АДМИНИСТРАЦИЯ КИРОВСКОГО РАЙОНА САНКТ - ПЕТЕРБУРГА

Государственное бюджетное общеобразовательное учреждение

лицей №378 Кировского района Санкт-Петербурга

РАССМОТРЕНА	СОГЛАСОВАНО	УТВЕРЖДЕНО
на МО учителей информатики и труда (технологии)	На заседании Педагогического совета ГБОУ лицея № 378 Кировского района Санкт-Петербурга	Директором ГБОУ лицея № 378 Кировского района Санкт-Петербурга
Ключева Е.Е. Протокол № 1 от «25» 08 2026 г.	Протокол № 13 от 27.08.2026 г.	Ковалюк С.Ю. Приказ № 488 от 27.08. 2026 г.

Ковалюк Светлана Юрьевна

Подписано цифровой подписью: Ковалюк Светлана Юрьевна
Дата: 2026.08.31 13:13:30 +03'00'

РАБОЧАЯ ПРОГРАММА

Курса внеурочной деятельности

«Школа информационной безопасности»

для обучающихся 7-8-х классов

Санкт-Петербург 2026

Пояснительная записка

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

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

При изучении информационной и кибербезопасности выделяются следующие:

обеспечение различных сфер экономики качественными информационными технологиями;

обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов. Киберугрозы существуют везде, где применяются информационные технологии.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальным реализация программы внеурочной деятельности

«Информационная безопасность».

Задача курса «Информационная безопасность» - совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями. Цель изучения курса

«Информационная безопасность» - дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности

и умения применять правила кибербезопасности во всех сферах деятельности.

Воспитательная цель курса – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

Цель программы – создание условий для формирования у учащихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности учащегося в сети «Интернет».

Для достижения поставленной цели решаются следующие задачи:

- Формирование у учащихся цифровой и информационной культуры;
- Воспитание у учащихся нравственности и культуры взаимоотношения с людьми на основе общечеловеческих ценностей в сети «Интернет»;
- Утверждение в сознании и чувствах учащихся правильных моделей поведения, ценностей, взглядов и убеждений для успешной жизнедеятельности учащегося в сети «Интернет»;
- Углубление знаний учебных дисциплин «Информатика», «ОБЖ» и «Обществознание» в процессе обучения в рамках программы;
- Интеллектуальное развитие учащихся, формирование творческих и прикладных качеств мышления;
- Развитие интереса к различным сферам информационных технологий;
- Совершенствование навыков самообразования, всестороннего развития и социализации;
- Обучение поиску и отборуинформации, еѐ интерпретации и применимости;
- Развитие логического мышления, умений обобщения и конкретизации, анализа и синтеза;
- Воспитание умения трудиться, самостоятельности, ответственности и творческого отношения к учѐбе;

Обучающие:

- Сформировать систему знаний в сфере обществознания, информационных технологий и основ безопасности жизнедеятельности;
- Обучить элементам системного мышления использовать инструменты активизации мышления;
- Отработка навыков и умений для безопасного и полезного использования информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и

грамотное изложение, а также восприятия и усвоения информации из сети

- «Интернет».

Развивающие:

- Развить интеллектуальные и социальные способности обучающихся;
- Развить навыки сетевого общения и коммуникации в сети «Интернет», поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов и осуществления сетевых покупок;
- Развить деловые и гражданские качества, такие как самостоятельность, ответственность, активность и аккуратность;
- Сформировать потребности в самопознании и саморазвитии.

Воспитательные:

- Воспитать культуру общения и поведения в сетевом пространстве;
- Воспитать целеустремлённость личности;
- Воспитать толерантную и культурную личность;
- Воспитать правильный образ гражданина.

Общая характеристика курса

Курс «Информационная безопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

Описание места учебного предмета в учебном плане.

На изучение информационной безопасности. Кибербезопасности отводится 1 час в неделю с 7 по 8 класс (34 часа за год в каждом классе, всего 68 часов).

Содержание учебного предмета

7 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

- Как работают мобильные устройства. Угрозы для мобильных устройств.
- Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).
- Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).
- Кто обеспечивает защиту киберпространства.
- Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

Модуль 2. Техника безопасности и экология (5 часов).

- Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП Компьютер и мобильные (сотовые) устройства в правилах безопасности.
- Компьютеры и мобильные устройства в экстремальных условиях. Везде ли есть Интернет. ТБ при работе с мобильными устройствами. Первая помощь при проблемах в интернете (службы помощи).
- Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Модуль 3. Проблемы Интернет-зависимости (2 часа).

- Виды Интернет-зависимости.Компьютер и зрение.

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

- Вирусы и антивирусы (8 часов).
- Вирусы и антивирусы.
- Как распространяются вирусы. Источники и причины заражения.
- Скорая компьютерная помощь. Признаки заражения компьютера. Что такое антивирусная защита. Как лечить компьютер.
- Защита мобильных устройств.
- Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.
- Защита файлов. Что такое право доступа.
- Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в

сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).

- Опасности мобильной связи. Предложенияпо установке вредоносных приложений.
- Мошеннические СМС.
- Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (10 часов).

- Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.
- «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам. Анонимность в сети.
- Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.).
- Различия этикета в разных странах.
- Как появился этикет, что это такое. Общие правила сетевого этикета.
- Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).
- Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение.
- Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и ихопасность, угрозы и оскорбления – чем это может закончиться.
- Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (2 часа).

- Собственность в Интернете. Авторское право. Интеллектуальная собственность.
- Платная ибесплатная информация.
- Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

8 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

- Информационная безопасность
- Защита персональных данных, почему она нужна. Категории персональных данных.

- Биометрические персональные данные.
- Источники данных в Интернете: почта, сервисы обмена файлами и др.
- Хранение данных вИнтернете.
- Возможности и проблемы социальных сетей.
- Безопасный профиль в социальных сетях. Составление сети контактов.

Модуль 2. Техника безопасности и экология (2 часа).

- Комплекс упражнений при работе за компьютером.
- Воздействиена зрение ЭЛТ, жидкокристаллических, светодиодных, монохромныхмониторов.

Модуль 3. Проблемы Интернет-зависимости (3 часа).

- Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.)и как польза превращается во вред.
- Киберкультура (массовая культура в сети) и личность.
- Психологическое воздействие информации на человека. Управление личностью через сеть.

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

- Вирусы и антивирусы (16 часов).
- Защита файлов. Права пользователей. Защита при загрузке и выключении компьютера.Безопасность при скачивании файлов.
- Безопасность при просмотре фильмов онлайн.
- Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.
- Защита программ и данных с помощью паролей, программных и электронных ключей,серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.
- Методы защиты фото и видеоматериалов от копирования в сети. Защита от копирования контента сайта.
- Как развивались вирусы.
- Могут ли вирусы воздействовать на аппаратуру ПК. Как вирусы воздействуют на файлы.
- Проверка на наличие вирусов. Сканеры и др. Может ли вирус воздействовать на рабочий стол.Источники заражения ПК.
- Антивирусное ПО, виды и назначение.

- Методы защиты от вирусов. Как распознаются вирусы.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (4 часа).

- Утечка и обнародование личных данных.
- Подбор и перехват паролей. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг).
- Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для
- «инвестирования» денег. Выигрыш в лотерею.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

- Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.

Модуль 7. Правовые аспекты защиты киберпространства (3 часа).

- Защита прав потребителей при использовании услуг Интернет.Защита прав потребителей услуг провайдера.
- Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

Планируемые результаты изучения курса

Предметные:

- Сформированы знанияо безопасном поведении
- при работе с компьютернымипрограммами, информацией в сети интернет;
- Сформированы умения соблюдать нормы информационной этики;
- Сформированы умения безопасно работать с информацией, анализировать и обобщатьполученную информацию.

Метапредметные:

- Развиваются компьютерная грамотность и информационная культура личности виспользовании информационных и коммуникационных технологий;
- Развиваются умения анализировать и систематизировать имеющуюся информацию;
- Развиваются познавательная и творческая активность в безопасном использованииинформационных и коммуникационных технологий.

Личностные:

- Вырабатывается сознательное и бережное
- отношение к вопросам собственной информационной безопасности;
- Формируются и развиваются нравственные, этические, патриотические качестваличности;
- Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Тематическое планирование

№ п/п	Наименование модулей	Кол-во часов		Воспитательный компонент
		7 класс	8 класс	
1	Общие сведения о безопасности ПК и Интернета	5	5	Гражданское воспитание; Патриотическое воспитание; Духовно-нравственное воспитание; адаптации обучающегося к изменяющимся условиям социальной и природной среды.
2	Техника безопасности и экология.	5	2	Ценности научного познания; формирование культуры здоровья; трудовое воспитание; экологическое воспитание.
3	Проблемы Интернет-зависимости	2	3	Гражданское воспитание; Патриотическое воспитание; Духовно-нравственное воспитание; адаптации обучающегося к изменяющимся условиям социальной и природной среды; ценности научного познания; формирование культуры здоровья; трудовое воспитание; экологическое воспитание.
4	Методы обеспечения безопасности ПК и Интернета.Вирусы и антивирусы	8	16	Адаптации обучающегося к изменяющимся условиям социальной и природной среды; ценности научного познания; формирование культуры здоровья; трудовое воспитание; экологическое воспитание.
5	Мошеннические действия в Интернете. Киберпреступления	2	4	Гражданское воспитание; Патриотическое воспитание; Духовно-нравственное воспитание; адаптации обучающегося к изменяющимся условиям социальной и природной среды; ценности научного познания; формирование культуры здоровья.

6	Сетевой этикет. Психология и сеть	10	1	Гражданское воспитание; Патриотическое воспитание; Духовно-нравственное воспитание; адаптации обучающегося к изменяющимся условиям социальной и природной среды**;** ценности научного познания; формирование культуры здоровья; трудовое воспитание; экологическое воспитание.
7	Правовые аспекты защиты киберпространства	2	3	Гражданское воспитание; Патриотическое воспитание.
	Всего часов:	**34**	**34**	

7 класс

№ урока	Дата	Тема	Кол-во часов
		Общие сведения о безопасности ПК и Интернета	**5**
1		Как работают мобильные устройства. Угрозы для мобильных устройств.	
2		Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).	
3		Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).	
4		Кто обеспечивает защиту киберпространства.	
5		Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.	
		Техника безопасности и экология.	**5**
6		Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	
7		Компьютеры и мобильные устройства в экстремальных условиях.	
8		Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	
9		Первая помощь при проблемах в интернете (службы помощи).	
10		Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	
		Проблемы Интернет-зависимости.	**2**
11		Виды Интернет-зависимости.	
12		Компьютер и зрение.	
		Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**8**
13		Как распространяются вирусы.	
14		Источники и причины заражения.	
15		Скорая компьютерная помощь. Признаки заражения компьютера.	
16		Что такое антивирусная защита. Как лечить компьютер.	
17		Защита мобильных устройств.	
18		Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	
19		Защита файлов. Что такое право доступа.	
20		Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	
		Мошеннические действия в Интернете. Киберпреступления.	**2**
21		Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	
22		Прослушивание разговоров. Определение местоположения телефона.	
		Сетевой этикет. Психология и сеть.	**10**
23		Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	
24		«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	
25		Анонимность в сети.	

26		Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	
27		Как появился нетикет, что это такое. Общие правила сетевого этикета.	
28		Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	
29		Этика дискуссий. Взаимное уважение при интернет-общении.	
30		Этикет и безопасность. Эмоции в сети, их выражение.	
31		Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	
32		Если вы стали жертвой компьютерной агрессии: службы помощи.	
		Правовые аспекты защиты киберпространства.	**2**
33		Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	
34		Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	

8 класс

№ урока	Дата	Тема	Кол-во часов
		Общие сведения о безопасности ПК и Интернета	**5**
1		Информационная безопасность	
2		Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.	
3		Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете.	
4		Возможности и проблемы социальных сетей.	
5		Безопасный профиль в социальных сетях. Составление сети контактов.	
		Техника безопасности и экология.	**2**
6		Комплекс упражнений при работе за компьютером.	
7		Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.	
		Проблемы Интернет-зависимости.	**3**
8		Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.	
9		Киберкультура (массовая культура в сети) и личность.	
10		Психологическое воздействие информации на человека. Управление личностью через сеть.	
		Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**16**
11		Защита файлов. Права пользователей.	
12		Защита при загрузке и выключении компьютера.	
13		Безопасность при скачивании файлов.	
14		Безопасность при просмотре фильмов онлайн.	

15		Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.	
16		Защита программ и данных с помощью паролей, программных и	
		электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	
17		Методы защиты фото и видеоматериалов от копирования в сети.	
18		Защита от копирования контента сайта.	
19		Как развивались вирусы.	
20		Могут ли вирусы воздействовать на аппаратуру ПК.	
21		Как вирусы воздействуют на файлы.	
22		Проверка на наличие вирусов. Сканеры и др.	
23		Может ли вирус воздействовать на рабочий стол.	
24		Источники заражения ПК.	
25		Антивирусное ПО, виды и назначение.	
26		Методы защиты от вирусов. Как распознаются вирусы.	
		Мошеннические действия в Интернете. Киберпреступления.	**4**
27		Утечка и обнародование личных данных.	
28		Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	
29		Виды мошенничества в Интернете. Фишинг (фарминг).	
30		Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	
		Сетевой этикет. Психология и сеть.	**1**
31		Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	
		Правовые аспекты защиты киберпространства.	**3**
32		Защита прав потребителей при использовании услуг Интернет.	
33		Защита прав потребителей услуг провайдера.	
34		Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	

Учебно-методическое и материально-технического обеспечения образовательного процесса

1. Персональный компьютер (ОС Winsows).
2. Интерактивная доска.

Методические материалы

1. Методическое пособие для учителя к учебникам М. С. Цветковой
2. Портал Международного квеста по цифровой грамотности