Муниципальное бюджетное общеобразовательное учреждение
Павлоградского муниципального района Омской области
«Павлоградская гимназия им. В.М. Тытаря»

ПРИНЯТО:	СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Заседание педагогического совета Протокол № 1 от 29 августа 2024 г.	Заместитель директора по ВР _____Губаренко О. И.	Директор МБОУ «Павлоградская гимназия им. В.М. Тытаря» _____/Попруга В. И./ «29» августа 2024 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 59089960D8ADE5A7334B0E9A178636DE
Владелец: Попруга Виталий Иванович
Действителен: с 14.02.2023 до 09.05.2024

Рабочая программа дополнительного образования

«Информационная безопасность»

Центр образования цифрового и гуманитарного профилей «Точка роста»

Направление: **техническое**

Возраст обучающихся: 7-17 лет

Срок реализации: 2024-2025 учебный год

Количество часов: 157

Составитель:

ФИО: Драновская Евгения Анатольевна

Педагог дополнительного образования

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Обучающие:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Воспитывающие:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Направленность программы – техническая.

Программа разработана с учётом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организациям обучения в общеобразовательных учреждениях» и «Санитарно-эпидемиологических требований к устройству, содержанию и организации режима работы общеразвивающих организаций дополнительного образования детей».

Актуальность дополнительной общеразвивающей программы «Информационная безопасность» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Реализация программы позволяет создать условия для развития и информационной защиты детей.

Возраст детей, участвующих в реализации программы.

Программа рассчитана для обучающихся от 7 до 17 лет. Принимаются все желающие, достигшие возраста 7 лет. Приём детей осуществляется на основании письменного заявления родителей (или законных представителей).

Особенности состава обучающихся: неоднородный (смешанный); постоянный.

Наполняемость группы: не менее 15 человек.

Уровень программы - стартовый, предполагает использование и реализацию общедоступных и универсальных форм организации материала, минимальную сложность предлагаемого для освоения содержания программы.

Организационно-педагогические условия реализации программы.

Периодичность в неделю	Продолжительность занятия	Кол-во часов в неделю	Кол-во часов в год
2 раза	40 минут	4,5 часа	157

Форма обучения: очная.

Форма проведения занятий: аудиторная, внеаудиторная.

Расписание занятий составлено с учетом школьного расписания в образовательных учреждениях и свободного времени обучающихся. Продолжительность по времени занятий и перемен - в соответствии с Уставом учреждения.

Форма организации занятий: групповая, индивидуально - групповая, коллективная.

Методы освоения программного материала:

В ходе реализации программы возможно использование различных **методов и приёмов** организации занятий:

- практический (опыты, упражнения);
- наглядный (иллюстрация, демонстрация, наблюдения обучающихся);
- словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут); работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование);
- идеометод (просмотр, обучение, упражнение, контроль).

Планируемые результаты.

Усвоение данной программы обеспечивает достижение следующих результатов:

Год обучения	Результаты освоения программы		
	Личностные	***Метапредметные***	***Предметные***
2022-2023	1. Вырабатывается сознательное и бережное отношение к вопросам собственной и информационной безопасности; 2. Формируются и развиваются нравственные, этические, патриотические качества личности; 3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.	1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий; 2. Развиваются умения анализировать и систематизировать имеющуюся информацию; 3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.	1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информации в сети интернет; 2. Сформированы умения соблюдать нормы информационной этики; 3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Система оценки результатов освоения программы- педагогическое , тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнение обучающимися диагностических заданий, участие в мероприятиях, защиты проектов, решение задач поискового характера, активности обучающихся на занятиях и т.п. **Материально-техническое обеспечение** реализации дополнительной общеразвивающей программы «Информационная безопасность» включают следующих перечень необходимого оборудования:

1. Кабинет «Точка роста»
2. Компьютер для педагога (ноутбук)
3. Ноутбуки для обучающихся
4. Доступ к сети Интернет

Паспорт программы

Название программы:«Информационная безопасность»

Платформа:Центр образования цифрового и гуманитарного профилей «Точка роста»

Направление:организация и технология защитыинформации, (техническое, социальное)

Вид программы: общеразвивающая

Уровень сложности: базовый

Форма реализации: очная

Возраст обучающихся: 7-17 лет

Срок реализации программы: 1 год (40 учебных недель)

Количество часов: 157

Кол-во часов на учебный год / в неделю: 2

Ожидаемые результаты освоения программы:

сформировать у обучающихся с учетом возрастных особенностейличностные результаты, которые позволят им грамотно ориентироваться винформационном мире с учетом имеющихся в нем угроз, понимать и выполнять правилаинформационной безопасности и отражать личностные качества в информационной деятельности.

УЧЕБНЫЙ ПЛАН

№ п/п	Тема	Всего часов	Теория	Практика	Формы контроля
1.	**Информация, компьютер и Интернет.**	**20**	**8**	**12**	**тестирование**
1.1.	Компьютер. История создания	5	2	3	Интерактивное занятие
1.2.	Интернет как средство поиска информации	5	2	3	Рефлексивная беседа
1.3.	Полезные и вредные страницы Интернета	5	2	3	Интерактивное занятие
1.4.	Ложные ссылки. Реклама	5	2	3	Интерактивное занятие
2.	**Безопасность общения**	**34**	**15**	**19**	**Творческая работа**
2.1	Общение в социальных сетях и мессенджерах	9	3	4	Тест
2.2.	С кем безопасно общаться в интернете	9	3	5	Интерактивное занятие
2.3	Пароли для аккаунтов социальных сетей	9	4	4	Рефлексивная беседа
2.4.	Безопасный вход в аккаунты	9	3	4	Викторина
3.	**Мир виртуальный и реальный. Интернет зависимость.**	**20**	**8**	**12**	**Творческая работа**
3.1.	Настройки конфиденциальности в социальных сетях.	4,5	2	2,5	Тест
3.2.	Публикация информации в социальных сетях	4,5	2	1	Викторина
3.3.	Кибербуллинг	5	2	2,5	Тест
3.4.	Фишинг	5	2	1	Тест
4.	**Методы безопасной работы в Интернете**	**23**	**10**	**13**	**Творческая работа**
4.1	Правила хранения паролей.	6	2,5	2,5	Викторина
4.2.	Онлайн генераторы паролей	6	2,5	1,5	Тест
4.3.	Виды аутентификации	6	2,5	1,5	Викторина
4.4.	Настройки безопасности аккаунта	6	2,5	2,5	Тест
5.	**Потребительские опасности в**	**20**	**6**	**14**	**Творческая работа**

	Интернете				
5.1.	Электронная торговля - ее опасности.	4,5	2	3,5	Тест
5.2.	Виды интернет - мошенничества	4,5	2	3,5	Викторина
5.3.	Сколько стоят ошибки в интернете.	5	2	3,5	Рефлексивная беседа
5.4.	Плагиат	5	2	3,5	Интерактивное занятие
6.	**Основные правила поведения сетевого взаимодействия**	**20**	**9**	**11**	**Творческая работа**
6.1	Как вести себя в гостях у «сетевых» друзей	4,5	1,5	2,5	Рефлексивная беседа
6.2.	Виды этикета	4,5	3	2,5	Творческая работа
6.3.	Общие правила сетевого этикета	5	3	3	Интерактивное занятие
6.4.	Безопасная работа в сети в процессе сетевой коммуникации	5	1,5	2,5	Викторина
7.	**Государственная политика в области в области защиты информации**	**20**	**8**	**12**	**Тестирование**
7.1.	Как государство защищает киберпространство	4,5	2	3	Интерактивное занятие
7.2.	Авторское право	4,5	2	3	Рефлексивная беседа
7.3.	Интеллектуальная собственность	5	2	3	Интерактивное занятие
7.4.	Как расследуются преступления в сети	5	2	3	Тест
8.	Итого	157	64	93	

Календарный учебный график

Дата	Тема	Всего часов	Теория	Практика	Формы контроля
Тема 1. Информация, компьютер и Интернет.					
	Компьютер. История создания	5	2	3	Интерактивное занятие
	Интернет как средство писка информации	5	2	3	Рефлексивная беседа
	Полезные и вредные страницы Интернета	5	2	3	Интерактивное занятие
	Ложные ссылки. Реклама	5	2	3	Интерактивное
Тема 2. Безопасность общения					
	Общение в социальных сетях и	9	3	4	Тест
	С кем безопасно общаться в интернете	9	3	5	Интерактивное занятие
	Пароли для аккаунтов социальных сетей	9	4	4	Рефлексивная беседа
	Безопасный вход в аккаунты	9	3	4	Викторина
Тема 3. Мир виртуальный и реальный. Интернет зависимость.					
	Настройки конфиденциальности в социальных сетях.	4,5	2	2,5	Тест
	Публикация информации в социальных сетях	4,5	2	1	Викторина
	Кибербуллинг	5	2	2,5	Тест
	Фишинг	5	2	1	Тест
Тема 4. Методы безопасной работы в Интернете.					
	Правила хранения паролей.	6	2,5	2,5	Викторина
	Онлайн генераторы паролей	6	2,5	1,5	Тест
	Виды аутентификации	6	2,5	1,5	Викторина
	Настройки безопасности аккаунта	6	2,5	2,5	Тест
Тема 5. Потребительские опасности в Интернете.					
	Электронная торговля - ее опасности.	4,5	2	3,5	Тест
	Виды интернет - мошенничества	4,5	2	3,5	Викторина
	Сколько стоят ошибки в интернете.	5	2	3,5	Рефлексивная беседа
	Плагиат	5	2	3,5	Интерактивное занятие
Тема 6. Основные правила поведения сетевого взаимодействия.					
	Как вести себя в гостях у «сетевых» друзей	4,5	1,5	2,5	Рефлексивная беседа
	Виды этикета	4,5	3	2,5	Творческая работа

	Общие правила сетевого этикета	5	3	3	Интерактивное занятие
	Безопасная работа в сети в процессе сетевой коммуникации	5	1,5	2,5	Викторина
Тема 7. Государственная политика в области в области защиты информации					
	Как государство защищает киберпространство	4,5	2	3	Интерактивное занятие
	Авторское право	4,5	2	3	Рефлексивная беседа
	Интеллектуальная собственность	5	2	3	Интерактивное занятие
	Как расследуются преступления в сети	5	2	3	Тест
8.	Итого	157	64	93	

ПЛАНИРУЕМЫЕ РАЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

В результате освоения данной программы по окончании учебного года обучающиеся:

Будут знать: об истории появления компьютера и Интернета. Правила работы с компьютером. Научиться соблюдать правила работы с файлами. Уметь отличать безопасные сайты и ссылки от вредоносных. Знать технические и программные возможности мобильных устройств. Преимущества мобильной связи и их опасность. Понимать пользу и опасности виртуального общения, социальных сетей. Основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами. Виды общения в Интернете. Правила безопасной работы при интернет-общении. Уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении. Основные понятия о компьютерных вирусах и контент-фильтрах. Принципы работы интернет - магазинов, понятие «электронные деньги». Дозировано использовать личную информацию в сети интернет. Правила сетевого этикета. Политику государства в области защиты информации.

Будут уметь: Правильно работать за компьютером. Пользоваться браузером для поиска полезной информации. Внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра. Выполнять основные действия с файлами. Копировать файлы, проверять файлы на вирусы. Уметь работать с информацией и электронной почтой. Владеть основными приемами поиска информации в сети Интернет. Соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе. Уметь применять программу. Отличать вредные игры от полезных. Использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры. Различать (распознавать) мошеннические действия. Корректно общаться в сети Интернет. Защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. - 20 ч.

Информация, компьютер и Интернет.

Теория: Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для урока. Интернет - средство для поиска полезной **информации**. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. **Полезные и вредные страницы Интернета**. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе – Цифровой образовательный контент (Сферум), IP-телефония. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.).

Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам**.** Что такое электронная почта. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. **Категории персональных данных**. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составление сети контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты **кибербезопасности**. Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасный серфинг. Безопасные ресурсы для поиска. Безопасность платежных систем. Безопасность геоинформационных систем. Безопасность систем бронирования билетов. Безопасность при удаленном доступе к ресурсам компьютера. Хакерские атаки. Виды хакерских атак. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств. Кибершпионаж.

Практика:

Практическая работа № 1. Поиск информации в сети Интернет. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.). Практическая работа № 2. Общение с использованием видеосвязи на примере цифровой образовательной платформы «Сферум».

Практическая работа № 3. Создание электронной почты

Практическая работа № 4. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

Практическая работа № 5 «Безопасность при удаленном доступе к ресурсам компьютера».

Тема № 2. 20-ч.

Безопасность общения. 34 часа.

Теория: Вводное занятие. Общение в социальных сетях и мессенжерах. С кем безопасно общаться в интернете. Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты.

Практика:

Практическая работа № 6. Регистрация и работа в социальных сетях.

Практическая работа № 7. Профиль пользователя. Анонимные социальные сети.

Практическая работа № 8. Создание сложных паролей. Правила хранения паролей.

Тема № 3. 20ч.

Мир виртуальный и реальный. Интернет зависимость.

Теория: Что такое Интернет-сообщество. Как не превратить своюжизнь в виртуальную? **Социальные сети**. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Если слишком долго находиться в Интернете: что такое интернет-зависимость? Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы **интернет - зависимости** (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения). Признаки игровой зависимости. Виртуальная личность - что это такое. Сайты знакомств. **Незнакомцы в Интернете**. Управление личностью через сеть. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. **Деструктивная информация** в Интернете - как ее избежать.

Практика:

Практическая работа № 9 Создание сообщества класса в детских социальных сетях

Практическая работа. № 10 «Создание видеоролика на тему «Проблемы Интернет - зависимости».

Тема № 4. 23ч.

Методы безопасной работы в Интернете.

Теория: Ищите в Интернете только то, что вам требуется. Как защититься от **вредного контента**. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает компьютер? **Вирусы** человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое **антивирусная защита**. Как лечить компьютер. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов.

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. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. **Меры личной безопасности при сетевом общении.** Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.

Практика:

Практическая работа № 11. Исследовательская работа «В поисках вируса» (выявление признаков заражения вирусом).

Практическая работа № 12 «Установка антивирусной программы».

Тема № 5. 20 ч.

Потребительские опасности в Интернете

Теория: Интернет и экономика - польза и опасность. Кто и как может навредить в Интернете. Электронная торговля - ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в **лотерею.** Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете. Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. **Мошенничество** при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Компьютерное пиратство. Плагиат. Кибер наемники и кибер детективы. Оценка ущерба от кибер преступлений.

Практика:

Прохождение интерактивного курса.

«Мошеннические действия в Интернете. Кибер преступления».

Практическая работа № 13. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

Тема № 6. 20 ч.

Основные правила поведения сетевого взаимодействия.

Теория: Что такое интернет-этикет. Как вести себя в гостях у«сетевых» друзей. Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. **Этика дискуссий**. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе - чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Практика:

Практическая работа № 14 «Пишу письмо другу»

Практическая работа № 15. «Выпуск видеоролика».

Тема № 7. - 20 ч.

Государственная политика в области защиты информации.

Теория: Как государство защищает киберпространство. **Войны нашего времени**. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства. **Собственность в Интернете**. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернет-мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.

Практика:

Практическая работа № 16 «Создание презентации «Информационная война. Информационное воздействие»

Практическая работа № 17 «Создание презентации «Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО».

СИСТЕМА ОЦЕНКИ ДОСТИЖЕНИЯ ПЛАНИРЕУМЫХ РЕЗУЛЬТАТОВ.

Согласно Стандарту, система оценки достижения планируемых результатов освоения курса занятий по внеурочной деятельности «Информационная безопасность» состоит из двух основных компонентов:

1. Оценка предметных результатов, которая предусматривает выявление уровня достижения обучающимися планируемых результатов по данному направлению деятельности с учётом предметных знаний, действий с предметным содержанием. По окончании изучения каждой темы проводится обследование уровня усвоения знаний умений и навыков, полученных на занятии в разнообразной форме: интерактивное занятие, викторины, творческая работа и т.д.

2. Оценка метапредметных результатов как сформированности регулятивных, коммуникативных и познавательных универсальных действий может быть отслежена в результате следующих действий:

- Выполнение специально сконструированных диагностических задач, направленных на оценку уровня сформированности конкретного вида универсальных учебных действий;
- Выполнение учебных и учебно-практических задач средствами учебных предметов;
- Выполнение комплексных заданий на межпредметной основе
- Работа по оцениванию метапредметных результатов проводится в виде промежуточной и итоговой аттестации обучающихся.

Низкий уровень: удовлетворительное владение теоретической информацией по темам курса, умение пользоваться литературой при подготовке сообщений, элементарные представления об исследовательской деятельности, пассивное участие в семинарах.

Средний уровень: достаточно хорошее владение теоретической информацией по курсу, умение систематизировать и подбирать необходимую литературу, проводить исследования и опросы, иметь представление о учебно-исследовательской деятельности, участие в конкурсах, организации и проведении мероприятий.

Высокий уровень: свободное владение теоретической информацией по курсу, умение анализировать литературные источники и данные исследований и опросов, выявлять причины, подбирать методы исследования, проводить учебно-исследовательскую деятельность, активно принимать участие в мероприятиях, конкурсах, применять полученную информацию на практике.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые документы:

1. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ;

2. Федеральный закон Российской Федерации от 21 июля 2011 г. №2252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;

3. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изм., внесенными Федеральными законами от 04.06.2014 г. № 145 -ФЗ, от 06.04.2015 г. № 68-ФЗ)

5. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 г. № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (Зарегистрировано в Минюсте России 03.03.2011 г. № 19993), (в ред. Изменений № 1, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 29.06.2011 г. № 85, Изменений № 2, утв. Постановлением Главного государственного санитарного врача РоссийскойФедерации от 25.12.2013 г. № 72, Изменений № 3, утв. Постановлением Главного государственного санитарного врача РФ от 24.11.2015 г. № 81)

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2- е издание: Издательство: ДМК-Пресс., 2017, 434 с.

2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с.

3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.

4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.

5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ "Интуит", 2016,571 с.

6. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учрежд. высш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с.

7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.

8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.

9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.