курс рассчитан на

35 часов обучения, поддержан электронными ресурсами по каждой теме, ориентирован на работу обучающихся с документами в области законодательства Российской Федерации в сфере информационной безопасности.

Учебно - тематическое планирование разработано на основе учебного пособия по курсу для 10-11 классов. Пособие включает в себя практические работы по уровням «знать» и «применять», а также набор проектных заданий для выполнения в группах учащихся на компьютерах. К пособию для каждой темы на сайте издательства размещено электронное приложение с набором ссылок на материалы (документы, федеральные законы и ссылки к проектным работам) для использования на занятиях: http://lbz.ru/metodist/authors/ib/10-11.php, возможно в демонстрационном режиме для использования педагогом при объяснении материала и организации обсуждений и дискуссий на занятиях.

Учебно-тематический план включает обязательный для изучения курса теоретический раздел 1 (Модули 1-4).

В рамках изучения курса обучающимся предложен дополнительный практический раздел 2 (Модуль 5), где представлены проектные работы, которые включают набор учебных практических работ и изучение открытого онлайн курса НОУ Интуит «Основы информационной безопасности» с прохождением тестирования по итогам изучения курса. Раздел 2 курса учащиеся осваивают в компьютерном классе или в дистанционной форме.

Модуль		*Всего часов*
Модуль 1. Правовые основы информационной безопасности	**Глава 1 Понятия юридической ответственности за правонарушения в области информационной**	*2*
1.1 .Понятия юридической ответственности за правонарушения в области информационной безопасности	1. Основные документы в области информационной безопасности Российской Федерации 2. Информация как объект правовых отношений	**2**
Модуль 2 Законодательство Российской Федерации о гражданско-	Подготовка презентации по теме в группах учащихся	**4**
правовой ответственности в сфере инфобезопасности	**Глава 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)**	
2.1 Законодательство Российской Федерации о гражданско-правовой ответственности	1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности 2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности	1

2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)	1. Ответственность за проступок в области присвоение авторства (плагиат) 2. Ответственность за проступок за оскорбления, в том числе в социальных сетях	1
Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности	**Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации)**	3
3.1. Понятие административной ответственности	1. Административное правонарушение. Основные понятия административного правонарушения 2. Особенности административной ответственности несовершеннолетних.	1
3.2 Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение 2. Ответственность за проступок -за оскорбления, в том числе в социальных сетях. 3. Ответственность за проступок - ложный вызов экстренных служб 4. Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ 5. Ответственность за проступок- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные) 6. Ответственность за проступок - нарушение правил защиты информации 7. Ответственность за проступок - представление ложных сведений для	2

	получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство 8. Ответственность за проступок -за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт. 9. Ответственность за проступок - нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	
Модуль 4 Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности	**Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)**	**8**
4.1 .Понятие уголовной ответственности	1. Уголовный кодекс Российской Федерации. 2. Виды наказаний в области уголовной ответственности	**2**
4.2 Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	1. Ответственность за преступления в области компьютерной информации и применения компьютеров. 2. Ответственность за преступления в области присвоения авторства (плагиат); авторских прав на лицензионное программное обеспечение. 3. Ответственность за преступления в области мошенничества (обмана). 4. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений. 5. Ответственность за преступления - за заведомо ложное сообщение о теракте. 6. Ответственность за преступления - за мошенничество в сфере компьютерной информации	**6**
Всего по разделу	**Модули 1-4**	**34**

Список источников информации:

Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/

2. Цветкова М. С, Якушина Е. В. Информационная безопасность.

Правила безопасного Интернета. 2-4 классы: учебное пособие. — М.: БИНОМ.

Лаборатория знаний, 2020. —112 с.
3. Цветкова М. С, Якушина Е. В. Информационная безопасность. Безопасное поведение в сети Интернет. 5-6 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний,2020. — 96 с.
4. Цветкова М. С, Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7-9 классы: учебное пособие. —М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
5. Цветкова М. С, Голубчиков СВ., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10-11классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
6. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/authors/ib/
7. «Безопасный Билайн», компания Билайн, URL: http://Moskva.beeline.ru/customers/help/safe-beeline/
8. «Безопасность», компания МТС, URL: http://www.safety.mts.ru/ru/
9. «Безопасное общение», компания Мегафон, URL: http://moscow.megafon.ru/bezopasnoeobschenie/
10. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/stopfraud/brochure.pdf
11. Открытый онлайн-курс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: https://academv.vandex.ru/events/online-courses/internet security/

Требования к результатам освоения программы:

Деятельность образовательного учреждения в обучении по направлению «Информационная безопасность» должна быть направлена на достижение обучающимися следующих **личностных результатов:**
- готовность и способность к самостоятельной, творческой и ответственной деятельности;
- навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности; готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни;
- сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
- эстетическое отношение к миру, включая эстетику научного и технического творчества;
- осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов;
- отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.

Метапредметными результатами освоения программы по направлению «Информационная безопасность» являются:
- умение самостоятельно определять цели и задачи деятельности; составлять планы; контролировать и корректировать их выполнение;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности;
- владение навыками познавательной, учебно-исследовательской и проектной деятельности, способность и готовность к самостоятельному поиску методов решения практических задач;
- умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию;
- умение использовать средства информационных и коммуникационных технологий (далее - ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, информационной безопасности;

Предметными результатами освоения программы по направлению «Информационная безопасность» являются:
- развитие инженерного мышления;
- навыки работы с реальными программно-аппаратными комплексами;
- навыки оценивания уровня безопасности компьютерных систем;
- навыки обеспечения информационной безопасности личного пространства