Токарева Виктория Алексеевна

Подписано цифровой подписью: Токарева Виктория Алексеевна
DN: cn=Токарева Виктория Алексеевна, o=ГБУ ИМЦ Кронштадтского района Санкт-Петербурга, ou=директор, email=kronnmc@obr.gov.spb.ru, c=RU
Дата: 2025.06.25 11:00:33 +03'00'

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ «ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЙ ЦЕНТР» КРОНШТАДТСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

ПРИНЯТА
Педагогическим советом
ГБУ ИМЦ Кронштадтского района
Санкт-Петербурга

Протокол №___3_____
от «__14_»___августа___2024 г.

УТВЕРЖДЕНА
Директор ГБУ ИМЦ
Кронштадтского района
Санкт-Петербурга

_____В.А. Токарева
Приказ № 18-Д «_20__»_января__2025 г.

РАБОЧАЯ ПРОГРАММА

курсов повышения квалификации

по дополнительной профессиональной программе

«Кибергигиена - информационная безопасность в сети Интернет»

(наименование программы)

(36 часов)

1,2,3,4 группы

Преподаватель: Рахманова Н.В.

г. Санкт-Петербург

2025

Раздел 1. Характеристика программы

1.1. Цель реализации программы – совершенствование профессиональных компетенций педагогов, необходимых для профессиональной деятельности в области формирования информационной безопасности несовершеннолетних в образовательной организации.

1.2. Планируемые результаты обучения:

Трудовые функции	Трудовые действия	Знать	Уметь
Общепедагогическая функция. Обучение.	Создание безопасной и комфортной образовательной среды	Знать ключевые понятия проблемы безопасности. Знать нормативно-правовую базу, регламентирующую вопросы информационной безопасности несовершеннолетних. Знать основные понятия информационной безопасности, основные риски и угрозы сети Интернет. Знать особенности восприятия негативной информации детьми разного возраста. Знать возможности технических и программных средств обеспечения информационной безопасности детей в сети Интернет.	Уметь распознавать риски и угрозы сети Интернет. Уметь организовывать работу по формированию информационной безопасности в ОО с педагогами, обучающимися, родителями.

1.3. Категория слушателей: педагоги, реализующие программы начального, основного, среднего, дополнительного и среднего профессионального образования.

1.4. Форма обучения – очная (с использованием дистанционных образовательных технологий).

1.5. Срок освоения программы: 36 ч.

1.6 Учебный план

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Самостоятельная работа, час	Формы контроля
			Лекция, час	Интерактивное (практическое) занятие, час		
1.	**Методический модуль**	**10**	**6**	**1,5**	**2,5**	Анкета Тест

2.	**Теоретический модуль**	**24**	**11,5**	**3,5**	**9**	Тест Опрос Практическая работа
3.	**Итоговая аттестация**	**2**	**0**	**2**	**0**	Тест Решение кейсов
	Итого:	**36**	**17,5**	**7**	**11,5**	

1.7 Календарный учебный график

Регламент занятий:

Учебные занятия в учреждении проходят 1- 2 раза в неделю (в соответствии с утвержденным Календарным учебным графиком).

Учебными днями являются понедельник, вторник, среда, четверг, пятница. В праздничные и выходные дни учебные занятия не проводятся.

Для всех видов аудиторных занятий академический час установлен в размере 45 минут. Занятия могут проводятся в виде сдвоенных академических часов (пара) с перерывом между часами 5 минут, между парами - не менее 10 минут.

№ п.п.	Наименование ДПП ПК	Категория слушателей	Объем ДПП ПК в часах	Количество групп	Количество человек в группе	Срок проведения занятий	Время занятий группы	Место проведения занятий
1	Кибергигиена - информационная безопасность в сети интернет	Работники образовательных учреждений	36	4	12	1 группа КИБ-01.25 19.05.2025 – 16.06.2025	Понедельник, вторник 11.10 – 14.30	Ауд. 5
					12	2 группа КИБ-02.25 19.05.2025 – 16.06.2025	Понедельник, вторник 14.40 – 18.00	Ауд. 5
					12	2 группа КИБ-03.25 13.10.2025 – 10.11.2025	Понедельник, среда 11.10 – 14.30	Ауд. 5
					12	2 группа КИБ-04.25 13.10.2025 – 10.11.2025	Понедельник, среда 14.40 – 18.00	Ауд. 5

Раздел 2. Содержание программы

№ п/п	**Наименование разделов (модулей) и тем**	**Всего часов**	**Виды учебных занятий, учебных работ**		**Самостоятельная работа, час**	**Формы контроля**
			Лекция, час	**Интерактивное (практическое) занятие, час**		

1.	**Методический модуль**	**10**	**6**	**1,5**	**2,5**	
1.1	Входная диагностика	0,5	0	0,5	0	Анкета
1.2	Введение в курс: актуальность, цели и задачи	1,5	1,5	0	0	
1.3	Теория смешанного обучения	3	1	1	1	Тест
1.4	Модели смешанного обучения	2	1,5	0	0,5	Тест
1.5	Подготовка к уроку по модели «ротация станций»	3	2	0	1	Тест
2.	**Теоретический модуль**	**24**	**11,5**	**3,5**	**9**	
2.1	Онлайн-идентичность и жизнь в «цифровом зазеркалье»	3	1	1	1	Тест
2.2	Персональные данные и цифровой след	4	1,5	1	1,5	Тест Опрос
2.3	Кибербуллинг	2	1,5	0	0,5	Тест
2.4	Принципы безопасного общения в интернете	2	1	0	1	Тест Практическая работа
2.5	Беспроводные соединения, аутентификация и стойкие пароли	2	1	0	1	Тест
2.6	Виды вредоносного ПО и как защитить свои устройства	2	1	0,5	0,5	Тест Практическая работа
2.7	Фишинг – как защитить себя от мошенников	2	1	0	1	Тест
2.8	Принципы безопасного поведения в сети	2	1	0	1	Практическая работа
2.9	Безопасное хранение данных	3	1	1	1	Тест
2.10	Дропперство в киберпреступлениях и как вид финансового мошенничества: что это и как с ним бороться	2	1,5	0	0,5	Тест
3.	**Итоговая аттестация**	**2**	**0**	**2**	**0**	**Тест Решение кейсов**
	Итого:	**36**	**17,5**	**7**	**11,5**	

2.2. Рабочая программа

1. Методический модуль

1.1 Входная диагностика (практическое занятие 0,5 ч.) – проводится с целью выявления образовательных потребностей слушателей. Анализ результатов анкетирования позволит скорректировать содержание занятий курсовой подготовки.

1.2 Введение в курс: актуальность, цели и задачи (лекции – 1,5 ч.)

Нормативно-правовая база по защите от киберпреступлений. Зачем нужно современному школьнику изучать курс «Уроки кибербезопасности»? Цели и задачи курса «Кибергигиена - информационная безопасность в сети интернет».

1.3 Теория смешанного обучения (лекция – 1 ч., практическая работа – 1 ч., самостоятельная работа – 1 ч.)

Теория о смешанной форме обучении. Технология смешанного обучения. Вопросы для самопроверки. Самостоятельная работа (Основные этапы построения смешанного обучения в правильном порядке. Распределить роли и деятельность учителя в соответствии с видами обучения).

1.4 Модели смешанного обучения (лекция – 1,5 ч., самостоятельная работа – 0,5 ч.)

Модели смешанного обучения. Вопросы для самопроверки.

1.5 Подготовка к уроку по модели «ротация станций» (лекция – 2 ч., самостоятельная работа – 1 ч.)

Лекция «Подготовка к уроку по модели «ротация станций»». Чек-лист для подготовки урока. Примеры уроков.

2. Теоретический модуль

2.1 Онлайн-идентичность и жизнь в «цифровом зазеркалье» (лекция – 1 ч., практическая работа – 1 ч., самостоятельная работа – 1 ч.)

Введение. Жизнь в «цифровом зазеркалье». Онлайн-идентичность. Памятка «Виды манипуляторов» (практическая работа). Вопросы для самопроверки. Тест "Виды аккаунтов".

2.2 Персональные данные и цифровой след (лекция – 1,5 ч., практическая работа – 1 ч., самостоятельная работа – 1,5 ч.)

Лекция «Персональные данные и цифровой след». Как повысить уровень конфиденциальности в социальных сетях и передавать о себе меньше данных? Вопросы для самопроверки. Тест «Персональные данные».

2.3 Кибербуллинг (лекция – 1,5 ч., самостоятельная работа – 0,5 ч.)

Определение и виды кибербуллинга. Куда сообщить об опасном контенте или угрозах в сети интернет? Действия классного руководителя при обнаружении кибербуллинга в классе. Куда обратиться за психологической помощью? Вопросы для самопроверки.

2.4 Принципы безопасного общения в интернете (лекция – 1 ч., самостоятельная работа – 1 ч.)

Правила безопасного общения в Интернете. Вопросы для самопроверки. Практическая работа.

2.5 Беспроводные соединения, аутентификация и стойкие пароли (лекция – 1 ч., самостоятельная работа – 1 ч.)

Безопасное использование беспроводных соединений. Вопросы для самопроверки.

2.6. Виды вредоносного ПО и как защитить свои устройства (лекция – 1 ч., практическая работа – 0,5 ч., самостоятельная работа – 0,5 ч.)

Виды вредоносного ПО и как защитить свои устройства. Методы защиты от вредоносных программ. Практическая работа «Чек-лист защиты от вредоносных программ». Вопросы для самопроверки. Тест «Распределите поведенческие ситуации с точки зрения безопасного поведения в сети интернет».

2.7 Фишинг – как защитить себя от мошенников (лекция – 1 ч., самостоятельная работа – 1 ч.)

Принципы безопасного поведения в сети. Как защитить себя от фишинга. Примеры сомнительных писем от госорганов. Вопросы для самопроверки.

2.8 Принципы безопасного поведения в сети (лекция – 1 ч., самостоятельная работа – 1 ч.)

Принципы безопасного поведения в сети. Правила онлайн-покупок. Вопросы для самопроверки.

2.9 Безопасное хранение данных (лекция – 1 ч., практическая работа – 1 ч., самостоятельная работа – 1 ч.)

Безопасное хранение данных. Правило резервного копирования данных. Вопросы для самопроверки.

2.10 Дропперство в киберпреступлениях и как вид финансового мошенничества: что это и как с ним бороться (лекция – 1,5 ч., самостоятельная работа – 0,5 ч.)

Дропперство - новые уловки финансовых мошенников. Дропперы - преступление и наказание. Дропперство в киберпреступлениях. Вопросы для самопроверки.

Раздел 3. Формы аттестации и оценочные материалы

Входной контроль

Форма: анкетирование.

Описание, требования к выполнению:

Анализ результатов входной диагностики позволит уточнить и конкретизировать содержание занятий по организации повышения квалификации. Анкета включает 50 вопросов.

Проверка проводится автоматически.

Критерии оценивания:

Примеры заданий:

1. Мои ожидания Мое обучение фокусируется на темах, которые меня интересуют.
    - Пока нет ответа
    - Почти никогда
    - Редко
    - Иногда
    - Часто
    - Почти всегда
2. На самом деле Мое обучение фокусируется на темах, которые меня интересуют
    - Пока нет ответа
    - Почти никогда
    - Редко
    - Иногда
    - Часто
    - Почти всегда

Текущий контроль

Раздел программы: Теоретический модуль

Форма: Практическая работа

Описание, требования к выполнению:

Практических работ - 3, время выполнения – 2,5 часа

Критерии оценивания:

Представлены ниже для каждой практической работы.

Примеры заданий:

Практическая работа № 1.

Тема «Виды вредоносного ПО и как защитить свои устройства»

Задание. Разработать чек-лист защиты от вредоносных программ и инструкцию по настройке безопасности браузера для обучающихся.

Необходимо:

1. В текстовом редакторе создать чек-лист защиты от вредоносных программ, используя предложенный шаблон.

2. Выбрать среду (текстовый, графический, онлайн-редактор и др.) для разработки памятки по настройке безопасности браузера для обучающихся.

3. Создать и оформить памятку по настройке безопасности браузера для обучающихся.

4. Готовые работы прикрепить на сайт дистанционного обучения.

Критерии оценивания: Оценивание: зачёт/незачёт. Зачёт, если:

- Все шаги практической работы выполнены верно.
- Содержание соответствует целям инструктивного материала.

- Инструктивный материал соответствует основным правилам оформления документов.

Незачёт, если не выполнено хотя бы одно условие.

Практическая работа № 2.

Тема «Принципы безопасного поведения в сети»

Задание. Разработать на основе предложенных материалов (на выбор): список правил сетевой гигиены, инфографику по защите персональных данных, по организации системы резервного хранения данных, инструкцию по настройке электронного ящика или профиля в социальной сети.

Необходимо:

1. Составить список правил сетевой гигиены для участников образовательной деятельности, используя предложенный набор правил. Оформить список правил в выбранной среде (текстовый, графический, онлайн-редактор и др.). Готовую работу прикрепить на сайт дистанционного обучения.

2. Выбрать одно из направлений технических интернет-рисков, которое Вы будете рассматривать в инструктивном материале (вирусы, почта, соцсеть и др.). Определить меры по профилактике с данными интернет-рисками. Создать и оформить в выбранной среде (текстовый, графический, онлайн-редактор и др.) один инструктивный материал по выбору:

a. инфографику по защите персональных данных обучающихся,

b. схему организации системы резервного хранения данных,

c. инструкцию по настройке электронного ящика,

d. памятку по настройке профиля в социальной сети.

e. свой инструктивный материал по данной теме.

3. Готовую работу прикрепить на сайт дистанционного обучения с описанием одного из направлений технических интернет-рисков и мер их профилактики данного интернет-риска. Разместить файл в облачном хранилище в совместной папке «Копилка материалов слушателей курса» в подкаталоге «Сетевая гигиена».

Критерии оценивания: Оценивание: зачёт/незачёт. Зачёт, если:

- Все шаги практической работы выполнены верно.
- Содержание соответствует целям инструктивного материала.
- Предложены решения по профилактике технических интернет-рисков.
- Инструктивный материал соответствует основным правилам оформления документов.

Незачёт, если не выполнено хотя бы одно условие.

Развернутый ответ на вопрос.

Тема: «Персональные данные и цифровой след»

Вопрос №1.

Проанализируйте, какую информацию о себе оставляете в сети вы?

Вопрос №2.

Может ли эта информация вам чем-то навредить? И можно ли использовать эту информацию против вас?

Критерии оценивания:

Характеристика ответа	Баллы
Дан полный, развёрнутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном ориентировании понятиями, умении выделять существенные и несущественные его признаки, причинно-следственные связи. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося.	100-90
Дан полный, развёрнутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается чёткая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочёты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа.	89-75
Дан полный, развёрнутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы; в ответе прослеживается чёткая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочёты, исправленные обучающимся с помощью преподавателя.	74-60
Дан полный, развёрнутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ чётко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочёты и незначительные ошибки, исправленные обучающимся с помощью преподавателя.	59-45
Дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки, которые обучающийся затрудняется исправить самостоятельно.	44-30
Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют	29-19

выводы. Умение раскрыть конкретные проявления обобщённых знаний не показано. Речевое оформление требует поправок, коррекции.	
Не получен ответ на заданный вопрос. Рассуждения носят отвлеченный характер.	18-0

Промежуточная аттестация

Промежуточная аттестация по модулям осуществляется по совокупности результатов всех видов контроля, предусмотренных программой в соответствующем модуле.

Итоговая аттестация

Форма: тестирование

Описание, требования к выполнению:

Итоговая аттестация проводится с целью выявления уровня знаний теоретического материала и готовность применения полученных знаний на практике и содержит 22 задания с оценкой по 1 баллу за каждый правильный ответ. В тест включены вопросы с выбором одного правильного ответа, нескольких правильных ответов и решение кейсов. Максимальное количество баллов – 22. Время на исполнение – 2 часа.

Критерии оценивания:

Оценивание: зачёт/незачёт Интерпретация результатов:14 – 22 баллов – зачёт; 0 – 13 баллов – незачёт.

Примеры заданий:

Вопрос 1.

Образовательный подход, который совмещает обучение с участием учителя (лицом к лицу) и онлайн-обучение. О какой технологии обучения идет речь?

a. дистанционное обучение
b. дифференцированное обучение
c. смешанное обучение

Вопрос 2.

Что лежит в основе смешанного обучения?

a. обучение учителем
b. онлайн-обучение
c. обучение в группах

Вопрос 3.

Ученики делятся на группы для выполнения разных видов учебной деятельности. В течение урока происходит перемещение групп таким образом, что каждому обучающемуся удается поработать с учителем, на онлайн-платформе и выполнить проект в группе.

О какой модели смешанного обучения идет речь?

a. ротация лабораторий
b. ротация станций

c. перевернутый класс
d. гибкая модель

Вопрос 4.

Выберите верное утверждение: “Основная задача учителя на уроке по модели “ротация станций - это…”

a. это фронтальная организация деятельности учащихся, объяснение нового материала и закрепление полученных знаний на практике
b. это проверка домашнего задания и осуществление контроля за деятельностью обучающихся
c. это управление процессом познания, получения навыков, освоения опыта, координация деятельности обучающихся

Вопрос 5.

По каким параметрам можно вычислить фейковый профиль?

Выберите несколько вариантов ответов

a. Профиль создан давно
b. Профиль создан недавно
c. Мало друзей и подписок
d. Есть плейлисты
e. Фото с других сайтов и стоков

Вопрос 6.

Как называются данные, которые пользователь оставляет неосознанно в интернете?

a. пассивный цифровой след
b. активный цифровой след

Вопрос 7.

Кому необходима психологическая помощь при кибербуллинге?

a. учителям
b. ребенку
c. родителям
d. ребенку и родителям

Вопрос 8.

Вирусы, которые самостоятельно распространяются через локальные и глобальные компьютерные сети.

a. черви
b. ботнеты
c. трояны

Вопрос 9.

Как называются файлы, которые записывают практически любую информацию о посетителе сайта: во сколько и с какого устройства человек заходил на страницу, какими товарами интересовался и так далее?

a. cookie файлы
b. облачные файлы
c. резервные файлы

Вопрос 10.

Верное или ложное это утверждение “Облачные хранилища могут быть использованы для резервного копирования данных”.

a. ложное
b. верное

Вопрос 11.

Вы ввели пароль, и система подтверждает, что вы настоящий пользователь.

a. аутентификация
b. авторизация
c. идентификация

Вопрос 12.

Выберите верное утверждение с точки зрения безопасности ваших данных.

a. Для разных учетных записей создавайте разные пароли.
b. Для разных учетных записей используйте одинаковый пароль.

Вопрос 13.

Безопасный URL-адрес, должен начинаться с …

a. http://
b. https://

Вопрос 14.

Какой вид аутентификации надежнее?

a. двухфакторная
b. однофакторная

Вопрос 15.

Аккаунт, который маскируется под реального человека и пытается вступать в диалог.

a. фейковый аккаунт
b. пользовательский аккаунт

Вопрос 16.

Любое устройство может выйти из строя, а хранящиеся на нем данные будут безвозвратно потеряны. Вспомните основное правило резервного копирования данных.

a. Правило 3-2-1
b. Правило 50/50
c. Правило 80/20

Вопрос 17.

Максим, ученик 7 класса, завел знакомство в социальных сетях. Он познакомился с Сергеем, с ним можно весело поболтать, поделиться своими переживаниями, ведь родители в разводе. Сергей выпросил у мальчика фото неприличного содержания, а через некоторое время начал требовать деньги, в ином случае угрожал обнародовать снимки. Ребенок его заблокировал и родителям ничего не сказал. Тогда Сергей написал родителям мальчика и тоже потребовал денег. Родители обратились в полицию, но там сказали, что таких историй очень много и отговорили писать заявление. В итоге шантажист действительно сдержал слово и разослал фото по всем контактам мальчика, которые взял со страницы Максима и его родителей. Началась травля.

Как вы считаете, должна ли школа помочь Максиму и его родителям? В чем, на ваш взгляд, должна заключаться эта помощь?

Вопрос 18.

Кейс основан на реальных событиях. Старшеклассники решили пошутить. Нашли фотографию, на которой занимаются сексом мужчина и женщина, и с помощью фотошопа заменили их лица на другие. В итоге получилось изображение, где одна из учениц 10 класса занимается сексом со своим учителем-мужчиной. Получившийся фотомонтаж разослали по общим чатам.

Какими, по вашему мнению, должны быть действия учителя? Как отреагирует на данное хулиганство администрация школы?

Вопрос 19.

Представьте, что компьютер, где вы собирали материалы, необходимые для работы, фотографии и видео за несколько лет и многое другое, сломался. Перед вами появилась страшная картинка с надписью “что-то пошло не так” или вообще черный экран. Вы в панике прибегаете в сервисный центр, но специалист говорит, что не может помочь отремонтировать устройство.

Порассуждайте, что необходимо было предпринять, чтобы не потерять данные, накопленные годами?

Вопрос 20.

Пользователю, у которого есть аккаунт в ВКонтакте, приходит на почту личным сообщением письмо со следующим содержанием: “архив на все ваши переписки будет создан через 24 часа и отправлен на почту maria@mail.ru”. Далее вам предлагают войти в аккаунт, чтобы отменить создание и передачу архива, а также сменить пароль по ссылке. [Источник:https://tvernews.ru/news/266739/]

Ваши действия:

a. перейду по ссылке
b. не буду переходить по ссылке

Вопрос 21.

Вы получили письмо от незнакомца со следующим содержанием:

“Дорогой друг!

Мы предлагаем вам быстрый доход со стабильным ежемесячным заработком от 50 тысяч рублей. Всего лишь нужно пройти обучение по работе с нашим сервисом. Я уже попробовал. Посмотри. как у меня получилось. Переходи по ссылке

Ваши действия:

a. не буду переходить по ссылке
b. перейду по ссылке

Вопрос 22.

Вчера вы провели вечер со своими друзьями, веселились, отдыхали, прощаясь, запланировали уже новую встречу. Утром от одного из друзей пришло письмо, помеченное как важное, со следующим содержанием.

“Привет, дружище.

Помогай, у племянницы случилось несчастье. Вся подробная информация здесь. Надеюсь на тебя!”

Ваши действия:

a. не буду переходить по ссылке
b. перейду по ссылке

Количество попыток: 2

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы

1. Об образовании в Российской Федерации / Федеральный закон от 29 декабря 2012 г. N 273-ФЗ (последняя редакция). – [Электронный ресурс]. – URL: http://www.consultant.ru// (дата обращения:– Режим доступа: свободный. – Текст: электронный.
2. Федеральные государственные образовательные стандарты общего образования [Электронный ресурс] // Министерство образования и науки Российской Федерации. 2012 // Режим доступа: http://минобрнауки.рф
3. Профессиональный стандарт «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)» / Приказ Минтруда России от 18.10.2013 г. № 544 Н (с изм. от 05.08.2016), рег. номер 30550. – [Электронный ресурс]. – URL: http://www.consultant.ru//(дата обращения:). – Режим доступа: свободный. – Текст: электронный.

Литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. – Москва : Издательство Юрайт, 2021. – 104 с. – ISBN 978-5-534-14590-8. – URL: https://urait.ru/bcode/477968 (дата обращения: 09.09.2022). – Режим доступа: по подписке. – Текст: электронный.
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов: Профобразование, 2019. – 702 с. – ISBN 978-5-4488-0070-2. – URL:

https://www.iprbookshop.ru/87995.html (дата обращения: 09.09.2022). – Режим доступа: по подписке. – Текст: электронный.
3. Информационная безопасность: Лабораторный практикум / сост.: Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. - Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. - 86 с. - ISBN 978-5-85219-007-9. http://www.iprbookshop.ru/86357.html (дата обращения: 02.09.2022). — Режим доступа: по подписке. — Текст : электронный.
4. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. – 3-е изд. – Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 154 с. – ISBN 978-54497-0338-5. – URL: https://www.iprbookshop.ru/89453.html (дата обращения: 09.09.2022). – Режим доступа: по подписке. – Текст: электронный.

Электронные обучающие материалы

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. – URL: http://www.bnti.ru/dbtexts/analmat/1_2008/ershov.pdf
2. Библиографическая ссылка. Общие требования и правила составления. ГОСТ Р 7.0.5-2008 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов: офиц. сайт. URL: http://docs.cntd.ru/document/1200063713 (дата обращения 20.05.2025).
3. Профилактика кибербуллинга среди обучающихся образовательной организации [Электронный ресурс] // Вологодский институт развития образования: сайт. URL: https://www.viro.edu.ru/attachments/article/10240/1741.pdf (дата обращения 20.09.2025)
4. Солдатова Г. [и др.] Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч.1: Лекции [Электронный ресурс] // Дети России Онлайн: сайт проектов Фонда Развития Интернет. URL http://detionline.com/assets/files/research/BookTheorye.pdf (дата обращения 17.05.2025)
5. Солдатова Г. [и др.] Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч.1: Практикум [Электронный ресурс] // Дети России Онлайн: сайт проектов Фонда Развития Интернет. URL http://detionline.com/assets/files/research/Book_Praktikum.pdf (дата обращения 17.05.2025)

Интернет-ресурсы

1. Безопасность в интернете [Электронный ресурс] // Яндекс.Справка: сайт. URL: https://browser.yandex.ru/help/security/protection.html (дата обращения 16.05.2025)
2. Безопасность в почте Яндекс [Электронный ресурс] // Яндекс.Справка: сайт. URL: https://yandex.ru/support/mail/web/security.html (дата обращения 12.05.2025)
3. Безопасность в почте Mail [Электронный ресурс] // Mail.Справка: сайт. URL: https://help.mail.ru/mail/settings (дата обращения 12.09.2025)
4. ВКонтакте: как настроить безопасность и приватность [Электронный ресурс] // Лаборатория Касперского: электронная энциклопедия. URL: https://www.kaspersky.ru/blog/vk-security-and-privacy-settings/22858/ (дата обращения 22.05.2025)
5. Дети России Онлайн [Электронный ресурс] // Сайт проектов Фонда Развития Интернет. URL: http://www.detionline.com/ (дата обращения 20.05.2025)

6. Двенадцать правил «цифровой гигиены» [Электронный ресурс] // Busines Daily: электронный деловой журнал. URL: https://prclub.spb.ru/2021/03/22/12-pravil-cifrovojgigieny/ (дата обращения 14.05.2025)
7. Двенадцать шагов к цифровой грамотности для взрослых и детей [Электронный ресурс] // АНО «Цифровая экономика»: сайт. URL: https://digital-likbez.datalesson.ru (дата обращения 14.05.2025)
8. Информационная безопасность в сети Интернет [Электронный ресурс] // Ульяновское региональное отделение Общероссийской общественной организации «Ассоциация юристов России»: сайт. URL: https://ulgov.ru/docs/20200203-brochura.pdf (дата обращения 16.05.2025)
9. Как отличить фейковый аккаунт ВКонтакте от настоящего [Электронный ресурс] // Модно и просто: статья во ВКонтакте. URL: https://vk.com/@76withlove-kak-otlichit-feikovyiakkaunt-vkontakte-ot-nastoyaschego (дата обращения 15.05.2025)
10. Методы и технологии защиты от вредоносных программ [Электронный ресурс] // Лаборатория Касперского: электронная энциклопедия URL: https://encyclopedia.kaspersky.ru/knowledge/malware-protection-methods-and-techniques/(дата обращения 11.05.2025)
11. Правила пользования Сайтом ВКонтакте [Электронный ресурс] // ВКонтакте.Справка: сайт. URL: https://vk.com/terms (дата обращения 20.05.2025)
12. Рекомендации по безопасному использованию сети Интернет [Электронный ресурс] // Безопасность пользователей сети Интернет: сайт. URL: https://safe-surf.ru/usersof/article/558561/ (дата обращения 12.05.2025).
13. Типы лицензий [Электронный ресурс] // Screenlifer: сайт. URL: https://screenlifer.com/tools/stat-guru-avtorskogo-prava-tipy-licenzij-na-audio-i-video/(дата обращения 19.05.2025)
14. Уроки Цифры [Электронный ресурс] // Урок Цифры - всероссийский образовательный проект в сфере информационных технологий: сайт. URL: урокцифры.рф (дата обращения 15.05.2025)
15. Условия размещения контента на RuTube [Электронный ресурс] // RuTube.Справка: сайт. URL: https://rutube.ru/info/content/ (дата обращения 17.05.2025)

4.2. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео-аудиовизуальные средства обучения. Наличие доступа педагогических работников и слушателей к информационно-телекоммуникационной сети интернет, оснащение компьютерным оборудованием: веб-камерой, аудиоколонками и (или) наушниками. Функционирующий интернет-портал с разработанным специализированным разделом, на базе которого реализуется обучение с использованием дистанционных образовательных технологий. В специализированном разделе интернет-портала размещаются лекционные материалы, материалы практических и самостоятельных работ, оценочные материалы согласно разработанной программе повышения квалификации.