

**Муниципальное образовательное учреждение дополнительного образования
«Тихвинский центр детского творчества»**

УТВЕРЖДЕНА
распоряжением директора
МОУ «Шугозерская СОШ»
от 18.10.2019 № 177

ПРИНЯТА
педагогическим советом
МОУ «Шугозерская СОШ»
(протокол от 15.10.2019 № 2)

УТВЕРЖДЕНА
распоряжением директора
МОУДО «ТЦДТ»
от 15.10.2019 № 01-09/117а

ПРИНЯТА
педагогическим советом
МОУДО «ТЦДТ»
(протокол от 15.10.2019 № 4)

**Дополнительная общеразвивающая программа
«Безопасность в сети Интернет»**

Возраст учащихся: 7- 17 лет
Срок реализации программы: 1
год
Автор - составитель:
Иванова Ирина Борисовна,
педагог дополнительного
образования

Тихвин
2019

Лист корректировки программы

Дата внесения изменений	На основании / в соответствии	Внесённые изменения (в каком разделе программы).	Кем внесены изменения (Ф.И.О.- подпись)
Составлена 27.08.2019	<ul style="list-style-type: none"> Федеральный закон Российской Федерации от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации". Концепция развития дополнительного образования детей. Утверждена распоряжением Правительства Российской Федерации от 4 сентября 2014 г. № 1726-р. Приказ Министерства образования и науки РФ от 29 августа 2013 г. № 1008 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам". «Примерные требования к содержанию и оформлению образовательных программ дополнительного образования детей (письмо Министерства образования РФ от 11.12.2006 N 06-1844). Постановление Главного государственного санитарного врача РФ от 4 июля 2014 г. № 41 "Об утверждении СанПиН 2.4.4.3172-14 "Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей". 	<p>1.Титульный лист – оформлен в соответствии с рекомендациями.</p> <p>2.Пояснительная записка, учебно-тематический план (каждого года обучения) , календарный учебный график (каждого года обучения), содержание (каждого года обучения), методическое обеспечение программы (каждый год обучения), рекомендуемая литература, система оценки результатов освоения программы - оформлены и выстроены в соответствии с методическими рекомендациями.</p>	Иванова И.Б

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

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».

Отличительная особенность. Дополнительная общеразвивающая программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для следующих уровней общего образования: начального общего образования, основного общего и среднего общего образования.

Актуальность дополнительной общеразвивающей программы «Безопасность в сети Интернет» 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 защиты детей.

Педагогическая целесообразность. Данная программа составлена на основе курса «Основы кибербезопасности» для общеразвивающих организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована. Содержание программного материала этих тем, как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному. Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углублённости, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

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.

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 учащихся: неоднородный (смешанный); постоянный. Допускается участие учащихся с ОВЗ, детей, оказавшихся в трудной жизненной ситуации.

Наполняемость группы:

1 год обучения
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.

Срок реализации программы - 1 год, объём 51 час.

Продолжительность образовательного процесса:

Периодичность в неделю	Продолжительность занятия	Кол-во часов в неделю	Кол-во часов в год
1 раз	45 минут	2 часа	64

Форма обучения: очная.

Форма проведения занятий: аудиторная, внеаудиторная.

Расписание занятий составлено с учетом школьного расписания в образовательных учреждениях и свободного времени учащихся. 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		
	<i>Личностные</i>	<i>Метапредметные</i>	<i>Предметные</i>
2019-2020	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.

В результате освоения данной программы по окончании учебного года учащиеся:

Будут знать	Будут уметь
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,	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

<p>электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами.</p> <p>Виды общения в Интернете. Правила безопасной работы приинтернет–общении.</p> <p>Уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении.</p> <p>Основные понятия о компьютерных вирусах и контент-фильтрах.</p> <p>Принципы работы интернет - магазинов, понятие «электронные деньги».</p> <p>Дозировано использовать личную информацию в сети интернет.</p> <p>Правила сетевого этикета.</p> <p>Политику государства в области защиты информации.</p>	<p>электронной почтой. Владеть основными приемами поиска информации в сети Интернет.</p> <p>Соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе.</p> <p>Уметь применять программу</p> <p>Отличать вредные игры от полезных.</p> <p>Использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры.</p> <p>Различать (распознавать) мошеннические действия.</p> <p>Корректно общаться в сети Интернет.</p> <p>Защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).</p>
--	--

Система оценки результатов освоения программы– педагогическое наблюдение, 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 «Безопасность в сети Интернет» включают следующих перечень необходимого оборудования:

1. Компьютер
2. Мультимедийный проектор
3. Интерактивная доска
4. Доступ к сети Интернет
5. Кабинет «Точка роста»

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№п/п	Тема	Всего часов	теория	практика	Формы контроля
1.	Информация, компьютер и Интернет.	12	5	7	тестирование
2.	Техника безопасности и экология	9	4	5	Творческая работа
3.	Мир виртуальный и реальный. Интернет зависимость.	9	4	5	Творческая работа
4.	Методы безопасной работы в Интернете	9	4	5	Творческая работа
5.	Потребительские опасности в Интернете	9	3	6	Творческая работа
6.	Основные правила поведения сетевого взаимодействия	9	3	6	Творческая работа
7.	Государственная политика в области в области защиты информации	7	2	5	тестирование
8.	Итого	64	25	39	

Календарный учебный график

Дата	Тема	Всего часов	Теория	Практика	Формы контроля
Тема 1. Информация, компьютер и Интернет. 12 часов					
	Компьютер и информация	1	1		Наблюдение
	Поиск информации в сети Интернет. Работа с мобильными устройствами	1		1	Практическое занятие
	Полезные и вредные страницы Интернета	1	1		Наблюдение
	Как работать в группе	1	1		Наблюдение
	Общение с использованием видеосвязи на примере Skype	1		1	Практическое занятие
	Категории персональных данных	1	1		Наблюдение
	Создание электронной почты	1		1	Практическое занятие
	Информационный буклет	2		2	Практическое занятие
	Кибербезопасность	1	1		Наблюдение
	Безопасность при удаленном доступе к ресурсам компьютера	2		2	Тестирование
Тема 2. Техника безопасности и экология					
	Гигиена при работе с компьютером	1	1		Наблюдение
	ПК и ЗОЖ. Организация рабочего места	2		2	Практическое занятие
	Как защитить компьютер от повреждений	1	1		Наблюдение
	Польза и вред компьютерных игр	1	1		Наблюдение
	Использование мобильного приложения Компас	2		2	Практическое занятие

	Компьютер и мобильные устройства в чрезвычайных ситуациях	2	1	1	Наблюдение
Тема 3. Мир виртуальный и реальный. Интернет зависимость. 9 часов					
	Социальные сети	1	1		Наблюдение
	Создание сообщества класса в детских социальных сетях	2		2	Практическое занятие
	Интернет-зависимости	1	1		Наблюдение
	Создание видеоролика на тему «Проблемы Интернет - зависимости»	2		2	Практическое занятие
	Незнакомцы в интернете	2	1	1	Наблюдение
	Деструктивная информация	1	1		Наблюдение
Тема 4. Методы безопасной работы в Интернете. 9 часов					
	Вредный контент	1	1		Наблюдение
	Вирусы	1	1		Наблюдение
	Колобанга в поисках вируса	2		2	
	Антивирусная защита	1	1		Наблюдение
	Установка антивирусной программы	2		2	
	Меры личной безопасности при сетевом общении	2	1	1	Наблюдение
Тема 5. Потребительские опасности в Интернете. 9 часов					
	Интернет и экономика - польза и опасность	1	1		Наблюдение
	Как не стать жертвой сетевых шуток и розыгрышей	2		2	Практическое занятие
	Лотерея	1	1		Наблюдение
	Правила поведения в сети с мошенниками и злоумышленниками	2		2	Практическое занятие
	Мошенничество	1	1		Наблюдение
	Мошеннические действия в Интернете. Киберпреступления	2		2	Практическое занятие
Тема 6. Основные правила поведения сетевого взаимодействия. 9 часов					
	Интернет-этикет	2	1	1	Наблюдение
	Пишу письмо другу	2		2	
	Этика дискуссий	1	1		Наблюдение
	Психологическая обстановка в Интернете	2	1	1	Наблюдение
	Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора»	2		2	Тестирование
Тема 7. Государственная политика в области защиты информации 7 часов					
	Войны нашего времени	2	1	1	Наблюдение
	Информационная война. Информационное воздействие	2		2	Практическое занятие
	Собственность в Интернете	1	1		Наблюдение
	Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО	2		2	Тестирование

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. - 12 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 - скайп, IP-телефония, ICQ. 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. Поиск информации в сети Интернет. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).

Практическая работа. Общение с использованием видеосвязи на примере Skype.

Практическая работа. Создание электронной почты

Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

Практическая работа «Безопасность при удаленном доступе к ресурсам компьютера».

Тема №2.-9ч.

Техника безопасности и экология

Теория: Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами. Компьютер и зрение. Компьютер и недостаток движения. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Комплекс упражнений при работе за компьютером. **Как защитить компьютер от повреждений.** Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности. **Польза и вред компьютерных игр.** Компьютер и мобильные устройства в чрезвычайных ситуациях. Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.

Практика:

Практическая работа. Использование мобильного приложения Компас

Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема №3.-9ч.

Мир виртуальный и реальный. Интернет зависимость.

Теория: Что такое Интернет-сообщество. Как не превратить свою жизнь 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. Создание сообщества класса в детских социальных сетях

Практическая работа. «Создание видеоролика на тему «Проблемы Интернет - зависимости».

Тема №4.-9ч.

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, целкомпьютерных 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. Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).

Практическая работа. «Установка антивирусной программы»;

Тема №5.-9ч.**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. Кибернаемники кибердетективы. Оценка ущерба от киберпреступлений.

Практика: Прохождение интерактивного курса.

«Мошеннические действия в Интернете. Киберпреступления».

Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

Тема №6.-9ч.**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:** гриффинг, 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 «Пишу письмо другу»

Практическая работа. «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора».

Тема №7. - 7 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 «Создание презентации «Информационная война. Информационное воздействие»

Практическая работа. «Создание презентации «Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО»

Методическое обеспечение программы

№	Тема	Форма занятия.	Приемы и методы.	Дидактический материал, ТСО.	Формы контроля
1.	Информация, компьютер и Интернет	Занятия: учебные, игровые практические.	Беседа, рассказ, показ.	Раздаточный материал иллюстративная наглядность.	Тестирование
2.	Техника безопасности и экология	Учебное занятие	Словесные, Практические, наглядные.	Раздаточный материал, иллюстративная наглядность	Творческая работа
3.	Мир виртуальный и реальный. Интернет зависимость	Занятия: учебные, игровые практические, проектно-исследовательские.	Беседа, рассказ, показ фото- и видеоматериалов, наблюдение.	Репродукции осенних пейзажей, гербарий, коллекции; презентации.	Творческая работа
4.	Методы безопасной работы в Интернете	Учебное занятие	Словесные практические наглядные, частично - поисковые	Инструкционно – технологические карты, иллюстративная наглядность	Творческая работа
5.	Потребительские опасности в Интернете	Занятия: учебные, игровые практические, проектно-исследовательские.	Объяснительно - иллюстративные практические наглядные.	Раздаточный материал, иллюстративная наглядность	Творческая работа
6.	Основные правила поведения сетевого взаимодействия	Учебное занятие	Словесные, практические, наглядные.	Раздаточный материал, иллюстративная наглядность	Тестирование
7.	Государственная политика в области в области защиты информации	Занятия: учебные, игровые практические, проектно-исследователь	Словесные, практические, наглядные	Раздаточный материал, иллюстративная наглядность	Тестирование

		ские			
--	--	------	--	--	--

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 - [https://rg.ru/2010/12/31 /deti-inform-dok.html](https://rg.ru/2010/12/31/deti-inform-dok.html);
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» - <http://base.garant.ru/12188176/>;
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) // <http://www.consultant.ru/>; <http://www.garant.ru/>
4. Федеральный государственный образовательный стандарт начального общего образования (1-4 классы) (Приказ Министерства образования и науки РФ от 6 октября 2009 г. N 373 "Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования" С изменениями и дополнениями от: 26 ноября 2010 г., 22 сентября 2011 г., 18 декабря 2012 г., 29 декабря 2014 г., 18 мая, 31 декабря 2015 г. <http://base.garant.ru/197127/#ixzz4tOU3n8rF>);
5. Федеральный государственный образовательный стандарт начального общего образования обучающихся с ограниченными возможностями здоровья (Приказ Министерства образования и науки РФ от 19 декабря 2014 г. N 1598 "Об утверждении федерального государственного образовательного стандарта начального общего образования обучающихся с ограниченными возможностями здоровья" <http://base.garant.ru/70862366/#ixzz4tOz0KaU2>);
6. Федеральный компонент государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования (1-4 классы) (с изменениями на 7 июня 2017 года).
7. Приказ Министерства образования и науки Российской Федерации от 30.08.2013 г. № 1015 (в ред. Приказов Минобрнауки России от 13.12.2013 г. №1342, от 28.05.2014 г. № 598, от 17.07.2015 г. № 734) «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования» (Зарегистрировано в Минюсте России 01.10.2013 г. № 30067) // <http://www.consultant.ru/>; <http://www.garant.ru/>
8. Приказ Минобрнауки России от 15 июня 2016 г. № 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров» // <http://www.consultant.ru/>; <http://www.garant.ru/>
9. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 № 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 № 85, Изменений № 2, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 25.12.2013 г. № 72, Изменений № 3, утв. Постановлением Главного государственного санитарного врача РФ от 24.11.2015 г. № 81) // <http://www.consultant.ru/>; <http://www.garant.ru/>
10. Постановление Главного государственного санитарного врача Российской Федерации от 10.07.2015 г. № 26 «Об утверждении СанПиН 2.4.2.3286-15 «Санитарно-эпидемиологические требования к условиям и организации обучения и воспитания в организациях, осуществляющих

образовательную деятельность по адаптированным основным общеобразовательным программам для обучающихся с ограниченными возможностями здоровья» (Зарегистрировано в Минюсте России 14.08.2015 г. № 38528) // <http://www.consultant.ru/>; <http://www.garant.ru/>

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: Безопасностьсетей: 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.

Дополнительная:

1. "Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26
2. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасностьобъекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с.
3. Клепа и железный друг//Клепа. - 2014. - № 8. - С. 1-33.Электронная версия журнала: <http://klepa.ru>.
4. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.
5. Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил
6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. - Феникс, 2008.

Интернет ресурсы

Полезные ссылки для учителя:

- 1) <http://www.kaspersky.ru>- антивирус «Лаборатория Касперского»;
- 2) <http://www.onlandia.org.ua/rus/> - безопасная web-зона;
- 3) [http:// www.interneshka.net](http://www.interneshka.net) - международный онлайн-конкурс по безопасному использованию Интернета;

- 4) Рыжков В.Н. Методика преподавания информатики// <http://nto.immpu.sgu.ru/sites/default/files/3/12697.pdf>;
- 5) <http://www.saferinternet.ru> - портал Российского Оргкомитета по безопасному использованию Интернета;
- 6) <http://content-filtering.ru> - Интернет СМИ «Ваш личный Интернет»;
- 7) <http://www.rgdb.ru> - Российская государственная детская библиотека
- 8) <http://www.saferinternet.ru/> - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
- 9) <http://www.saferunet.ru/> - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
- 10) <http://www.fid.su/> - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
- 11) <http://www.microsoft.com/Rus/athome/security/kids/etusivu.html>- Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете"
— интерактивный курс по Интернет-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;
- 12) <http://www.ifap.ru>

Полезные ссылки для обучающихся:

- 1) http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids - ClubSymantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;
- 2) <http://www.nachalka.com/bezopasnost> - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям;
- 3) <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html> - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;
- 4) <http://www.ifap.ru/library/book099.pdf> - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;
- 5) <http://www.interneshka.net/children/index.phtml> - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;
- 6) <http://www.oszone.net/6213/-OS.zone.net-Компьютерный> информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;
- 7) <http://www.rgdb.ru/innocuous-internet-> Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов

для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;

8) <https://www.google.ru/safetycenter/families/start/basics/> - Центр безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени;

9) <https://ege.yandex.ru/security/> - Тесты по безопасности;

10) <http://www.slideshare.net/shperk/ss-47136465> - Безопасность в Интернете. Анатолий Шперх;

11) <http://shperk.ru/v-seti/prokrustovo-lozhe.html> - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;

12) <http://shperk.ru/sovety/avtoritet.html> - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;

13) <http://habrahabr.ru/company/mailru/blog/252091/> - Советы по безопасности.

<http://www.ifap.ru>

Тест по безопасности в сети Интернет

1. Как могут распространяться компьютерные вирусы?
 - a. Посредством электронной почты.
 - b. При просмотре веб-страниц.
 - c. Через клавиатуру.
 - d. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
 - a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
 - b. Он защищает компьютер от вирусов.
 - c. Он обеспечивает защиту секретных документов.
 - d. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
 - a. Да
 - b. Да, если вы знаете отправителя
 - c. Нет, поскольку данные отправителя можно легко подделать
 - d. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
 - a. Продолжить Будто ничего не произошло.
 - b. Нажать кнопку «ОК» или «ДА»
 - c. Обратится за советом к учителю, родителю или опекуну.
 - d. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
 - a. Удалить его, не открывая.
 - b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
 - c. Открыть вложение, если такое имеется в сообщении.
 - d. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
 - a. Переслать его пяти друзьям.
 - b. Переслать его не пяти друзьям, а десяти друзьям.
 - c. Не пересылать никакие «письма счастья»
 - d. Ответить отправителю, что вы больше не хотите получать от него/нееписьма.
7. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?
 - a. Во всех случаях.
 - b. Когда кто-то просит об этом.
 - c. когда собеседник в чате просит об этом.
 - d. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.

8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?
- Запомнить его.
 - Постараться забыть пароль.
 - Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
 - Сообщить пароль родителям.
9. Что такое сетевой этикет?
- Правила поведения за столом.
 - Правила дорожного движения.
 - Правила поведения в Интернете.
 - Закон, касающийся Интернета.
10. Что запрещено в интернете?
- Запугивание других пользователей.
 - Поиск информации.
 - Игры.
 - Общение с друзьями

Тест по безопасности в сети Интернет
«Основы безопасности в Интернете» Осторожно, вирус!

- Что является основным каналом распространения компьютерных вирусов?
 - Веб-страницы
 - Электронная почта
 - Флеш-накопители (флешки)
- Для предотвращения заражения компьютера вирусами следует:
 - Не пользоваться Интернетом
 - Устанавливать и обновлять антивирусные средства
 - Не чихать и не кашлять рядом с компьютером
- Если вирус обнаружен, следует:
 - Удалить его и предотвратить дальнейшее заражение
 - Установить какую разновидность имеет вирус
 - Выяснить как он попал на компьютер
- Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
 - Применение брандмауэра
 - Обновления операционной системы
 - Антивирусная программа
- Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
 - Уничтожение компьютерных вирусов
 - Создание и распространение компьютерных вирусов и вредоносных программ
 - Установка программного обеспечения для защиты компьютера

Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
 - a. Свои увлечения
 - b. Свой псевдоним
 - c. Домашний адрес
2. Чем опасны социальные сети?
 - a. Личная информация может быть использована кем угодно в разных целях
 - b. При просмотре неопознанных ссылок компьютер может быть взломан
 - c. Все вышеперечисленное верно
3. Виртуальный собеседник предлагает встретиться, как следует поступить?
 - a. Посоветоваться с родителями и ничего не предпринимать без их согласия
 - b. Пойти на встречу одному
 - c. Пригласить с собой друга
4. Что в Интернете запрещено законом?
 - a. Размещать информацию о себе
 - d. Размещать информацию других без их согласия
 - c. Копировать файлы для личного использования
5. Действуют ли правила этикета в Интернете?
 - a. Интернет - пространство свободное от правил
 - b. В особых случаях
 - c. Да, как и в реальной жизни

Тест по безопасности в сети Интернет

1. Когда можно полностью доверять новым онлайн-друзьям?
 - a) Ничто не может дать 100%-ную гарантию того, что онлайн-другу можно доверять
 - b) Поговорив по телефону
 - c) После обмена фотографиями
 - d) Когда есть общие друзья
 - e) После длительного онлайн-знакомства (переписки)
2. Что делать, если ты столкнулся с троллем в Сети?
 - a) Сообщить модераторам сайта
 - b) Рассказать взрослым
 - c) Игнорировать выпады тролля
 - d) Заблокировать тролля
 - e) Проучить или доказать свою правоту
3. Как пожаловаться на неприемлемый контент на YouTube?
 - a) Выразить свое недовольство в комментариях к видео
 - b) Отметить видео “флажком”, который находится под ним
 - c) Такого функционала нет
 - d) Найти электронный адрес автора видео и написать ему сообщение

4. Что является признаком фишинг-сообщения?
 - a) В сообщении много ошибок, неточностей и противоречий
 - b) Сообщение содержит обещание большой выгоды с минимальными усилиями
 - c) В сообщении требуется срочно сменить пароль от электронной почты по причине вероятной попытки взлома электронного ящика, при этом сообщение не отправлено с официального адреса почтовой службы
 - d) В сообщении запрашиваются твои личные данные, финансовая информация, пароли
 - e) Сообщение содержит угрозу для жизни и здоровья близких людей
5. Как обезопасить себя при первой встрече с онлайн-другом?
 - a) Заранее пообщаться с “незнакомцем” по телефону, попросить прислать фотографии, таким образом убедиться, что он тот, за кого себя выдает
 - b) Убедиться, что у вас есть общие увлечения и темы для разговора в реальной жизни
 - c) Встречаться с интернет-незнакомцами очень опасно, лучше не назначать встречу, если не знакомы с человеком лично
 - d) Попросить присутствовать взрослых
 - e) Сообщить о встрече родителям/взрослым, спросить их совета
 - f) Взять на встречу друзей и выбрать людное место в светлое время суток
6. Где можно найти информацию для реферата в Интернете?
 - a) На сайтах средств массовой информации
 - b) В электронной библиотеке
 - c) В поисковой системе
 - d) В Википедии
7. Какую информацию о себе опасно выкладывать в Интернете в открытом доступе?
 - a) Дату рождения
 - b) О своих интересах
 - c) Информацию о доходах родителей
 - d) Домашний адрес и телефон
 - e) Место работы родителей
8. Как пожаловаться на неприемлемый контент на YouTube?
 - a) Отметить видео “флажком”, который находится под ним
 - b) Такого функционала нет
 - c) Выразить свое недовольство в комментариях к видео
 - d) Найти электронный адрес автора видео и написать ему сообщение
9. Что делать, если вы стали жертвой интернет-мошенничества?
 - a) Сообщить взрослым
 - b) Сменить все пароли
 - c) Попробовать решить проблему самостоятельно
 - d) Позвонить на Линию помощи «Дети онлайн»
10. Как нужно себя вести, если вы стали жертвой кибербуллинга?

- a) Обратиться за поддержкой к модераторам сайта
- b) Пытаться бороться с обидчиками в одиночку
- c) Заблокировать обидчиков
- d) Сообщить родителям/взрослым
- e) Ничего не делать
- f) Обратиться на Линию помощи «Дети онлайн»

11. Как защититься от негативного контента?

- a) Установить программы родительского контроля
- b) Сообщить модераторам сайта, пожаловаться на неприемлемый контент с помощью специальных инструментов, доступных на сайте
- c) Обратиться к автору негативного контента
- d) Не обращать на него внимания
- e) Использовать безопасный поиск Google и безопасный режим на YouTube
- f) рос:

12. Что следует делать, если на сайте вас просят отправить бесплатное сообщение на короткий номер?

- a) Как можно быстрее отправить СМС
- b) Постараться найти стоимость СМС на сайте, после этого поискать в интернете, какова стоимость отправки СМС на этот номер, и перепроверить эту информацию. До перепроверки информации не отправлять СМС
- c) Использовать телефон друга или знакомого чтобы, отправить СМС

13. Что делать, если ты столкнулся с троллем в Сети?

- a) Игнорировать выпады тролля
- b) Проучить или доказать свою правоту
- c) Заблокировать тролля
- d) Рассказать взрослым
- e) Сообщить модераторам сайта

14. Как защитить свою электронную почту от взлома и махинаций?

- a) Регулярно менять пароли
- b) Активировать систему двухэтапной верификации на сервисах, которые позволяют это сделать
- c) Никому не сообщать свой пароль
- d) Периодически менять адрес электронной почты, менять провайдеров
- e) Не открывать сообщения с незнакомых и подозрительных адресов
- f) Создавать разные пароли от разных аккаунтов, включая электронную почту, систему электронного банкинга и пр.

15. При каких условиях можно доверять письму от неизвестного отправителя?

- a) Никогда нельзя доверять письму от неизвестного отправителя
- b) К вам обращаются по имени
- c) Отправитель использует логотип авторитетной компании
- d) Письмо содержит важную информацию о ваших близких
- e) Отправитель ссылается на ваших друзей

16. Что делать, если вам пришло письмо о том, что вы выиграли в лотерее?
- a) Отметить сообщение как спам
 - b) Перейти по ссылке в письме, ведь в редких случаях информация может оказаться правдой
 - c) Удалить его
 - d) Заблокировать отправителя
 - e) Написать в ответ разоблачающее письмо мошенникам
17. Что делать, если вам приходит сообщение по электронной почте или во всплывающих окнах о том, что ваш компьютер заражён?
- a) Пройти по предлагаемым ссылкам и скачать антивирусную систему
 - b) Закрыть всплывающее окно и не нажимать на ссылки в нём
 - c) Просканировать компьютер на возможные вирусы, при этом не переходить по неизвестным ссылкам
18. Как защитить компьютер от атак вредоносных программ?
- a) Никогда не переходить по ссылкам из всплывающих окон
 - b) Перед запуском проверять все файлы, скачанные из Интернета, с помощью антивируса
 - c) Регулярно обновлять браузер, операционную систему, антивирусную программу и прикладное программное обеспечение
 - d) Установить на компьютер сразу несколько антивирусных программ
 - e) Установить антивирусную программу с официального сайта
 - f) Не открывать вложения в письмах, присланных с неизвестных электронных адресов, а также с осторожностью относиться к письмам, которые пришли с известного вам адреса, но чье содержание кажется подозрительным: аккаунт ваших знакомых может быть взломан и содержать вирусы
19. Какие функции браузера не следует использовать на общественном компьютере?
- a) Безопасный поиск
 - b) Автозаполнение форм
 - c) Автосохранение паролей
 - d) Режим инкогнито
20. В каком случае нарушается авторское право?
- a) При размещении на YouTube собственного видеоролика с концерта любимой группы
 - b) При использовании материалов Википедии для подготовки реферата со ссылкой на источник
 - c) При размещении не лицензионного контента в социальных сетях
 - d) При просмотре не лицензионного контента в социальных сетях
 - e) При чтении романа Л.Н. Толстого «Война и мир» в Интернете
21. Что в Интернете запрещено законом?
- a) Размещать информацию о себе
 - b) Размещать информацию других без их согласия
 - c) Копировать файлы для личного использования

22. Действуют ли правила этикета в Интернете?
- a) Интернет - пространство свободное от правил
 - b) В особых случаях
 - c) Да, как и в реальной жизни
23. Чем опасны социальные сети?
- a) Личная информация может быть использована кем угодно в разных целях
 - b) При просмотре неопознанных ссылок компьютер может быть взломан
 - c) Все вышеперечисленное верно
24. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
- a) Применение брандмауэра
 - b) Обновления операционной системы
 - c) Антивирусная программа
25. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
- a) Уничтожение компьютерных вирусов
 - b) Создание и распространение компьютерных вирусов и вредоносных программ
 - c) Установка программного обеспечения для защиты компьютера

Пронумеровано, прошито, скреплено печатью

23 *Гвардейск* *1994* *мск*

Директор

И.Л. Ковалев

