**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН**
**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ ДАГЕСТАН**
**«ДАГЕСТАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»**

***УТВЕРЖДАЮ:***
***Ректор ГБУ ДПО РД «ДИРО»***
***_____Г.А. Ахмедова***
***«__30__» ____12_____2022г.***

# ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
**(повышения квалификации)**
# «ПЛАНИРОВАНИЕ И ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ»

**(18 часов)**

**Разработчик программы:**
Дибиров М.Д., учитель информатики
и ИКТ МБОУ «Каспийская гимназия №11»

**Махачкала, - 2022**

# ЛИСТ СОГЛАСОВАНИЯ

**Проректор по учебно-методической и научной работе:** _____/Курбанов А.Д./
*подпись* *Ф.И.О.*

**Руководитель структурного подразделения:** _____/ Омарова З.К./
*подпись* *Ф.И.О.*

**Руководитель учебно-методического управления:** _____/Эльдарушева М.Д./
*подпись* *Ф.И.О.*

**Рецензенты:**

1.Гасанова З.А., зам. заведующего кафедрой «Информационные технологии и информационная безопасность» ГАОУ ВО «ДГУНХ»;
2.Алиева С.М., почетный работник воспитания и просвещения РФ, учитель высшей категории, зам. директора по ИТ МБООУ «СОШ №6» им. Омарова М.О. г. Каспийск

**Программа утверждена на заседании учебно-методического совета ДИРО**

**Протокол №** 9 **от** «29» 12 2022г.

**Председатель УМС:** _____ /Далгатов Х.Г./
*подпись* *Ф.И.О.*

## Раздел 1. Характеристика программы

**Цель реализации программы –** совершенствование компетенций слушателей в области информационной безопасности и защиты детей и подростков от деструктивных сетевых воздействий.

### 1.1. Планируемые результаты обучения:

| Трудовая функция | Трудовое действие | Знать | Уметь |
|---|---|---|---|
| Общепедагогическая функция. Обучение. | Формирование навыков,связанных с информационно-коммуникационными технологиями | - основные методы противодействия деструктивным сетевым информационным воздействиям на обучающихся;<br>-законы и иные нормативные правовые акты по использованию ресурсов Интернет в образовательном процессе;<br>- основы психодидактики, поликультурного образования, закономерностей поведения в социальных сетях. | -организовать систему организационно-технических мер по защите информации, в том числе, персональных данных в информационных системах, включая электронные дневники и электронные журналы успеваемости;<br>-осуществлять эффективное противодействие деструктивным сетевым информационным воздействиям на обучающихся.<br>разрабатывать и реализовывать программы развития образовательной организации в целях создания безопасной и комфортной образовательной среды;<br>-формировать навыки, связанные с информационно-коммуникационными технологиями (далее – ИКТ);<br>- регулировать поведение обучающихся для обеспечения безопасной образовательной среды. |

| | | | |
|---|---|---|---|
| Воспитательная деятельность | Использование конструктивных воспитательных усилий родителей (законных представителей) обучающихся, помощь семье в решении вопросов воспитания ребенка. Регулирование поведения обучающихся для обеспечения безопасной образовательной среды | -основы психодидактики, поликультурного образования, закономерностей поведения в социальных сетях. | -регулировать поведение обучающихся для обеспечения безопасной образовательной среды;<br>-формировать у обучающихся культуру здорового и безопасного образа жизни;<br>-формировать толерантность и навыки поведения в изменяющейся поликультурной среде;<br>-использовать конструктивные воспитательные усилия родителей (законных представителей) обучающихся, осуществлять помощь семье в решении вопросов воспитания ребенка. |

**1.3. Категория слушателей:** педагогические и руководящие кадры образовательных организаций.

**1.4. Форма обучения** – очная с использованием дистанционных образовательных технологий.

**1.5. Срок освоения программы:** 18ч.

## Раздел 2. Содержание программы

### 2.1 Учебный (тематический) план

| № п/п | Наименование разделов (модулей) и тем | Всего часов | В том числе по видам занятий (час) | | | | | Форма контроля |
|---|---|---|---|---|---|---|---|---|
| | | | ЛЗ | | ПЗ | | СР | |
| | | | очно | дист | очно | дист | | |
| 1. | Входная диагностическая работа | **1** | | | | 1 | | **тестирование** |
| **Модуль 1. Основы информационной безопасности и нормативно-правовая база использования ресурсов интернет в образовательном процессе ( 8 ч.)** | | | | | | | | |
| 1.1 | Нормативно-правовая база и организация безопасного использования электронных образовательных ресурсов. Правовое обеспечение информационной безопасности образовательной среды | **2** | 1 | | | | 1 | |
| 1.2 | Обеспечение безопасности персональных данных обучающихся и педагогов | **2** | 2 | | | | | |
| 1.3 | Особенности взаимодействия обучающихся и педагогов образовательной организации в условиях информационной безопасности | **2** | | | 2 | | | |
| 1.4 | Основные методы выявления и создание контент-фильтрации деструктивных информационных воздействий в сети Интернет. Способы защиты от негативной информации в Интернете | **2** | 2 | | | | | |
| | **Итого по модулю № 1:** | **8** | **5** | | **2** | | **1** | |
| **Модуль 2. Угрозы информационной безопасности. (4ч.)** | | | | | | | | |
| 2.1 | Общее понятие. Причины и источники угроз информационной безопасности. Виды и классификация угроз информационной безопасности | **2** | 1 | | | | 1 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2 | Современные технологии обеспечения информационной безопасности | **2** | | | **2** | | | |
| | **Итого по модулю № 2:** | **4** | **1** | | **2** | | **1** | |
| **Модуль 3. Информационная культура родителей как фактор обеспечения информационной безопасности детей в сети Интернет. (4 ч. )** | | | | | | | | |
| 3.1 | Информационное просвещение родителей (законных представителей) о возможности защиты детей от информации, причиняющей вред их здоровью и развитию | **2** | 1 | | | | 1 | |
| 3.2 | Опасности и виды информационных угроз для детей (виды манипулятивных воздействий на детей и подростков в сети Интернет) | **2** | 1 | | 1 | | | |
| | **Итого по модулю № 3:** | **4** | **2** | | **1** | | **1** | |
| | Итоговая аттестация | **1** | | | | **1** | | **тестирование** |
| | **ИТОГО** | **18** | **8** | | **5** | **2** | **3** | |

**2.2. Рабочая программа (содержание)**

**Входная диагностическая работа** (тестирование **-1 час)**

Практическое занятие. Выполнение теста. Диагностика базовой подготовки в области информационной безопасности и защиты персональных данных.

**Модуль 1. Основы информационной безопасности и нормативно-правовая база использования ресурсов интернет в образовательном процессе (8ч.)**

**1.1. Нормативно-правовая база и организация безопасного использования электронных образовательных ресурсов. Правовое обеспечение информационной безопасности образовательной среды (лекция-1 час, самостоятельная работа 1 ч).**

Лекция. Нормативно-правовая база применения дистанционных образовательных технологий и электронного обучения. Нормативно-правовое регулирование применения ресурсов «Интернет» для обучения и воспитания. Организация безопасной электронной образовательной среды. Требования к сайтам образовательных организаций.

Самостоятельная работа. Проверить свой школьный сайт на соответствие новым требованиям ИБ.

**1.2. Обеспечение безопасности персональных данных обучающихся и педагогов (лекция- 2 часа).**

Лекция. Анализ нормативно-правовых материалов, содержащих требования обеспечения информационной безопасности в образовательной организации. Определение модели угроз безопасности информации. Разработка системы организационно-технических мер по защите информации. Разграничение доступа к данным. Резервное копирование. Нормативные требования к комплексным системам защиты компьютерных сетей от вирусов и вредоносных программ.

Организация системы ограничения обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Технологии организации системы ограничения обучающихся к негативной информации. Формы организации системы ограничения обучающихся к негативной информации.

**1.3. Особенности взаимодействия обучающихся и педагогов образовательной организации в условиях информационной безопасности (практ. – 2 часа).**

Практическое занятие. Практические особенности эффективного и безопасного использования систем и технологий дистанционного обучения. Дидактические возможности цифровых образовательных ресурсов. Показатели и критерии качества образования и эффективности образовательного процесса в электронной сетевой среде.

Условия создания безопасной развивающей информационной среды для детей и подростков. Исследования особенностей информационной социализации детей и подростков, эффекты воздействия информационной продукции на психическое здоровье, развитие и эмоциональное благополучие детей и подростков.

**1.4. Основные методы выявления и создание контент-фильтрации деструктивных информационных воздействий в сети Интернет. Способы защиты от негативной информации в Интернете (лекция -2 часа).**

Лекция. Основные требования законодательства РФ к методам и способам обработки и защиты персональных данных обучающихся и их законных представителей. Требования законодательства РФ к организации обработке, хранению и доступа к персональным данным граждан. Методы разграничения доступа к персональным данным. Уведомление о функционировании систем обработки персональных данных. Требования к защите персональных данных различных категорий.

Создание эффективной системы защиты персональных данных в образовательной организации. Реализация основных требований к защите персональных данных работников образовательной организации. Согласия на обработку персональных данных. Типичные нарушения при обработке персональных данных педагогов, вспомогательного персонала и обучающихся.

**Модуль 2. Угрозы информационной безопасности (4ч)**

**2.1. Общее понятие. Причины и источники угроз информационной безопасности. Виды и классификация угроз информационной безопасности (лекция – 1 часа, самостоятельная работа -1 ч).**

Лекция. Информационная безопасность. Основные источники угроз информационной безопасности. Примеры и эффекты негативного воздействия информационной продукции на психическое и психологическое развитие и здоровье ребенка. Методы и средства защиты информации. Управление доступом.

Самостоятельная работа. Анализ и обсуждение информационных угроз личности. Источники и особенности угроз: кибер-слежка, онлайн мошенничество, поддельные письма, фишинг, фальшивые сайты.

**2.2. Современные технологии обеспечения информационной безопасности (практическое занятие -2 ч).**

Практическое занятие. Информационные угрозы, их виды, причины. Классификация угроз по различным критериям: угроза непосредственно информационной информации; компоненты, на которые нацелены угрозы; угрозы по способу осуществления; угрозы по расположению источника. Вредоносные программы, их виды. Компьютерные преступления, их виды. Современные технологии защиты информационных систем; уязвимость и отрицательные стороны технологий защиты информационных систем; применение технологий защиты информационных систем для пресечения действий возможных типов нарушителей и угроз; требования к технологиям информационной безопасности.

**Модуль 3. Информационная культура родителей как фактор обеспечения информационной безопасности детей в сети Интернет (2ч.)**

**3.1. Информационное просвещение родителей (законных представителей) о возможности защиты детей от информации, причиняющей вред их здоровью и развитию (лекция -1 час, самостоятельная работа -1 ч).**

Лекция. Уроки медиа-безопасности для родителей (законных представителей) обучающихся: информирование родителей о видах информации, способной причинить вред здоровью и развитию несовершеннолетних; о способах незаконного распространения информации в сетях интернет и мобильной связи; о международных принципах и нормах, регулирующих вопросы информационной безопасности несовершеннолетних; о способах защиты от противоправных и

иных общественно-опасных посягательств в информационно-телекоммуникационных сетях.

Информационный поток: позитивное и негативное влияние. Актуальность проблемы исследования рисков информационного потока, поступающего из сети Интернет. Информационная безопасность ребенка как состояние защищенности детей, при котором отсутствует, риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Самостоятельная работа. Анализ информационных угроз сети интернет для детей и подростков. Проблемы информационных угроз сети Интернет для детей и подростков. Разработка «Правил использования информации из интернет-ресурса с целью обеспечения информационной безопасности» для родителей /для детей и подростков.

**3.2. Опасности и виды информационных угроз для детей (виды манипулятивных воздействий на детей и подростков в сети Интернет) (лекция –1 час, практическое занятие-1 ч).**

Лекция. Формирование основных правил безопасного использования Интернет-ресурсов. Виды деструктивных информационных воздействий в сети Интернет на детей и подростков: социальные вирусы, информационные вбросы, моббинг, буллинг, троллинг; искажение истории, причин и следствий социальных процессов и явлений; навязывание ложных ценностей; русофобия; пропаганда экстремизма и терроризма; асоциальные группы в социальных сетях; компьютерная преступность. Анализ основных видов, особенностей и психологических механизмов деструктивных информационных воздействий в сети Интернет.

Практическое занятие. Анализ основных видов деструктивных информационных воздействий в сети Интернет. Проанализировать особенности и психологические механизмы их воздействия на детей и подростков. Анализ основных психологических механизмов манипулятивных воздействий.

**4. Итоговая аттестация** ( практическое занятие - 1 ч. ).

## Раздел 3. Формы аттестации и оценочные материалы

### Входной контроль

**Форма:** тестирование

**Описание, требования к выполнению:**

Входной контроль включает 25 тестовых заданий с выбором одного или нескольких правильных ответов. Время на выполнение - 1 час.

**Критерии оценивания:** Тестирование пройдено успешно, если правильно выполнено не менее 51% заданий

**Примеры заданий:**

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными субъектами информационной безопасности являются:**

- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

**3) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- Регламентированной
- Правовой
- Защищаемой

**4) Наиболее распространены угрозы информационной безопасности корпоративной системы:**

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

**5) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

- Владелец сети
- Администратор сети
- Пользователь сети

**Итоговая аттестация**

**Форма:** тестирование

**Описание, требования к выполнению:**

Итоговая аттестация проходит в формате тестирования, которое состоит из заданий по всем модулям программы. Результат итогового тестирования является критерием определения качества усвоения слушателями содержания программы. Тест состоит из 30 тестовых заданий на выбор правильного(-ных) ответа(-ов), каждый верный ответ оценивается в 1 балл. время выполнения - 1 час

**Критерии оценивания:**

Тестирование пройдено успешно, если правильно выполнено не менее 51% заданий

**Примеры заданий:**

**1) Утечкой информации в системе называется ситуация, характеризуемая:**

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

**2) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

- Целостность
- Доступность
- Актуальность

**3) Угроза информационной системе (компьютерной сети) – это:**

- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

**4) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:**

- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

**5) Политика безопасности в системе (сети) – это комплекс:**

- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

## Раздел 4. Организационно-педагогические условия реализации программы

### 4.1. Учебно-методическое и информационное обеспечение программы

**Нормативные документы**


1. Федеральный закон от 29 декабря 2012 г.№ 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 06.03.2006 № Э5-ФЗ (ред. от 31.12.2014) «О противодействии терроризму».
3. Федеральный закон от 29 декабря 2010 года № 436-ФЭ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 02.07.2021).
4. Федеральный закон «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» от 28.07.2012 №139-ФЗ.
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» с изменениями, вступившими в силу с 01.09.2015 г.
6. Федеральный закон от 21 июля 2014 года № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».
7. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с последними изменениями от 13 июля 2015 г. 264-ФЗ).
8. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".
9. Федеральный закон от 7 мая 2013 г. №99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона "О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных" и федерального закона "О персональных данных".
10. Постановление Правительства Российской Федерации от 19 августа 2015 года № 857 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных».
11. О национальных целях и стратегических задачах Российской Федерации на период до 2024 года: указ Президента РФ с изменениями на 21 июля 2020 года) Доступ из справ. -правовой системы «Гарант». Источник: https://base.garant.ru/71937200/ (дата обращения 03.04.2022);


**Основная литература**


1. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва: Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный

// Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 06.12.2022).
2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/450371 (дата обращения: 06.12.2022).
3. Долматов, А. В. Проблемы и особенности правового регулирования защиты персональных данных / А. В. Долматов, Е. А. Долматов // Юрист ВУЗа. – 2019. – № 5. – С. 13-23. – EDN IDVHYB. URL: https://www.elibrary.ru/item.asp?id=37416407 (дата обращения: 06.12.2022).

**Дополнительная литература**

1. Долматов А.В., Долматов Е.А. Особенности и проблемы правового регулирования защиты персональных данных // Вестник Санкт-Петербургской юридической академии. 2018. №3 (40). – СПб.: АНО ВО СПбЮА, С. 53 - 60.
2. Долматов А.В., Долматов Е.А., Долматов Д.А. Информационные технологии в образовательном процессе и науке. Учебное пособие /- СПб.: АНО ВО СПбЮА, 2018 - 184 с.
3. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449350 (дата обращения: 06.12.2022).
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449285 (дата обращения: 06.12.2022).

**Интернет-ресурсы.**

1.Портал персональных данных уполномоченного органа по защите прав субъектов персональных данных: Нормативно-правовая база https://pd.rkn.gov.ru/registerOffenders/legalacts/
2.Интернет-педсовет: -http://pedsovet.org/ .
3.Портал МИНОБР.ОРГ. http://www.minobr.org/ .
4.http://www.edu.ru/index.php «Российское образование» Федеральный портал.

5.http://eor.edu.ru Федеральный центр информационно-образовательных ресурсов. Единое окно доступа к электронным образовательным ресурсам всех уровней системы образования РФ.

### 4.2. Материально-технические условия реализации программы

#### 4.2.1. Технические средства обучения

ЦНППМПР располагает необходимой материально-технической базой, обеспечивающей эффективную реализацию дополнительной профессиональной программы повышения квалификации «Планирование и организация деятельности по обеспечению информационной безопасности обучающихся в образовательной организации».

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятий | Наименование оборудования, программного обеспечения |
|---|---|---|
| Лекторий -1,2 | лекция | Медиастена 3х3 (Цветной дисплей Samsung)<br>Моноблок iCL<br>Кафедра с сенсорным экраном и микрофоном<br>Акустичкская система Volta (многоканальный усилитель, профессиональная многоканальная беспроводная радиосистема с ручным динамическим микрофоном)<br>Панорамная камера<br>Портативный рекордер<br>Колонка |
| Медиатека | | Моноблок iCL<br>МФУ KYOCERA |
| Учебная аудитория 2,3 | Практические занятия, итоговое тестирование | Моноблок iCL<br>Принтер KYOCERA<br>Проектор Maxell<br>Экран для проектора Digis<br>Интерактивная панель Lumien<br>Интерактивный флипчарт<br>Интерактивная панель IQTouch |
| Коворкинг | Индивидуальные консультации | Монитор Samsung<br>Системный блок Lenovo<br>Принтер KYOCERA<br>МФУ KYOCERA<br>Интерактивная панель Lumien<br>Интерактивный флипчарт<br>Тележка для ноутбуков (SCHOOLLBOX)<br>Ноутбук Acer |