

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ
ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
РАБОТНИКОВ ОБРАЗОВАНИЯ РЕСПУБЛИКИ ИНГУШЕТИЯ»

«УТВЕРЖДАЮ»

Ректор ГБОУ ДПО «ИПК РО РИ»

И.Я. Мальсагова

2026 г.



*Дополнительная профессиональная программа
повышения квалификации*

**«Противодействие террористическим угрозам
в сети Интернет»**

Принята на заседании

Ученого совета

ГБОУ ДПО «ИПК РО РИ»

Протокол

от «24» апреля 2026 г.

№ 4

Назрань

2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Противодействие террористическим угрозам
в сети Интернет»

Объём: 16 академических часов

Форма обучения: очная с применением дистанционных образовательных технологий
(ДОТ)

Разработчик программы:
Проректор по НМР Абадиев А.М.

РАЗДЕЛ 1. ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Современность характеризуется профессиональной компетенцией учителей информатики и информационно-коммуникационные технологии в области распознавания, анализа и противодействия террористическим угрозам в информационно-телекоммуникационной сети Интернет, а также формирование системной квалификационной работы и трудоустройство в соответствии с требованиями трудового договора «Информатика» и «Информационные технологии» стандарта «Подготовка педагогической деятельности в сфере информатики» в области информатики, системы работы с информацией (распознавание, анализ, противодействие террористическим угрозам в сети Интернет).

Программа реализуется на дистанционных образовательных технологиях.

- освоение студентами в действующей информационной сети Интернет и области информатики и информационно-коммуникационные технологии в области распознавания, анализа и противодействия террористическим угрозам в сети Интернет;
- приобретение студентами навыков работы с информацией (распознавание, анализ, противодействие террористическим угрозам в сети Интернет);
- формирование системной квалификационной работы и трудоустройство в соответствии с требованиями трудового договора «Информатика» и «Информационные технологии» стандарта «Подготовка педагогической деятельности в сфере информатики» в области информатики, системы работы с информацией (распознавание, анализ, противодействие террористическим угрозам в сети Интернет).

Программа реализуется на дистанционных образовательных технологиях. Программа реализуется на дистанционных образовательных технологиях. Программа реализуется на дистанционных образовательных технологиях. Программа реализуется на дистанционных образовательных технологиях. Программа реализуется на дистанционных образовательных технологиях.

СОДЕРЖАНИЕ ПРОГРАММЫ

Раздел 1. Характеристика программы

- 1.1. Цель реализации программы
- 1.2. Планируемые результаты обучения
- 1.3. Категория обучающихся
- 1.4. Форма обучения
- 1.5. Срок освоения программы

Раздел 2. Содержание программы

- 2.1. Учебный (тематический) план
- 2.2. Календарный учебный график
- 2.3. Рабочая программа (содержание по темам)

Раздел 3. Формы аттестации и оценочные материалы

- 3.1. Входной контроль
- 3.2. Текущий и промежуточный контроль
- 3.3. Итоговая аттестация

Раздел 4. Организационно-педагогические условия реализации программы

- 4.1. Учебно-методическое обеспечение
- 4.2. Материально-технические условия

РАЗДЕЛ 1. ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Совершенствование профессиональной компетенции учителей информатики и информационно-коммуникационных технологий в области распознавания, анализа и противодействия террористическим угрозам в информационно-телекоммуникационной сети Интернет, а также организации системной профилактической работы с обучающимися в соответствии с требованиями трудовой функции «**Воспитательная деятельность**» профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», утвержденного Приказом Минтруда России от 18.10.2013 № 544н.

Программа направлена на достижение следующих **задач**:

- ознакомить слушателей с действующей нормативно-правовой базой в сфере противодействия терроризму и экстремизму в сети Интернет;
- сформировать системное понимание механизмов и инструментов распространения террористической идеологии в цифровой среде;
- обучить практическим методам идентификации и верификации деструктивного контента в социальных сетях, мессенджерах и иных интернет-ресурсах;
- выработать навыки организации профилактических мероприятий с учётом специфики педагогической деятельности учителя информатики;
- сформировать готовность к оперативному реагированию на факты обнаружения террористического контента и алгоритм взаимодействия с уполномоченными органами.

1.2. Планируемые результаты обучения

Планируемые результаты обучения сформированы на основе требований профессионального стандарта «Педагог» (Приказ Минтруда России от 18.10.2013 № 544н), трудовых функций «Воспитательная деятельность» (код В/02.6) и «Развивающая деятельность» (код С/02.6).

Трудовая функция (код)	Трудовое действие	Знать	Уметь
Воспитательная деятельность (В/02.6)	Разработка и реализация воспитательных программ, в том числе в части профилактики правонарушений, асоциального и деструктивного поведения обучающихся	Основные положения федерального законодательства в сфере противодействия терроризму и экстремизму в информационном пространстве (ФЗ № 35-ФЗ, № 114-ФЗ, № 149-ФЗ); понятийный аппарат в сфере антитеррористической деятельности	Разрабатывать методические сценарии профилактических уроков и внеклассных мероприятий по теме противодействия террористическим угрозам в сети Интернет для обучающихся 5–11 классов
Воспитательная деятельность (В/02.6)	Формирование толерантности и навыков поведения в изменяющейся поликультурной среде; применение инструментария и методов диагностики	Виды и типологию террористических угроз в сети Интернет (вербовка, пропаганда, финансирование, координация); механизмы вербовки и радикализации молодёжи через цифровые платформы	Идентифицировать признаки террористического и экстремистского контента в открытых источниках сети Интернет (социальные сети, мессенджеры, форумы, видеохостинги, игровые платформы)
Воспитательная деятельность (В/02.6)	Создание детско-взрослых общностей обучающихся с их родителями (законными представителями); формирование нравственной атмосферы образовательной организации	Психологические механизмы воздействия экстремистских организаций на молодёжную аудиторию через цифровые платформы; факторы риска и признаки вовлечённости обучающихся в деструктивные сообщества	Применять инструменты верификации информации и проверки достоверности цифровых материалов с целью оценки их соответствия нормам законодательства
Воспитательная деятельность (В/02.6)	Общение с детьми, признание их достоинства; помощь в сознательном регулировании поведения для обеспечения	Алгоритм взаимодействия педагогических работников с правоохранительными органами, Роскомнадзором и Генеральной	Использовать официальные каналы и платформы для подачи обращений о деструктивном контенте (Роскомнадзор, Генеральная прокуратура)

	безопасной образовательной среды	прокуратурой РФ при обнаружении деструктивного контента	РФ, «Стоп-Контент», НЦБТИ МВД России)
Развивающая деятельность (С/02.6)	Выявление в ходе наблюдения поведенческих и личностных проблем обучающихся, связанных с особенностями их развития	Содержание, методику и инструментарий организации профилактических мероприятий в образовательной организации по противодействию вовлечению обучающихся в деструктивные интернет-сообщества	Консультировать обучающихся и родителей (законных представителей) по вопросам безопасного поведения в информационно-телекоммуникационной среде; анализировать цифровую активность обучающихся с целью выявления признаков вовлечённости в деструктивные сообщества

1.3. Категория обучающихся

Должность	Учитель информатики и информационно-коммуникационных технологий
Квалификационные требования	Высшее образование или среднее профессиональное образование по направлениям подготовки «Образование и педагогические науки», «Информатика и вычислительная техника», «Информационная безопасность» либо иное образование и дополнительное профессиональное образование по направлению деятельности
Место работы	Образовательные организации общего образования Республики Ингушетия
Предварительные требования к знаниям	Предварительное знание темы программы не является обязательным условием допуска к обучению
Технические требования к слушателям	Наличие персонального компьютера (ноутбука, планшета) с доступом в сеть Интернет (скорость не менее 10 Мбит/с) для участия в занятиях с применением ДОТ

1.4. Форма обучения

Очная с применением дистанционных образовательных технологий (ДОТ).

Дистанционные образовательные технологии реализуются посредством:

- системы видеоконференц-связи (МАХ, VK Видеозвонки или аналогичная отечественная платформа);
- системы управления обучением (LMS) ГБОУ ДПО ИПК РО РИ на базе платформы Moodle (далее — ЭИОС ИПК);
- электронного учебного кабинета программы в ЭИОС ИПК, где размещаются учебно-методические материалы, задания, форумы обсуждения, форма загрузки аттестационной работы.

1.5. Срок освоения программы

16 академических часов (1 академический час = 45 минут). Рекомендуемый режим освоения: **2 учебных дня** по 8 академических часов. Допускается иной режим по согласованию с образовательной организацией, направляющей слушателей.

РАЗДЕЛ 2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный (тематический) план

№	Наименование разделов / модулей и тем	Всего часов	Лекции (ч.)	Интерактивные занятия / практикумы (ч.)	Самостоятельная работа (ч.)	Форма контроля
МОДУЛЬ 1. Нормативно-правовые и концептуальные основы противодействия терроризму и экстремизму						
1.1	Система законодательного регулирования в сфере противодействия терроризму и экстремизму в информационном пространстве	2	1	—	1	Входное тестирование
1.2	Правовое положение педагогического работника в системе профилактики терроризма и экстремизма. Ответственность за непринятие мер	2	—	1	1	Текущий контроль (дискуссия / опрос)
Итого по модулю 1		4	1	1	2	
МОДУЛЬ 2. Террористические угрозы в цифровой среде: типология, механизмы, признаки						
2.1	Виды террористических угроз в сети Интернет. Механизмы вербовки, пропаганды и радикализации молодёжи через цифровые платформы	2	1	—	1	Текущий контроль (тест в ЭИОС ИПК)

2.2	Критерии идентификации деструктивного и экстремистского контента. Работа с чек-листом	2	—	1	1	Текущий контроль (кейс-задание)
2.3	Уязвимые группы обучающихся. Признаки вовлечённости в деструктивные сообщества. Региональная специфика Республики Ингушетия	1	—	1	—	Текущий контроль (устный опрос)
Итого по модулю 2		5	1	2	2	
МОДУЛЬ 3. Практические инструменты противодействия. Взаимодействие с уполномоченными органами						
3.1	Цифровые инструменты верификации информации. Алгоритм действий педагога при обнаружении угрозы	2	—	1	1	Текущий контроль (практическая работа в ЭИОС ИПК)
3.2	Взаимодействие с уполномоченными органами. Использование официальных платформ. Документирование фактов	2	—	2	—	Промежуточная аттестация (зачёт по модулям 1–3)
Итого по модулю 3		4	—	3	1	
МОДУЛЬ 4. Педагогическая профилактика и методическая работа						
4.1	Методика организации профилактических мероприятий в образовательной организации. Возрастная дифференциация содержания	1	—	1	—	Текущий контроль (устный опрос)
4.2	Разработка методического сценария урока /	1	—	1	—	Текущий контроль

	внеклассного мероприятия. Консультирование обучающихся и родителей по вопросам цифровой безопасности					(черновик сценария)
Итого по модулю 4		2	—	2	—	
ИТОГОВАЯ АТТЕСТАЦИЯ						
—	Защита практического проекта (методического сценария урока / внеклассного мероприятия)	1	—	—	—	Защита проекта (аттестационная комиссия)
ИТОГО по программе		16	2	8	5	Удостоверение о ПК
<i>в том числе: аудиторные занятия</i>		10	2 (20%)	8 (80%)	—	
<i>из них с применением ДОТ</i>		6	—	5	1	

2.2. Календарный учебный график

День обучения	Время	Тема / Содержание	Форма проведения	Аудит. / ДОТ
ДЕНЬ 1				
День 1	09:00–09:45	Тема 1.1. Система законодательного регулирования (лекция). Входное тестирование (15 мин.)	Лекция + тестирование	Аудитория
	09:45–10:00	<i>Перерыв</i>		
	10:00–10:45	Тема 1.2. Правовое положение педагога. Ответственность. Интерактивная дискуссия	Интерактивное занятие	Аудитория
	10:45–11:00	<i>Перерыв</i>		
	11:00–12:30	Самостоятельная работа: изучение нормативных актов в ЭИОС ИПК (задание 1)	Самостоятельная работа	ДОТ / ЭИОС
	12:30–13:15	<i>Обед</i>		

	13:15–14:00	Тема 2.1. Виды угроз. Механизмы вербовки и радикализации (лекция)	Лекция	Аудитория
	14:00–14:15	<i>Перерыв</i>		
День 1 (продолжение)	14:15–15:00	Тема 2.2. Критерии идентификации контента. Работа с чек-листом (практикум в малых группах)	Интерактивное занятие	Аудитория / ДОТ
День 1 (продолжение)	15:00–15:15	<i>Перерыв</i>		
День 1 (продолжение)	15:15–16:00	Тема 2.3. Уязвимые группы. Признаки вовлечённости. Региональная специфика (групповая работа)	Интерактивное занятие	Аудитория
День 1 (продолжение)	16:00–17:30	Самостоятельная работа: выполнение кейс-задания по теме 2.2 (задание 2) в ЭИОС ИПК	Самостоятельная работа	ДОТ / ЭИОС
ДЕНЬ 2				
День 2	09:00–09:45	Тема 3.1. Цифровые инструменты верификации информации. Алгоритм действий педагога (практикум-демонстрация)	Интерактивное занятие	ДОТ
	09:45–10:00	<i>Перерыв</i>		
	10:00–11:30	Тема 3.1 (продолжение). Самостоятельная практическая работа: верификация учебного кейса в ЭИОС ИПК (задание 4)	Практическая работа	ДОТ / ЭИОС
	11:30–11:45	<i>Перерыв</i>		
	11:45–13:15	Тема 3.2. Взаимодействие с уполномоченными органами. Симуляция подачи обращения. Документирование (практикум)	Интерактивное занятие	ДОТ
	13:15–14:00	<i>Обед</i>		
	14:00–14:30	Промежуточная аттестация: зачёт по модулям 1–3 (тестирование в ЭИОС ИПК, 15 вопросов, 20 минут)	Тестирование (зачёт)	ДОТ / ЭИОС

	14:30–14:45	Перерыв		
	14:45–15:30	Тема 4.1. Методика организации профилактических мероприятий. Возрастная дифференциация (практикум)	Интерактивное занятие	Аудитория
	15:30–15:45	Перерыв		
	15:45–16:30	Тема 4.2. Разработка методического сценария. Индивидуальная консультация (мастерская)	Интерактивное занятие	Аудитория
	16:30–16:45	Перерыв		
	16:45–17:30	Итоговая аттестация: защита практического проекта (методического сценария)	Защита проекта (комиссия)	Аудитория / ДОТ

2.3. Рабочая программа (содержание по темам)

МОДУЛЬ 1. Нормативно-правовые и концептуальные основы противодействия терроризму и экстремизму

Тема 1.1. Система законодательного регулирования в сфере противодействия терроризму и экстремизму в информационном пространстве

Краткое содержание (тезисы):

- **1. Конституционные основы** — ст. 13, 29, 55 Конституции РФ как правовая база ограничений в сфере информации; принцип недопустимости пропаганды, возбуждающей ненависть.
- **2. Федеральный закон № 35-ФЗ «О противодействии терроризму»** — понятийный аппарат (терроризм, террористическая деятельность, террористический акт); субъекты противодействия; роль НАК и его региональных структур в Республике Ингушетия.
- **3. Федеральный закон № 114-ФЗ «О противодействии экстремистской деятельности»** — понятие экстремистской деятельности; экстремистские материалы; порядок признания материалов экстремистскими; Федеральный список экстремистских материалов Минюста России.
- **4. Федеральный закон № 149-ФЗ «Об информации...»** — основания для ограничения доступа к сайтам; порядок внесения в реестры Роскомнадзора; ответственность за распространение запрещённой информации.
- **5. Уголовная ответственность** — составы преступлений: ст. 205–205.6, 208, 280, 280.1, 280.3, 282–282.3 УК РФ.
- **6. Административная ответственность** — ст. 20.3, 20.3.2, 20.29 КоАП РФ.
- **7. Стратегические документы** — Стратегия национальной безопасности РФ (Указ № 400 от 02.07.2021); Стратегия противодействия экстремизму до 2025 г. (Указ № 344); Комплексный план НАК на 2024–2028 гг.; Концепция информационной безопасности детей (Распоряжение Правительства РФ № 1105-р от 28.04.2023).

Самостоятельная работа (1 ч.): в ЭИОС ИПК слушатели изучают тексты ключевых нормативных актов и выполняют **задание 1** — заполнение сравнительной таблицы «Понятие терроризма / экстремизма: разграничение по российскому законодательству» (загрузка в ЭИОС ИПК).

Формируемые результаты:

- **Знать:** основные положения федерального законодательства в сфере противодействия терроризму и экстремизму (ФЗ № 35-ФЗ, № 114-ФЗ, № 149-ФЗ); понятийный аппарат.
- **Уметь:** использовать официальные ресурсы для работы с нормативной базой (КонсультантПлюс, pravo.gov.ru).

Тема 1.2. Правовое положение педагогического работника в системе профилактики.

Ответственность за непринятие мер

Вид занятия: интерактивное занятие (дискуссия с анализом ситуаций), очная форма, 1 ч. + самостоятельная работа (ЭИОС ИПК), 1 ч.

Краткое содержание (тезисы):

- **1. Обязанности педагогического работника** по ФЗ № 273-ФЗ «Об образовании» (ст. 48): обязанность заботиться о нравственном воспитании обучающихся; недопустимость пропаганды деструктивных взглядов.
- **2. Профессиональный стандарт «Педагог»** — трудовая функция «Воспитательная деятельность» (В/02.6): трудовое действие «Разработка и реализация воспитательных программ, в том числе в части профилактики правонарушений, асоциального и деструктивного поведения обучающихся».
- **3. Система субъектов профилактики в образовательной организации** — классный руководитель, педагог-психолог, социальный педагог, заместитель директора по ВР, учитель информатики как эксперт в сфере ИКТ.
- **4. Алгоритм взаимодействия внутри образовательной организации** при выявлении угрозы — от учителя к администрации, далее к уполномоченным органам.
- **5. Ответственность за непринятие мер** — разбор ситуационных кейсов: границы компетенции учителя; риски бездействия.
- **6. Интерактивная дискуссия** — кейс: «Учитель информатики обнаружил в браузерной истории школьного компьютера следы посещения ресурса из реестра Роскомнадзора. Каковы его действия?»

Самостоятельная работа (1 ч.): изучение методических рекомендаций Минпросвещения России по профилактике экстремизма в ОО (2023); фиксация в рабочем листе двух трудовых действий из должностной инструкции учителя информатики, связанных с профилактикой деструктивного поведения.

Формируемые результаты:

- **Знать:** алгоритм взаимодействия педагогических работников с правоохранительными органами при обнаружении деструктивного контента.
- **Уметь:** консультировать обучающихся и родителей по вопросам безопасного поведения в информационно-телекоммуникационной среде.

МОДУЛЬ 2. Террористические угрозы в цифровой среде: типология, механизмы, признаки

Тема 2.1. Виды террористических угроз в сети Интернет. Механизмы вербовки, пропаганды и радикализации молодёжи через цифровые платформы

Вид занятия: лекция (очная), 1 ч. + самостоятельная работа (ЭИОС ИПК), 1 ч.

Краткое содержание (тезисы):

- **1. Типология угроз в интернет-пространстве** — классификация: онлайн-вербовка, пропаганда и агитация, распространение экстремистских материалов, координация террористической деятельности, финансирование через криптовалюты. Соотношение понятий «терроризм» и «экстремизм» в цифровой среде.
- **2. Платформы и каналы** — мессенджеры (Telegram); социальные сети; видеохостинги; игровые платформы (Discord, Roblox, Steam) — особая значимость в контексте несовершеннолетней аудитории; тематические форумы.
- **3. Механизм радикализации («воронка вовлечения»)** — поэтапное рассмотрение: привлечение через «хайповый» контент → формирование доверия → изоляция от окружения → внедрение идеологии → мотивация к действию. Психологические приёмы: апелляция к социальной несправедливости, чувству принадлежности, героизации, религиозному долгу.
- **4. Запрещённые организации** — обзор перечня ФСБ России и решений судов о признании организаций террористическими; порядок актуализации перечня.
- **5. Региональный контекст** — актуальные угрозы для молодёжи СКФО; использование религиозной риторики в вербовочных материалах, ориентированных на регион.

Самостоятельная работа (1 ч.): задание 2 — составление схемы «Этапы вовлечения подростка в деструктивное сообщество» (загрузка в ЭИОС ИПК).

Формируемые результаты:

- **Знать:** виды и типологию террористических угроз в сети Интернет; психологические механизмы воздействия на молодёжную аудиторию через цифровые платформы.
- **Уметь:** анализировать цифровую активность обучающихся с целью своевременного выявления признаков вовлечённости в деструктивные сообщества.

Тема 2.2. Критерии идентификации деструктивного и экстремистского контента.

Работа с чек-листом

Вид занятия: интерактивное занятие (практикум в малых группах), очная форма с элементами ДОТ, 1 ч. + самостоятельная работа (ЭИОС ИПК), 1 ч.

Краткое содержание (тезисы):

- **1. Формальные критерии экстремистских материалов** — признаки в соответствии с законодательством: призывы к насилию; разжигание ненависти по религиозному / национальному признаку; пропаганда организаций из реестра; демонстрация символики запрещённых организаций. Использование Федерального списка экстремистских материалов Минюста России (minjust.gov.ru).
- **2. Содержательные признаки** — что анализировать: текстовый контент (лозунги, хэштеги, характерная лексика); визуальный контент (символика, образы);

аудиовизуальный контент; метаданные (анализ аккаунтов, история публикаций, связи).

- **3. Чек-лист идентификации** — представление чек-листа: 12 критериев-вопросов для оценки сомнительного интернет-материала.
- **4. Практикум «Анализ учебных кейсов»** — работа в малых группах (3–4 чел.); анализ 3 специально подготовленных обезличенных учебных кейсов с применением чек-листа; обсуждение результатов в общей группе.
- **5. Ограничения и риски** — что нельзя делать при подозрении на деструктивный контент: распространять, пересылать, публично обсуждать с обучающимися без предварительной подготовки.

Самостоятельная работа (1 ч.): задание 3 — анализ двух учебных кейсов из ЭИОС ИПК с применением чек-листа и заполнением формы отчёта (загрузка в ЭИОС ИПК).

Формируемые результаты:

- **Знать:** перечень запрещённых организаций; формальные и содержательные критерии идентификации деструктивного контента.
- **Уметь:** идентифицировать признаки террористического и экстремистского контента в открытых источниках сети Интернет.

Тема 2.3. Уязвимые группы обучающихся. Признаки вовлечённости. Региональная специфика Республики Ингушетия

Вид занятия: интерактивное занятие (групповая работа, брейнсторминг), очная форма, 1 ч.

Краткое содержание (тезисы):

- **1. Факторы риска** — психологические (низкая самооценка, поиск идентичности, подростковый кризис); социальные (изоляция, конфликты в семье, буллинг); информационные (низкий уровень медиаграмотности).
- **2. Поведенческие признаки вовлечённости** — что может заметить учитель информатики: изменение поведения на уроке; специфическая лексика; демонстрация символики; конфиденциальность при работе с устройствами.
- **3. Алгоритм реагирования при подозрении** — привлечение педагога-психолога; конфиденциальность информации; недопустимость прямого обвинения; взаимодействие с родителями.
- **4. Региональная специфика** — обсуждение в группе: актуальные угрозы для молодёжи Республики Ингушетия; культурные и конфессиональные особенности профилактической работы; обмен наблюдениями из практики.
- **5. Мини-брейнсторминг** — «Какие признаки вовлечённости вы как учитель информатики можете заметить первым?»

Формируемые результаты:

- **Знать:** психологические механизмы воздействия на молодёжную аудиторию; факторы риска и признаки вовлечённости.
- **Уметь:** анализировать цифровую активность обучающихся; консультировать обучающихся и родителей по вопросам безопасного поведения.

МОДУЛЬ 3. Практические инструменты противодействия. Взаимодействие с уполномоченными органами

Тема 3.1. Цифровые инструменты верификации информации. Алгоритм действий педагога при обнаружении угрозы

Вид занятия: интерактивное занятие (практикум-демонстрация + индивидуальная практическая работа), ДОТ, 1 ч. + самостоятельная работа, 1 ч.

Краткое содержание (тезисы):

- **1. Инструменты верификации** (демонстрация на экране): обратный поиск изображений — Яндекс.Картинки, TinEye; проверка домена — WHOIS, web.archive.org; анализ источника через поисковые системы; ресурсы верификации фактов — lapsha.media.
- **2. Проверка ресурсов через официальные реестры:** реестр Роскомнадзора (eais.rkn.gov.ru) — проверка конкретного URL; Федеральный список экстремистских материалов Минюста РФ; перечень террористических организаций ФСБ России.
- **3. Пошаговый алгоритм действий педагога:**
 - Шаг 1: зафиксировать (скриншот с адресной строкой и системным временем; URL; дата и время);
 - Шаг 2: Первичная оценка — применить чек-лист идентификации;
 - Шаг 3: Незамедлительный доклад администрации (директору / заместителю директора по ВР);
 - Шаг 4: Направление обращения в уполномоченные органы;
 - Шаг 5: при признаках вовлечённости обучающегося — подключение педагога-психолога, инспектора ПДН;
 - Шаг 6: Ведение документации о принятых мерах.

Самостоятельная работа (1 ч.): задание 4 — верификация предложенного учебного кейса с использованием изученных инструментов; заполнение формы отчёта в ЭИОС ИПК.

Формируемые результаты:

- **Знать:** алгоритм взаимодействия педагогических работников с правоохранительными органами; методы цифровой гигиены и кибербезопасности.
- **Уметь:** применять инструменты верификации информации; идентифицировать признаки деструктивного контента.

Тема 3.2. Взаимодействие с уполномоченными органами. Использование официальных платформ. Документирование фактов

Вид занятия: интерактивное занятие (практикум-симуляция), ДОТ, 2 ч. Промежуточная аттестация (зачёт по модулям 1–3).

Краткое содержание (тезисы):

- **1. Роскомнадзор: форма подачи обращений** — пошаговое руководство по rkn.gov.ru; требования к данным; сроки рассмотрения; типичные ошибки; правовые основания (ст. 15.1, 15.3, 15.6 ФЗ № 149-ФЗ).
- **2. Генеральная прокуратура РФ: интернет-приёмная** — форма обращения через erp.genproc.gov.ru; компетенция прокуратуры; требования к оформлению.
- **3. «Стоп-Контент» и горячие линии** — платформа stopcontentrf.ru; горячая линия Лиги безопасного интернета; НЦБТИ МВД России.

- **4. Правила документирования фактов** — скриншот с адресной строкой и системным временем; запись экрана; архивирование через web.archive.org; оформление докладной записки — разбор шаблона.
- **5. Практикум «Симуляция подачи обращения»** — заполнение формы обращения в Роскомнадзор на основе учебного кейса (без реальной отправки); заполнение шаблона докладной записки на имя директора; разбор ошибок.

Промежуточная аттестация (зачёт по модулям 1–3): тестирование в ЭИОС ИПК, 15 вопросов (10 закрытых + 5 открытых), 20 минут, пороговый балл — 10 из 15.

Формируемые результаты:

- **Знать:** алгоритм взаимодействия с правоохранительными органами и Роскомнадзором; официальные каналы блокировки контента.
- **Уметь:** использовать официальные каналы для подачи обращений о деструктивном контенте; документировать выявленные факты.

МОДУЛЬ 4. Педагогическая профилактика и методическая работа

Тема 4.1. Методика организации профилактических мероприятий в образовательной организации. Возрастная дифференциация содержания

Вид занятия: интерактивное занятие (практикум с анализом образцов), очная форма, 1 ч.

Краткое содержание (тезисы):

- **1. Принципы профилактической работы** — системность; возрастная адекватность; позитивная направленность (формирование ценностей, а не запугивание); вовлечённость обучающихся как субъектов; культурная чувствительность.
- **2. Возрастная дифференциация содержания:**
 - 5–6 класс (10–12 лет): базовые правила безопасного поведения в Сети, понятие «опасный контент», «надёжный взрослый»;
 - 7–8 класс (12–14 лет): механизмы манипуляции, критическое мышление, цифровая идентичность;
 - 9–11 класс (14–17 лет): правовая ответственность, механизм вербовки, алгоритм безопасного поведения, гражданская позиция.
- **3. Методические форматы** — проблемная беседа; анализ кейсов; дебаты; квест по цифровой безопасности; создание учебного контента самими школьниками; родительский всеобуч.
- **4. Структура методического сценария** — анализ образца-эталона: паспорт мероприятия, поэтапный план с хронометражем, методы и приёмы, практические задания, рефлексия, список источников.
- **5. Ресурсы для педагогов** — методические материалы Минпросвещения России, Лиги безопасного интернета, Роскомнадзора; образовательные платформы (edu.gov.ru, урокцифры.рф).

Формируемые результаты:

- **Знать:** содержание и методику проведения профилактических мероприятий в образовательной организации; принципы возрастной дифференциации содержания.
- **Уметь:** разрабатывать методические сценарии профилактических занятий с учётом возрастной специфики.

Тема 4.2. Разработка методического сценария. Консультирование обучающихся и родителей по вопросам цифровой безопасности
Вид занятия: интерактивное занятие (мастерская / индивидуальная работа с консультационной поддержкой), очная форма, 1 ч.

Краткое содержание (тезисы):

- **1. Медиаграмотность и критическое мышление** как долгосрочная профилактика — модель SIFT (Stop — Investigate the source — Find better coverage — Trace claims) в адаптации для российских школьников.
- **2. Работа с родителями** — форматы взаимодействия: родительское собрание; индивидуальная консультация; информационная рассылка. Типичные ошибки родителей в вопросах цифровой безопасности детей. Правовая ответственность родителей (ст. 63, 64 Семейного кодекса РФ).
- **3. Роль учителя информатики в системе профилактики** — уникальность позиции: эксперт в цифровой среде, консультант для коллег, обучающихся и родителей. Принцип «не навреди»: избегать чрезмерной драматизации, стигматизации.
- **4. Мастерская «Разработка методического сценария»** — индивидуальная работа по созданию итоговой аттестационной работы; консультационная поддержка преподавателя; взаимная проверка черновиков в парах.
- **5. Инструктаж по порядку итоговой аттестации** — требования к оформлению; порядок загрузки в ЭИОС ИПК; регламент защиты; критерии оценки.

Формируемые результаты:

- **Знать:** содержание и методику профилактических мероприятий; принципы формирования медиаграмотности обучающихся.
- **Уметь:** разрабатывать методические сценарии; консультировать обучающихся и родителей по вопросам безопасного поведения в информационно-телекоммуникационной среде.

РАЗДЕЛ 3. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

3.1. Входной контроль

Цель: определение исходного уровня знаний слушателей в области противодействия терроризму и экстремизму в сети Интернет для актуализации субъектного опыта и дифференциации подхода в процессе обучения.

Форма проведения	Тестирование в ЭИОС ИПК (при дистанционном выполнении) или на бумажных носителях (при очном проведении)
Время проведения	Начало Дня 1 (до начала лекции по теме 1.1), продолжительность — 15 минут
Количество вопросов	10 вопросов (8 закрытых с выбором ответа + 2 открытых)
Влияние на итоговую оценку	Результаты не влияют на итоговую оценку; используются преподавателем для корректировки акцентов в учебном процессе

Примеры заданий входного контроля:

Вопрос 1. Какой федеральный закон устанавливает основные понятия и меры в сфере противодействия терроризму в Российской Федерации?

- А) Федеральный закон от 25.07.2002 № 114-ФЗ
- Б) **Федеральный закон от 06.03.2006 № 35-ФЗ (верный ответ)**
- В) Федеральный закон от 27.07.2006 № 149-ФЗ
- Г) Федеральный закон от 29.12.2010 № 436-ФЗ

Вопрос 2. Укажите, какой орган ведёт Федеральный список экстремистских материалов в Российской Федерации:

- А) Федеральная служба безопасности (ФСБ России)
- Б) Роскомнадзор
- В) **Министерство юстиции Российской Федерации (верный ответ)**
- Г) Генеральная прокуратура Российской Федерации

Вопрос 3. К какой трудовой функции профессионального стандарта «Педагог» относится обязанность учителя осуществлять профилактику деструктивного поведения обучающихся?

- А) «Общепедагогическая функция. Обучение»
- Б) «Педагогическая деятельность по реализации программ начального общего образования»
- В) **«Воспитательная деятельность» (верный ответ)**
- Г) «Развивающая деятельность»

Вопрос 4 (открытый). Перечислите не менее трёх платформ или каналов в сети Интернет, которые могут использоваться для распространения экстремистского контента.

Вопрос 5. Что из перечисленного НЕ является признаком экстремистских материалов согласно российскому законодательству?

- А) Призывы к насилию по национальному признаку
- Б) Пропаганда деятельности запрещённых организаций
- В) **Критика решений органов государственной власти в официальных СМИ (верный ответ)**
- Г) Демонстрация символики запрещённых террористических организаций

3.2. Текущий и промежуточный контроль

Текущий контроль (по темам)

Тема	Форма текущего контроля	Краткое описание	Критерий зачёта
1.2	Устный опрос / дискуссия	Ответы на вопросы по ситуационным кейсам о правовом положении педагога; обоснованность позиции	Активное участие; корректное применение норм профстандарта и законодательства

2.1	Автоматизированный тест в ЭИОС ИПК (10 вопросов)	Проверка знаний о видах угроз и механизмах вербовки; проводится по завершении темы	Не менее 7 из 10 баллов
2.2	Кейс-задание (задание 3, ЭИОС ИПК)	Анализ двух учебных кейсов с применением чек-листа; заполнение формы отчёта; загрузка в ЭИОС ИПК	Выявлено не менее 3 из 5 признаков по каждому кейсу; обоснование представлено в полном объёме
2.3	Устный опрос (брейнсторминг)	Называние признаков вовлечённости обучающихся, которые может заметить учитель информатики	Группа называет не менее 5 конкретных признаков с обоснованием
3.1	Практическая работа (задание 4, ЭИОС ИПК)	Верификация учебного кейса с использованием изученных инструментов; заполнение формы отчёта	Верификация проведена по всем пунктам алгоритма; отчёт заполнен в полном объёме
4.2	Черновик методического сценария (взаимная проверка)	Представление черновика итоговой аттестационной работы; взаимная проверка в парах по установленным критериям	Наличие всех обязательных структурных элементов сценария (паспорт, план, задания, рефлексия)

Промежуточная аттестация (зачёт по модулям 1–3)

Форма	Тестирование в ЭИОС ИПК
Количество вопросов	15 (10 закрытых вопросов с выбором ответа + 5 открытых вопросов)
Время выполнения	20 минут
Пороговый балл	10 из 15 (67%)
При наборе менее 10 баллов	Предоставляется право пересдачи до начала итоговой аттестации

Примеры заданий промежуточной аттестации:

Задание 1 (открытый вопрос). Опишите пошаговый алгоритм действий учителя информатики, обнаружившего на школьном компьютере следы посещения ресурса с признаками экстремистского контента. Укажите не менее 5 шагов с указанием их содержания.

Задание 2. Через какой ресурс педагогический работник может подать обращение о выявленном деструктивном контенте непосредственно в Роскомнадзор?

А) pravo.gov.ru Б) minjust.gov.ru В) rkn.gov.ru (верный ответ) Г) edu.gov.ru

Задание 3 (открытый вопрос). Перечислите не менее 4 психологических или поведенческих признаков, которые могут свидетельствовать о вовлечённости обучающегося в деструктивное интернет-сообщество.

3.3. Итоговая аттестация

Форма итоговой аттестации	Защита практического проекта
Наименование аттестационной работы	Методический сценарий урока (внеклассного мероприятия) по теме противодействия террористическим угрозам в сети Интернет для обучающихся 7–11 классов
Объём текстовой части	Не менее 5 страниц (формат А4, Times New Roman 12 pt, интервал 1,5, поля стандартные) без учёта приложений
Срок загрузки работы в ЭИОС ИПК	Не позднее чем за 24 часа до защиты
Регламент защиты	Устное представление — 7–10 минут; вопросы комиссии — 5 минут; вынесение решения
Состав аттестационной комиссии	Председатель — заместитель директора ИПК РО РИ по УМР; преподаватель курса; методист кафедры ИКТ в образовании

Обязательные структурные элементы аттестационной работы:

- паспорт мероприятия (класс / возрастная группа, цель, задачи, планируемые результаты в формате «знать / уметь», оборудование и ресурсы);
- поэтапный план занятия с хронометражем (не менее 4 этапов: организационный, основной теоретический, практический, рефлексия);
- не менее 2 практических заданий / кейсов для обучающихся (составлены самостоятельно, не дублируют учебные материалы курса);
- описание применяемых методов и приёмов;
- раздел «Рефлексия»;
- список использованной литературы и нормативных источников (не менее 5 позиций, в том числе не менее 3 нормативных актов);
- учёт региональной специфики Республики Ингушетия — обязателен.

Критерии оценки итоговой аттестационной работы

№	Критерий оценки	Показатели	Макс. балл	Факт. балл
1	Соответствие содержания теме, цели и целевой аудитории (возрастная адекватность, учёт уровня цифровой грамотности обучающихся)	Полное / частичное / несоответствие	20	
2	Наличие и корректность нормативно-правового обоснования (ссылки на актуальные законодательные акты; использование не менее 3 нормативных источников)	Корректные / частично корректные / отсутствуют	15	
3	Методическая грамотность: структура занятия (цель, задачи, этапы, методы, рефлексия), логика изложения, соответствие методических приёмов возрасту	Высокая / средняя / низкая	20	

4	Практическая применимость: наличие не менее 2 кейсов / заданий, их содержательная ценность и выполнимость в условиях реального класса	Разнообразные / единичные / отсутствуют	15	
5	Использование цифровых инструментов и ресурсов в методическом сценарии (платформы, сервисы, интерактивные элементы)	Эффективное / формальное / отсутствует	10	
6	Учёт региональной специфики Республики Ингушетия (социокультурный контекст, актуальные угрозы региона, конфессиональные особенности)	Учтена / частично / не учтена	10	
7	Качество презентации и защиты: ясность изложения, структурированность, уверенность, полнота и корректность ответов на вопросы комиссии	Высокое / среднее / низкое	10	
ИТОГО			100	

Шкала перевода баллов в оценку

Набранные баллы	Оценка	Решение
90–100	Отлично	Работа выполнена на высоком профессиональном уровне, все критерии соблюдены в полной мере. Удостоверение выдаётся.
75–89	Хорошо	Работа выполнена на достаточном уровне, большинство критериев соблюдены. Удостоверение выдаётся.
60–74	Удовлетворительно	Работа выполнена на базовом уровне, имеются существенные недостатки. Удостоверение выдаётся с рекомендацией по доработке материала.
Менее 60	Неудовлетворительно	Работа не соответствует требованиям. Назначается повторная аттестация. Удостоверение не выдаётся.

РАЗДЕЛ 4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Учебно-методическое обеспечение

4.1.1. Нормативные правовые акты

№	Наименование документа	Реквизиты
1	Конституция Российской Федерации	Принята 12.12.1993 (с изм. от 04.10.2022)
2	Федеральный закон «О противодействии терроризму»	от 06.03.2006 № 35-ФЗ
3	Федеральный закон «О противодействии экстремистской деятельности»	от 25.07.2002 № 114-ФЗ
4	Федеральный закон «Об информации, информационных технологиях и о защите информации»	от 27.07.2006 № 149-ФЗ

5	Федеральный закон «Об образовании в Российской Федерации»	от 29.12.2012 № 273-ФЗ
6	Уголовный кодекс Российской Федерации (ст. 205–205.6, 208, 280, 280.1, 280.3, 282–282.3)	от 13.06.1996 № 63-ФЗ
7	Кодекс Российской Федерации об административных правонарушениях (ст. 20.3, 20.3.2, 20.29)	от 30.12.2001 № 195-ФЗ
8	Стратегия национальной безопасности Российской Федерации	Указ Президента РФ от 02.07.2021 № 400
9	Стратегия противодействия экстремизму в Российской Федерации до 2025 года	Указ Президента РФ от 29.05.2020 № 344
10	Концепция информационной безопасности детей	Распоряжение Правительства РФ от 28.04.2023 № 1105-р
11	Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»	от 29.12.2010 № 436-ФЗ
12	Профессиональный стандарт «Педагог»	Приказ Минтруда России от 18.10.2013 № 544н
13	Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам	Приказ Минобрнауки России от 01.07.2013 № 499
14	Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024–2028 годы	Утверждён решением НАК
15	Региональные нормативные акты Республики Ингушетия в сфере профилактики терроризма и экстремизма в образовательных организациях	Актуальные постановления Правительства РИ; планы работы АТК РИ на 2025–2026 уч. год

4.1.2. Основная литература

1. Антонян, Ю. М. Терроризм и его причины : монография / Ю. М. Антонян. — Москва : Норма, 2020. — 304 с.
2. Бочарников, И. В. Противодействие экстремизму и терроризму в молодёжной среде : учебное пособие / И. В. Бочарников, В. Ю. Голубовский. — Москва : МГОУ, 2021. — 256 с.
3. Гришко, А. Я. Экстремизм в сети Интернет: проблемы противодействия / А. Я. Гришко. — Москва : Юрлитинформ, 2021. — 192 с.
4. Кузьмин, А. В. Цифровая безопасность школьников: практическое руководство для учителей / А. В. Кузьмин. — Санкт-Петербург : БХВ-Петербург, 2022. — 320 с.
5. Мацкевич, И. М. Криминология экстремизма и терроризма : учебник / И. М. Мацкевич. — Москва : Проспект, 2022. — 432 с.
6. Профилактика экстремизма и терроризма среди обучающихся : методические рекомендации для педагогических работников образовательных организаций / сост. Д. А. Сергеев [и др.]. — Москва : Минпросвещения России, 2023. — 96 с.

7. Рыжков, Е. А. Информационная безопасность в образовании : учебное пособие / Е. А. Рыжков, С. В. Симонович. — Москва : Академия, 2022. — 352 с.

4.1.3. Дополнительная литература

1. Волков, Е. Н. Критерии, признаки, определения и классификации вредоносных психологических воздействий в системах тоталитарных организаций / Е. Н. Волков // Журнал практического психолога. — 2022. — № 3. — С. 14–29.
2. Лукаш, С. Н. Медиаграмотность как инструмент противодействия манипулятивным технологиям в образовательной среде / С. Н. Лукаш, Н. В. Шестакова // Педагогика. — 2023. — № 7. — С. 48–57.
3. Петрищев, В. Е. Азбука терроризма / В. Е. Петрищев. — 4-е изд., перераб. и доп. — Москва : ОЛМА-ПРЕСС, 2020. — 480 с.
4. Тихомиров, С. А. Правовое регулирование сети Интернет в России : учебное пособие / С. А. Тихомиров. — Москва : Проспект, 2023. — 208 с.
5. Шалагин, А. Е. Экстремизм в молодёжной среде: социальный анализ и профилактика / А. Е. Шалагин // Вестник Казанского юридического института МВД России. — 2022. — № 4 (50). — С. 112–118.

4.1.4. Интернет-ресурсы

№	Наименование ресурса	URL
1	Официальный интернет-портал правовой информации	pravo.gov.ru
2	Сайт Министерства просвещения Российской Федерации	edu.gov.ru
3	Сайт Роскомнадзора (форма обращений, реестры)	rkn.gov.ru
4	Реестр запрещённых сайтов Роскомнадзора	ea.is.rkn.gov.ru
5	Сайт Министерства юстиции РФ (Федеральный список экстремистских материалов)	minjust.gov.ru
6	Интернет-приёмная Генеральной прокуратуры РФ	epp.genproc.gov.ru
7	Платформа «Стоп-Контент»	stopcontentrf.ru
8	Правовая система КонсультантПлюс	consultant.ru
9	Национальный антитеррористический комитет (НАК)	nac.gov.ru
10	Лига безопасного интернета	ligainternet.ru
11	Проект «Лапша Медиа» (верификация информации)	lapsha.media
12	ЭИОС ГБОУ ДПО ИПК РО РИ (электронный учебный кабинет программы)	[внутренний URL ЭИОС ИПК]

4.2. Материально-технические условия

4.2.1. Для проведения очных занятий

№	Наименование	Количество / Характеристика
1	Учебная аудитория	Площадью не менее 30 кв. м, оснащённая рабочими местами для слушателей
2	Персональные компьютеры (ноутбуки) для слушателей	По 1 на каждого слушателя (или использование личных устройств — BYOD)
3	Персональный компьютер (ноутбук) преподавателя	1 единица с разрешением экрана не менее 1920×1080
4	Мультимедийный проектор или интерактивная панель	1 единица, разрешение не менее 1920×1080
5	Экран / интерактивная доска	1 единица
6	Доступ к сети Интернет в аудитории	Скорость не менее 50 Мбит/с; для слушателей — Wi-Fi или проводное подключение
7	Гарнитуры (наушники с микрофоном) для слушателей	По 1 на каждого слушателя (для работы с ДОТ)
8	Веб-камера	Для преподавателя — 1 единица; для слушателей — при необходимости

4.2.2. Программное обеспечение

№	Программное обеспечение	Назначение
1	ЭИОС ИПК РО РИ (Moodle)	Размещение учебных материалов, заданий; тестирование; загрузка работ слушателей; ведение журнала успеваемости
2	Система видеоконференц-связи (MAX / Яндекс Телемост)	Проведение занятий в режиме ДОТ; трансляция экрана преподавателя; чат участников
3	Microsoft Office / LibreOffice / Яндекс 360	Работа с текстовыми документами, презентациями, таблицами
4	Браузер (Яндекс.Браузер, Chrome, Firefox)	Работа с онлайн-ресурсами, реестрами, официальными сайтами органов власти
5	Яндекс.Картинки (обратный поиск изображений)	Практикум по верификации информации (тема 3.1)
6	КонсультантПлюс (сетевая версия или интернет-версия)	Работа с нормативными правовыми актами (темы 1.1, 1.2)
7	Программа для скриншотов (Яндекс.Скриншотер, LightShot или встроенные инструменты ОС)	Практикум по документированию фактов (тема 3.2)
8	Canva / Яндекс.Презентации / PowerPoint	Разработка слушателями презентаций к защите итоговой аттестационной работы

4.2.3. Требования к дистанционной части (ДОТ)

При проведении занятий с применением дистанционных образовательных технологий обеспечиваются:

- стабильный доступ слушателей к ЭИОС ИПК РО РИ через личный кабинет (регистрация и авторизация осуществляются до начала курса);
- размещение в электронном учебном кабинете программы учебных презентаций, нормативных актов, чек-листов, учебных кейсов, шаблонов документов и форм заданий — не позднее чем за 24 часа до начала соответствующего занятия;
- техническая поддержка слушателей по вопросам работы в ЭИОС ИПК (контакты технического специалиста сообщаются слушателям в первый день обучения);
- хранение результатов всех видов контроля в ЭИОС ИПК в течение не менее 5 лет.