

**ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
ПЕДАГОГОВ**

**«ЦИФРОВАЯ БЕЗОПАСНОСТЬ РЕБЕНКА:
ПРОФИЛАКТИКА И РЕАГИРОВАНИЕ НА
ОНЛАЙН-РИСКИ»**

Объем: 100 академических часов

Проект практико-ориентированной программы

СОДЕРЖАНИЕ

1. Общие положения
2. Актуальность программы
3. Цель и задачи программы
4. Формируемые профессиональные компетенции
5. Ожидаемые результаты обучения
6. Учебно-тематический план (100 часов)
7. Содержание модулей
8. Детализированный учебно-тематический план
9. Матрица соответствия целей, компетенций, результатов обучения и оценивания
10. Организация учебного процесса
11. Входная диагностика и текущий контроль
12. Самостоятельная работа
13. Формирующее и итоговое оценивание
14. Посткурсовое сопровождение и мониторинг
15. Профессиональное портфолио слушателя
16. Учебно-методическое обеспечение
17. Итоговая модель результата программы

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа повышения квалификации педагогов «Цифровая безопасность ребенка: профилактика и реагирование на онлайн-риски» предназначена для педагогов организаций среднего образования, классных руководителей, кураторов, социальных педагогов, педагогов-психологов, заместителей руководителей и руководителей организаций образования.

Современная образовательная среда включает не только физическое пространство школы, но и цифровые платформы, социальные сети, мессенджеры, игровые сервисы, электронные образовательные ресурсы и другие онлайн-среды, в которых дети учатся, взаимодействуют и проводят значительную часть времени.

Педагог может оказаться одним из первых взрослых, который замечает изменения в поведении ребенка, связанные с кибербуллингом, мошенничеством, шантажом, опасным онлайн-знакомством, распространением персональной информации, нежелательным контентом или иными цифровыми рисками. При этом педагог не выполняет функции следователя, технического эксперта или психолога: его профессиональная задача состоит в своевременном распознавании риска, установлении безопасного контакта с ребенком, оценке срочности ситуации, фиксации минимально необходимых сведений и включении соответствующего школьного и межведомственного механизма помощи.

Методологической и учебно-методической основой программы являются методические материалы КЦ 111 по профилактике и реагированию на киберпреступления и онлайн-риски в отношении несовершеннолетних и учебное пособие для педагогов «Цифровая безопасность ребенка: профилактика и первичное реагирование педагога на киберпреступления и онлайн-риски», разработанное при поддержке Юнисеф.

Форма обучения: очная, дистанционная или смешанная. Направленность программы: практико-ориентированная. Общий объем: 100 академических часов.

2. АКТУАЛЬНОСТЬ ПРОГРАММЫ

Цифровая безопасность ребенка становится частью профессиональной компетентности современного педагога. Онлайн-риски могут проявляться через изменения в эмоциональном состоянии, поведении, отношениях со сверстниками и учебной деятельности. Педагог может первым заметить тревожность после получения сообщений, страх телефона, избегание одноклассников, конфликты в школьных чатах, пропуски занятий, резкое снижение успеваемости, выраженный страх огласки или признаки давления со стороны неизвестного интернет-пользователя.

Неправильная реакция взрослого - обвинение ребенка, публичное обсуждение ситуации, требование показать чувствительные материалы, самостоятельный контакт с предполагаемым нарушителем - может повысить уровень риска и привести к повторной травматизации. Поэтому педагогу необходимы не только знания о цифровых угрозах, но и понятный, отработанный алгоритм профессиональных действий.

3. ЦЕЛЬ И ЗАДАЧИ ПРОГРАММЫ

3.1. Цель программы

Формирование профессиональной готовности педагогов к профилактике, распознаванию и первичному реагированию на онлайн-риски и киберугрозы в отношении несовершеннолетних, а также к созданию безопасной цифровой среды образовательной организации.

3.2. Задачи программы

1. Сформировать представление о современных онлайн-рисках для детей и подростков.
2. Научить распознавать признаки кибербуллинга, онлайн-груминга, сексуализированного вымогательства, кибермошенничества, опасного взаимодействия через игры и мессенджеры и других цифровых угроз.
3. Сформировать навыки первичной оценки безопасности ребенка.
4. Освоить модель определения уровня срочности ситуации.

5. Научить вести поддерживающий разговор с ребенком без давления, обвинения и повторной травматизации.
6. Сформировать понимание профессиональных границ педагога.
7. Научить безопасно фиксировать цифровые сведения и соблюдать требования конфиденциальности.
8. Освоить алгоритмы школьной и межведомственной маршрутизации.
9. Сформировать навыки взаимодействия с родителями и «безопасным взрослым».
10. Познакомить педагогов с принципами психологической первой помощи ребенку.
11. Освоить инструменты цифровой гигиены и профилактики онлайн-рисков.
12. Научить разрабатывать профилактические занятия для обучающихся разных возрастов.
13. Сформировать навыки разработки локального алгоритма реагирования образовательной организации.
14. Развить навыки профессиональной саморегуляции и профилактики эмоционального истощения педагогов.

4. ФОРМИРУЕМЫЕ ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ

Диагностико-профилактическая компетенция: способность распознавать возможные признаки онлайн-рисков и определять необходимость вмешательства.

Коммуникативная компетенция: умение безопасно разговаривать с ребенком, находящимся в состоянии страха, стыда, тревоги или растерянности.

Риск-ориентированная компетенция: способность определить уровень срочности ситуации и выбрать адекватный следующий шаг.

Цифровая компетенция: понимание основных механизмов онлайн-угроз, принципов защиты аккаунтов, приватности и цифровых данных.

Организационная компетенция: способность использовать внутришкольные и межведомственные маршруты реагирования.

Профилактическая компетенция: способность разрабатывать и проводить занятия по цифровой безопасности.

Этическая компетенция: соблюдение конфиденциальности, минимизации данных и прав ребенка.

Рефлексивная компетенция: способность анализировать собственные действия и использовать профессиональную поддержку в сложных случаях.

5. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

После завершения программы слушатель:

- различает основные виды онлайн-рисков;
- распознает «красные флаги» потенциально опасных ситуаций;
- понимает границы профессиональной роли педагога;
- умеет начать безопасный разговор с ребенком;
- использует нейтральные и поддерживающие формулировки;
- не допускает обвиняющей или стигматизирующей коммуникации;
- применяет четырехуровневую модель определения срочности;
- способен провести минимальный скрининг безопасности;
- знает, какие цифровые сведения необходимо сохранить;
- понимает, какие материалы нельзя запрашивать, копировать или распространять;
- знает последовательность школьной и межведомственной маршрутизации;
- способен взаимодействовать с родителями без обвинения ребенка;
- распознает признаки эмоционального кризиса и риска самоповреждения;
- владеет базовыми приемами психологической первой помощи;
- способен провести профилактическое занятие с детьми;

- может разработать памятку или алгоритм для родителей;
- способен провести самоаудит цифровой безопасности образовательной организации;
- участвует в разработке локального алгоритма реагирования школы.

6. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН (100 ЧАСОВ)

№	Модуль	Лекц ии	Практи ка	Само ст. работа	Контро ль	Все го
1	Цифровая безопасность ребенка как профессиональная компетенция педагога	1	3	2	0	6
2	Современные онлайн-риски для детей и подростков	2	6	2	0	10
3	Профессиональная роль педагога: полномочия, этика, конфиденциальность	1	5	2	0	8
4	Безопасная коммуникация с ребенком	2	8	2	0	12
5	Оценка срочности и первичный скрининг безопасности	1	7	2	0	10
6	Цифровые сведения, персональные данные и сохранение цифровых следов	1	5	2	0	8
7	Школьная и межведомственная маршрутизация	1	7	2	0	10
8	Психологическая первая помощь и взаимодействие с родителями	1	7	2	0	10
9	Профилактика онлайн-рисков и цифровая гигиена	1	7	2	0	10
10	Методика профилактической работы в образовательной организации	1	6	1	0	8
11	Профессиональная безопасность педагога	1	2	1	0	4
12	Итоговая аттестация	0	0	0	4	4
	ИТОГО	13	63	20	4	100

В совокупности практические занятия, самостоятельная и проектная работа составляют 76% объема курса, что соответствует его деятельностной направленности.

7. СОДЕРЖАНИЕ МОДУЛЕЙ

МОДУЛЬ 1. ЦИФРОВАЯ БЕЗОПАСНОСТЬ РЕБЕНКА КАК ПРОФЕССИОНАЛЬНАЯ КОМПЕТЕНЦИЯ ПЕДАГОГА

Объем: 6 академических часов

Цель модуля. Сформировать у педагогов целостное представление о цифровой безопасности ребенка как части безопасной образовательной среды и определить место педагога в системе профилактики и первичного реагирования на онлайн-риски.

1.1. Ребенок в современной цифровой среде

- цифровая среда как продолжение социальной и образовательной среды ребенка;
- социальные сети, мессенджеры, онлайн-игры, видеосервисы, образовательные платформы и закрытые сообщества как пространства общения несовершеннолетних;

- сочетание образовательных возможностей и потенциальных рисков цифровой среды;
- переход рисков из онлайн-среды в офлайн и обратно;
- влияние онлайн-взаимодействий на эмоциональное состояние, поведение, отношения со сверстниками и учебную деятельность ребенка;
- особенности цифрового поведения детей разных возрастных групп.

1.2. Понятие цифровой безопасности ребенка

- безопасность жизни и здоровья;
- психологическое благополучие;
- достоинство и частная жизнь;
- персональные данные и цифровая репутация;
- финансовая безопасность;
- права и законные интересы ребенка.

1.3. Почему цифровая безопасность становится педагогической задачей

- тревожность и страх после получения сообщений;
- отказ пользоваться телефоном или постоянная проверка телефона;
- избегание отдельных одноклассников;
- пропуски занятий и снижение учебной мотивации;
- конфликты в школьных чатах и публичное высмеивание;
- выраженный страх огласки;
- признаки давления со стороны неизвестного интернет-пользователя.

1.4. Место педагога в системе защиты ребенка

- заметить проблему;
- безопасно установить контакт;
- выслушать ребенка;
- оценить наличие непосредственной угрозы;
- не допустить дальнейшего вреда;
- зафиксировать минимально необходимые сведения;
- передать информацию по установленному маршруту;
- обеспечить педагогическое сопровождение ребенка.

1.5. Базовая формула профессионального реагирования

- Заметить → установить контакт → проверить безопасность → поддержать → определить срочность → зафиксировать минимум сведений → передать по маршруту → сопровождать.

Практическая работа

- Разбор ситуаций: «Конфликт или кибербуллинг?», «Обычное онлайн-знакомство или потенциально опасный контакт?», «Проблема дисциплины или сигнал неблагополучия?», «Что должен сделать педагог, а что выходит за пределы его компетенции?».

Самостоятельная работа

- Составление карты «Какие цифровые риски могут возникать среди обучающихся моей образовательной организации?».

Результат освоения модуля. Педагог понимает свою профессиональную роль в обеспечении цифровой безопасности ребенка и способен отличать обычную педагогическую ситуацию от ситуации, требующей специального реагирования.

МОДУЛЬ 2. СОВРЕМЕННЫЕ ОНЛАЙН-РИСКИ ДЛЯ ДЕТЕЙ И ПОДРОСТКОВ

Объем: 10 академических часов

Цель модуля. Научить педагогов распознавать основные виды онлайн-рисков, понимать механизмы вовлечения ребенка и выделять признаки потенциально опасной ситуации.

2.1. Нежелательный и запрещенный контент

- материалы, способные причинить вред развитию ребенка;
- насильственный и сексуализированный контент;
- контент, связанный с самоповреждением;
- опасные челленджи;
- пропаганда противоправного поведения;
- манипулятивные сообщества;
- фейковые объявления, «кастинги», «работа», «подарки» и «задания».

2.2. Кибербуллинг

- понятие кибербуллинга;
- отличие единичного конфликта от систематической травли;
- оскорбления и унижения;
- исключение из групп;
- распространение слухов;
- публикация фотографий без согласия;
- создание фейковых аккаунтов;
- травля в классных и родительских чатах;
- угрозы и запугивание;
- перенос школьного буллинга в цифровую среду;
- поведенческие признаки: страх телефона, избегание сверстников, тревожность, замкнутость, пропуски, снижение успеваемости.

2.3. Онлайн-груминг

- механизм постепенного установления доверительных отношений с ребенком с последующим давлением или эксплуатацией;
- незнакомый человек проявляет чрезмерный интерес к ребенку;
- дарит игровые предметы или деньги;
- предлагает перейти из открытой платформы в закрытый чат;
- просит хранить общение в секрете;
- выясняет личные данные, информацию о семье и расписании;
- просит фото или видеосвязь;
- обсуждает сексуализированные темы;
- предлагает личную встречу.

2.4. Сексуализированное вымогательство

- шантаж с использованием фото, видео или другой личной информации;
- возможные требования: деньги, дополнительные фотографии, видеозвонок, пароль или доступ к аккаунту, продолжение общения, личная встреча;
- психологический механизм воздействия: стыд + страх огласки + срочность требований.

2.5. Опасное взаимодействие через игры и мессенджеры

- игровые чаты и закрытые группы;
- переход из игры в личный мессенджер;
- внутриигровые подарки как инструмент установления доверия;
- предложения «дружбы»;
- получение персональных данных ребенка;
- попытки организовать офлайн-встречу.

2.6. Кибермошенничество

- фишинговые ссылки;

- «бесплатные» игровые предметы;
- кража аккаунтов;
- запрос SMS-кодов;
- ложные розыгрыши;
- фиктивная онлайн-работа;
- «легкий заработок»;
- использование банковских карт несовершеннолетних;
- получение и перевод чужих денег;
- вовлечение в дроппинг;
- оформление SIM-карт или счетов для третьих лиц.

2.7. Комбинированные риски

- одна ситуация может одновременно включать несколько рисков: онлайн-знакомство → доверие → получение фотографии → шантаж → требование денег → угроза встречи.

Практическая работа

- Кейс-анализ: «Друг из игры», «Закрытый Telegram-чат», «Фотография класса появилась в фейковом аккаунте», «Предложение легкого заработка», «Если не заплатишь — всем отправлю», «Новый друг знает школу ребенка», «Травля в классном чате».
- По каждому кейсу определить основной риск, дополнительные риски, признаки угрозы, вопросы для первичного уточнения, уровень срочности и первые действия.

Результат освоения модуля. Педагог способен распознавать типовые онлайн-риски и выделять признаки, требующие немедленного или планового реагирования.

МОДУЛЬ 3. ПРОФЕССИОНАЛЬНАЯ РОЛЬ ПЕДАГОГА: ПОЛНОМОЧИЯ, ЭТИКА И КОНФИДЕНЦИАЛЬНОСТЬ

Объем: 8 академических часов

Цель модуля. Сформировать у педагогов понимание границ профессиональной ответственности при получении информации об онлайн-угрозе.

3.1. Что педагог должен делать

- принимать информацию серьезно;
- проверять безопасность ребенка;
- оказывать первичную поддержку;
- сообщать ответственным специалистам;
- соблюдать конфиденциальность;
- фиксировать минимально необходимые сведения;
- сопровождать ребенка в пределах своей компетенции.

3.2. Что педагог не должен делать

- проводить собственное расследование;
- устанавливать личность предполагаемого нарушителя;
- искать его аккаунты;
- вступать с ним в переписку;
- выдавать себя за ребенка;
- организовывать встречу;
- просить ребенка продолжать контакт «для доказательств»;
- давать окончательную юридическую квалификацию;
- обещать наказание нарушителя;
- самостоятельно исследовать устройство ребенка.

3.3. Принцип минимально необходимой информации

- выяснять только то, что требуется для оценки безопасности, определения срочности и передачи информации;
- не заставлять ребенка многократно пересказывать ситуацию.

3.4. Конфиденциальность

- кто может иметь доступ к сведениям;
- почему нельзя обсуждать ситуацию в педагогическом коллективе без необходимости;
- почему недопустимо обсуждение случая в родительском или классном чате;
- защита личности ребенка;
- передача информации только тем специалистам, которым она необходима.

3.5. Недопущение повторной травматизации

- публичное обсуждение недопустимо;
- нельзя демонстрировать переписку;
- нельзя требовать повторно рассказывать травмирующие детали;
- нельзя задавать обвиняющие вопросы;
- нельзя проводить публичное «примирение» ребенка с агрессором без оценки риска;
- нельзя демонстрировать интимные или травмирующие материалы другим людям.

3.6. Этическая дилемма «конфиденциальность — безопасность»

- если ребенок просит никому не рассказывать, педагог объясняет, что будет бережно относиться к информации, но при угрозе безопасности обязан подключить тех взрослых и специалистов, которые могут защитить ребенка.

Практическая работа

- Практикум «Можно / нельзя / зависит от ситуации»: слушатели распределяют 20 действий педагога по трем категориям и обосновывают решение.

Результат освоения модуля. Педагог действует в пределах профессиональной компетенции и понимает этические границы работы с чувствительной информацией.

МОДУЛЬ 4. БЕЗОПАСНАЯ КОММУНИКАЦИЯ С РЕБЕНКОМ

Объем: 12 академических часов

Цель модуля. Сформировать навыки поддерживающего разговора с ребенком без давления, обвинения и повторной травматизации.

4.1. Почему первая реакция взрослого имеет значение

- ребенок может бояться наказания;
- испытывать стыд;
- считать себя виноватым;
- опасаться огласки;
- бояться потерять телефон;
- опасаться мести;
- не понимать, является ли ситуация опасной;
- задача педагога - сохранить контакт.

4.2. Начало разговора

- спокойный тон;
- отсутствие оценок;
- короткие предложения;
- один вопрос за раз;
- время на ответ;
- пример: «Я тебя слушаю», «Расскажи столько, сколько сейчас можешь», «Сначала мне важно понять, ты сейчас в безопасности?».

4.3. Открытые и закрытые вопросы

- сначала нейтральные открытые вопросы: «Расскажи, что произошло», «Что сейчас тебя больше всего беспокоит?»;
- затем конкретные вопросы, необходимые для оценки безопасности.

4.4. Ребенок боится или стыдится

- «Ты можешь отвечать коротко»;
- «Не обязательно рассказывать все сразу»;
- «Я здесь, чтобы помочь, а не обвинять».

4.5. Ребенок молчит

- не торопить;
- не требовать ответа;
- предоставлять время;
- предлагать отвечать «да / нет / не знаю»;
- сохранять контакт.

4.6. Обвиняющие и обесценивающие фразы

- не использовать: «Зачем ты это сделал?», «Как ты мог поверить?», «Почему сразу не рассказал?», «Сам виноват», «Я же предупреждал»;
- не использовать: «Успокойся», «Не плачь», «Ничего страшного», «Забудь об этом»;
- заменять их признанием эмоций и конкретным безопасным следующим шагом.

4.7. Возрастная адаптация

- 7–10 лет: простые короткие вопросы, конкретные понятия, минимум профессиональной терминологии, помощь безопасного взрослого;
- 11–14 лет: особое внимание страху наказания, приватности, отношениям со сверстниками, давлению через игры и социальные сети;
- 15–17 лет: уважение автономности подростка, отсутствие морализаторства, объяснение последствий и вариантов помощи, участие подростка в безопасных решениях.

4.8. Письменное общение

- одно сообщение - один вопрос;
- короткие формулировки;
- отсутствие длинных инструкций;
- проверка возможности безопасно писать;
- не задавать чувствительные вопросы, если устройство может контролироваться другим лицом.

Практическая работа

- Ролевые упражнения: «Первые пять минут разговора», «Ребенок молчит», «Ребенок боится, что родители узнают», «Подросток считает себя виноватым», «Переформулируй опасный вопрос».

Результат освоения модуля. Педагог способен провести первичный поддерживающий разговор, не превращая его в допрос.

МОДУЛЬ 5. ОЦЕНКА СРОЧНОСТИ И ПЕРВИЧНЫЙ СКРИНИНГ БЕЗОПАСНОСТИ

Объем: 10 академических часов

Цель модуля. Научить педагога быстро отличать ситуацию непосредственной угрозы от ситуации, требующей плановой помощи.

5.1. Главный принцип

- Сначала безопасность - потом детали.

5.2. Критический уровень

- непосредственная угроза жизни;
- насилие происходит сейчас;
- предполагаемый нарушитель рядом;
- ребенок удерживается;
- назначена опасная встреча;
- угрозы убийством или похищением;

- выраженный риск суицида или самоповреждения.

5.3. Высокий уровень

- груминг;
- сексуализированный шантаж;
- требование интимных материалов;
- угроза публикации;
- предложение встречи;
- повторяющееся давление;
- неизвестный взрослый знает местонахождение ребенка.

5.4. Средний уровень

- кибербуллинг без непосредственной угрозы жизни;
- подозрительные онлайн-контакты;
- мошенничество;
- потеря аккаунта;
- конфликт, требующий школьного сопровождения.

5.5. Консультационный уровень

- запросы по приватности;
- профилактике;
- семейным цифровым правилам;
- настройкам безопасности.

5.6. Минимальный скрининг

- Где сейчас ребенок?
- Может ли он безопасно говорить?
- Есть ли опасный человек рядом?
- Происходит ли что-то опасное прямо сейчас?
- Есть ли угроза встречи?
- Есть ли шантаж?
- Что требуют?
- На какой платформе идет контакт?
- Есть ли рядом безопасный взрослый?
- Есть ли признаки риска самоповреждения?

5.7. Когда прекращается обычный разговор

- при обнаружении критического риска педагог не продолжает детальное выяснение обстоятельств, а включает срочный маршрут реагирования.

Практическая работа

- Практикум: 15 ситуационных карточек. Задача слушателя - определить уровень, обосновать, сформулировать первые три вопроса и выбрать дальнейший маршрут.

Результат освоения модуля. Педагог способен в ограниченное время оценить срочность ситуации и принять решение о дальнейших действиях.

МОДУЛЬ 6. ЦИФРОВЫЕ СВЕДЕНИЯ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ И СОХРАНЕНИЕ ЦИФРОВЫХ СЛЕДОВ

Объем: 8 академических часов

Цель модуля. Научить педагогов безопасно обращаться с цифровой информацией и не создавать дополнительного риска для ребенка.

6.1. Что является полезным цифровым идентификатором

- название платформы;
- никнейм;
- username;
- ID;

- URL;
- номер телефона;
- электронная почта;
- дата и время;
- текст угроз;
- сведения о переводе денег;
- платежные реквизиты;
- информация о назначенной встрече.

6.2. Что не должен делать педагог

- самостоятельно устанавливать IP-адрес;
- определять геолокацию нарушителя;
- взламывать аккаунты;
- восстанавливать удаленную переписку техническими средствами;
- скачивать материалы;
- проводить цифровую экспертизу.

6.3. Работа со скриншотами

- разбираются случаи, когда фиксация переписки может быть полезной, и ситуации, когда копирование материала недопустимо.

6.4. Особо чувствительные материалы

- если речь идет о сексуализированных материалах с участием несовершеннолетнего: не просить ребенка присылать их; не пересылать; не показывать коллегам; не сохранять «на всякий случай»; не размещать в школьных чатах; фиксировать прежде всего источник, аккаунт, ссылку и идентификаторы.

6.5. Персональные данные

- ФИО;
- телефон;
- адрес;
- школа;
- геолокация;
- фотография;
- данные семьи;
- аккаунты;
- переписка;
- основной принцип: собирать только то, что необходимо для обеспечения безопасности и маршрутизации.

6.6. Защита аккаунтов

- уникальные пароли;
- двухфакторная аутентификация;
- SMS-коды;
- активные сессии;
- восстановление доступа;
- подозрительные ссылки.

Практическая работа

- Практикум «Что сохранить - что не сохранять».
- Заполнение учебной формы минимальной фиксации.

Результат освоения модуля. Педагог умеет фиксировать необходимые цифровые сведения, не нарушая принцип минимизации данных и не распространя чувствительный контент.

МОДУЛЬ 7. ШКОЛЬНАЯ И МЕЖВЕДОМСТВЕННАЯ МАРШРУТИЗАЦИЯ

Объем: 10 академических часов

Цель модуля. Сформировать у педагогов способность не только выявлять риск, но и правильно передавать информацию и сопровождать ребенка.

7.1. Что такое маршрутизация

- заранее определенная последовательность передачи информации специалистам, которые обладают соответствующими полномочиями;
- основная формула: безопасность → первичная оценка → уровень риска → передача → сопровождение.

7.2. Внутришкольный маршрут

- взаимодействие педагога;
- классного руководителя;
- администрации;
- педагога-психолога;
- социального педагога;
- ответственного за профилактическую работу.

7.3. Роль администрации

- организует реагирование;
- обеспечивает выполнение локального алгоритма;
- координирует взаимодействие специалистов;
- контролирует защиту ребенка;
- предотвращает публичное обсуждение случая.

7.4. Психологическая служба

- подключается при страхе;
- панике;
- выраженном стыде;
- травле;
- психологическом кризисе;
- риске самоповреждения.

7.5. Взаимодействие с КЦ 111

- назначение КЦ 111;
- ситуации, в которых целесообразно обращение;
- информация, которую необходимо передать;
- принципы последующего сопровождения.

7.6. Органы внутренних дел и экстренные службы

- угроза жизни;
- текущее насилие;
- шантаж;
- сексуализированное вымогательство;
- опасная встреча;
- распространение чувствительных материалов;
- реальная угроза здоровью.

7.7. Органы защиты прав ребенка и другие службы

- межведомственная координация;
- защита прав ребенка;
- социальная поддержка;
- медицинская помощь;
- психологическая помощь.

7.8. Сопровождение после передачи

- передача информации не означает, что педагогическая поддержка ребенка заканчивается;
- школа продолжает контролировать безопасность;
- предупреждать повторную травлю;
- обеспечивать психологическое сопровождение;
- корректировать образовательные условия при необходимости.

Практическая работа

- Создание карты маршрутизации для конкретной школы.
- Задание «Кому передать и почему?».

Результат освоения модуля. Слушатель знает, кому, когда и какую информацию необходимо передавать, и умеет организовывать последующее педагогическое сопровождение.

МОДУЛЬ 8. ПСИХОЛОГИЧЕСКАЯ ПЕРВАЯ ПОМОЩЬ И ВЗАИМОДЕЙСТВИЕ С РОДИТЕЛЯМИ

Объем: 10 академических часов

Цель модуля. Сформировать навыки первичной эмоциональной поддержки ребенка и конструктивного взаимодействия с семьей.

8.1. Психологическая первая помощь

- не является психотерапией;
- не является диагностикой;
- не является консультированием по сложным психологическим проблемам;
- для педагога это безопасный контакт, спокойное присутствие, снижение эмоционального напряжения и помощь в определении следующего шага.

8.2. Признаки острого стресса

- плач;
- дрожь;
- оцепенение;
- невозможность сосредоточиться;
- растерянность;
- паника;
- выраженный страх;
- повторяющиеся высказывания о вине.

8.3. Стыд и чувство вины

- педагог не усиливает переживания ребенка обвиняющими вопросами;
- необходимо отделять действие нарушителя от поведения ребенка.

8.4. Риск самоповреждения

- серьезно относиться к высказываниям «Я больше не могу», «Мне незачем жить», «Лучше бы меня не было» и сообщениям о намерении причинить себе вред;
- в таких случаях обычная беседа прекращается и применяется соответствующий срочный маршрут.

8.5. Родители как ресурс безопасности

- родителю рекомендуется сохранять спокойствие;
- не обвинять;
- не стыдить;
- не устраивать допрос;
- не требовать удалить все немедленно;
- не угрожать ребенку лишением телефона;
- не писать предполагаемому нарушителю самостоятельно.

8.6. Родитель в панике

- педагог помогает перейти от эмоций к действиям: безопасность → сведения → помощь → маршрут.

8.7. Понятие «безопасного взрослого»

- взрослый, которому ребенок доверяет и присутствие которого снижает риск;
- им может быть родитель, другой родственник, педагог, психолог или иной взрослый, способный безопасно поддержать ребенка.

8.8. Когда информирование родителя требует осторожности

- если предполагаемая угроза может исходить от родителя, опекуна, близкого взрослого, педагога или тренера, информация не должна автоматически передаваться лицу, которое может усилить угрозу.

Практическая работа

- Ролевые ситуации: «Родитель обвиняет ребенка», «Родитель хочет найти нарушителя самостоятельно», «Родитель требует показать всю переписку», «Ребенок боится возвращаться домой».

Результат освоения модуля. Педагог владеет базовым алгоритмом психологической поддержки и способен конструктивно взаимодействовать с родителем.

МОДУЛЬ 9. ПРОФИЛАКТИКА ОНЛАЙН-РИСКОВ И ЦИФРОВАЯ ГИГИЕНА

Объем: 10 академических часов

Цель модуля. Научить педагогов переходить от реагирования на уже возникшую проблему к системной профилактике.

9.1. Цифровая гигиена

- рассматривается как система регулярных безопасных практик ребенка и семьи.

9.2. Приватность

- закрывать профиль;
- ограничивать круг пользователей, которые могут писать;
- управлять комментариями;
- контролировать видимость публикаций;
- проверять подписчиков.

9.3. Геолокация

- обсуждаются риски публикации школы;
- адреса;
- маршрута;
- расписания;
- текущего местонахождения.

9.4. Пароли

- уникальный пароль;
- отсутствие персональной информации в пароле;
- двухфакторная защита;
- недопустимость передачи кодов.

9.5. Безопасность общения

- не переходить сразу в закрытый чат;
- не отправлять личные материалы незнакомцам;
- сообщать взрослому о давлении;
- прекращать контакт при угрозах;
- не идти на встречу в одиночку.

9.6. Игровая безопасность

- незнакомые игроки;
- подарки;

- игровые валюты;
- голосовые чаты;
- переход в другие приложения;
- мошенничество с аккаунтами.

9.7. Финансовая безопасность

- карты;
- переводы;
- QR;
- SMS-коды;
- «легкий заработок»;
- дроппинг;
- фишинг.

9.8. Искусственный интеллект и новые цифровые риски

- генеративный контент;
- поддельные изображения;
- фейковые голосовые сообщения;
- имитация личности;
- автоматизированное мошенничество;
- необходимость регулярного обновления профилактического содержания по мере появления новых технологий.

9.9. Профилактика без запугивания

- неэффективная формула: «Интернет опасен - ничего никому не отправляйте»;
- более эффективная формула: «Как распознать давление → что сделать → кому сообщить → как получить помощь».

Практическая работа

- Разработка мини-памятки «5 правил цифровой безопасности для моего класса».

Результат освоения модуля. Педагог способен формировать у обучающихся практические навыки цифровой безопасности.

МОДУЛЬ 10. МЕТОДИКА ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Объем: 8 академических часов

Цель модуля. Научить слушателей проектировать профилактическую деятельность с учетом возраста детей и реальных рисков цифровой среды.

10.1. Принципы профилактической работы

- возрастная;
- регулярная;
- практическая;
- неназидательная;
- безопасная;
- ориентированная на навыки.

10.2. Работа с детьми 7–10 лет

- кто такой незнакомец в интернете;
- личная информация;
- фотографии;
- опасные просьбы;
- «секрет от родителей»;
- безопасный взрослый.

10.3. Работа с детьми 11–14 лет

- социальные сети;

- игровые чаты;
- кибербуллинг;
- онлайн-дружба;
- давление;
- личные фотографии;
- пароли;
- безопасность групповых чатов.

10.4. Работа с подростками 15–17 лет

- цифровая репутация;
- персональные границы;
- ответственность;
- шантаж;
- интимный контент;
- финансовое мошенничество;
- «легкий заработок»;
- риски самостоятельных встреч.

10.5. Форматы занятий

- классный час;
- кейс;
- тренинг;
- дискуссия;
- ролевая игра;
- мини-проект;
- цифровая викторина;
- анализ ситуации.

10.6. Что нельзя использовать в профилактике

- реальные интимные материалы;
- шокирующие изображения;
- публичное обсуждение реального ребенка;
- унижающие примеры;
- морализаторство;
- обвинение пострадавшего.

10.7. Работа с родителями

- семейные цифровые правила;
- доверительный разговор;
- родительский контроль;
- приватность;
- мошенничество;
- действия при угрозах.

10.8. Самоаудит образовательной организации

- есть ли локальный алгоритм;
- знают ли педагоги маршрут;
- знают ли дети, к кому обращаться;
- есть ли профилактические материалы;
- как защищаются персональные данные;
- как реагируют на кибербуллинг;
- организована ли работа с родителями.

Практическая работа

- Разработка 30–40-минутного профилактического занятия для выбранной возрастной группы.

Результат освоения модуля. Педагог способен самостоятельно разработать профилактическое занятие и включить его в воспитательную работу.

МОДУЛЬ 11. ПРОФЕССИОНАЛЬНАЯ БЕЗОПАСНОСТЬ ПЕДАГОГА

Объем: 4 академических часов

Цель модуля. Предупредить эмоциональное истощение специалистов, работающих со сложными случаями.

11.1. Эмоционально сложные ситуации

- педагог может сталкиваться с рассказами о насилии;
- шантажом;
- травлей;
- угрозами;
- сексуальной эксплуатацией;
- самоповреждением.

11.2. Вторичная травматизация

- постоянное возвращение мыслями к случаю;
- бессонница;
- тревога;
- чувство бессилия;
- раздражительность;
- снижение эмпатии;
- желание самостоятельно «спасти» ребенка, выйдя за профессиональные границы.

11.3. Профессиональные границы как способ защиты

- педагог не обязан самостоятельно решать ситуацию;
- правильный профессиональный алгоритм: увидел → отреагировал → передал специалистам → продолжил педагогическое сопровождение.

11.4. Супервизия и командная поддержка

- обсуждение сложного случая;
- методический разбор;
- консультация психолога;
- помощь администрации;
- командный анализ обезличенного кейса;
- принцип: анализируется алгоритм действий, а не личность педагога.

Практическая работа

- Разработка персональной схемы «Что я делаю, если столкнулся с эмоционально тяжелым случаем».

Результат освоения модуля. Педагог умеет сохранять профессиональные границы и пользоваться системой организационной поддержки.

МОДУЛЬ 12. ИТОГОВАЯ АТТЕСТАЦИЯ

Объем: 4 академических часов

Цель модуля. Определить способность слушателя применять полученные знания в реальной педагогической ситуации.

12.1. Итоговый ситуационный кейс

- слушатель получает комплексную ситуацию и определяет основные риски;

- устанавливает уровень срочности;
- формулирует первые вопросы ребенку;
- выбирает поддерживающие фразы;
- называет вопросы и действия, которые недопустимы;
- определяет необходимые цифровые сведения;
- указывает, что нельзя копировать или пересылать;
- определяет школьный и межведомственный маршрут;
- определяет необходимость психологической помощи;
- предлагает действия по дальнейшему сопровождению.

12.2. Защита практического проекта

- вариант 1: «Локальный алгоритм реагирования образовательной организации на онлайн-риски»;
- вариант 2: «Программа профилактики цифровых рисков для обучающихся»;
- вариант 3: «Комплект классных часов по цифровой безопасности»;
- вариант 4: «Методический комплект для педагогов и родителей»;
- вариант 5: «Модель системы цифровой безопасности образовательной организации».

12.3. Критерии оценивания

- правильность определения риска;
- приоритет безопасности ребенка;
- соблюдение профессиональных границ;
- качество коммуникации;
- корректность фиксации сведений;
- обоснованность маршрутизации;
- соблюдение конфиденциальности;
- практическая применимость разработанного продукта.

Практическая работа

- Комплексный ситуационный кейс и защита итогового проекта.

Результат освоения модуля. Слушатель демонстрирует комплексное применение алгоритма профессионального реагирования и готовность к переносу результата в практику образовательной организации.

7.1. Логика освоения программы

Модуль 1: понимаю свою роль

Модуль 2: распознаю угрозу

Модуль 3: знаю границы своих полномочий

Модуль 4: умею правильно поговорить с ребенком

Модуль 5: определяю срочность

Модуль 6: правильно работаю с цифровыми сведениями

Модуль 7: знаю, куда передать информацию

Модуль 8: поддерживаю ребенка и взаимодействую с семьей

Модуль 9: умею предупреждать риски

Модуль 10: организую профилактическую работу

Модуль 11: сохраняю собственную профессиональную устойчивость

Модуль 12: демонстрирую способность применять алгоритм комплексно

РАСПОЗНАТЬ → ПОДДЕРЖАТЬ → ОЦЕНИТЬ РИСК → НЕ НАВРЕДИТЬ → ЗАФИКСИРОВАТЬ НЕОБХОДИМОЕ → ПЕРЕДАТЬ ПО МАРШРУТУ → СОПРОВОЖДАТЬ → ПРОФИЛАКТИРОВАТЬ

8. ДЕТАЛИЗИРОВАННЫЙ УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН (100 ЧАСОВ)

№	Тема занятия	Часы	Форма проведения	Практическое задание	Результат обучения
1.1	Ребенок в современной цифровой среде: обучение, общение, социализация и риски	2	Интерактивная лекция	Составить карту цифровой среды современного школьника	Определяет основные цифровые пространства, в которых находится ребенок
1.2	Цифровая безопасность как компонент безопасной образовательной среды	2	Семинар-практикум	Проанализировать 5 школьных ситуаций и определить наличие цифрового риска	Отличает обычную педагогическую ситуацию от потенциальной угрозы
1.3	Роль педагога в системе защиты ребенка	2	Кейс-сессия	Разработать схему «Что должен и чего не должен делать педагог»	Понимает профессиональную роль педагога при онлайн-рисках
2.1	Нежелательный и запрещенный контент. Опасные челленджи и манипулятивные сообщества	2	Лекция + анализ примеров	Классифицировать примеры цифрового контента по степени риска	Распознает потенциально опасный контент
2.2	Кибербуллинг: формы, признаки и отличие от единичного конфликта	2	Case-study	Проанализировать ситуацию травли в школьном чате	Различает конфликт, буллинг и кибербуллинг
2.3	Онлайн-груминг и вовлечение ребенка через социальные сети, игры и закрытые чаты	2	Практический семинар	По кейсу «Друг из игры» выявить этапы вовлечения	Распознает признаки онлайн-груминга
2.4	Сексуализированное вымогательство, шантаж и опасные онлайн-знакомства	2	Кейс-тренинг	Определить признаки давления, срочность и первые действия педагога	Выявляет признаки высокого и критического риска
2.5	Кибермошенничество, фишинг, кража аккаунтов, «легкий заработок» и дроппинг	2	Практикум	Разобрать 4 схемы вовлечения несовершеннолетних в финансовое мошенничество	Распознает основные мошеннические схемы
3.1	Профессиональные полномочия педагога при выявлении онлайн-угрозы	2	Лекция-дискуссия	Разграничить функции педагога, психолога, администрации и правоохранительных органов	Соблюдает границы профессиональной компетенции
3.2	Что педагог не должен делать: расследование, поиск нарушителя, самостоятельный контакт	2	Анализ ошибок	Разобрать 10 ошибочных действий педагога и предложить правильную альтернативу	Избегает действий, способных увеличить риск
3.3	Конфиденциальность и защита персональных данных ребенка	2	Практический семинар	Определить, кому и какой объем информации может быть передан	Применяет принцип минимально необходимой информации
3.4	Недопущение повторной травматизации ребенка	2	Кейс-практикум	Переработать обвиняющие и травмирующие вопросы в нейтральные	Соблюдает этические принципы общения
4.1	Первая реакция педагога на сообщение ребенка об онлайн-угрозе	2	Мини-лекция + тренинг	Сформулировать первые 3–5 фраз педагога	Устанавливает безопасный первичный контакт
4.2	Открытые, нейтральные и уточняющие вопросы	2	Коммуникативный практикум	Переформулировать наводящие вопросы	Задаст вопросы без давления и подсказывания ответа
4.3	Разговор с ребенком, испытывающим страх, стыд или чувство вины	2	Ролевая игра	Смоделировать разговор «ребенок — педагог»	Использует поддерживающие формулировки
4.4	Что делать, если ребенок молчит, плачет или отказывается отвечать	2	Тренинг	Отработать алгоритм «один вопрос — один ответ»	Поддерживает контакт без давления
4.5	Фразы, которые нельзя использовать. Обвинение, стыжение и обесценивание	2	Практикум	Таблица «опасная фраза — почему нельзя — безопасная замена»	Исключает травмирующие речевые конструкции
4.6	Возрастная адаптация общения: 7–10, 11–14, 15–17 лет. Письменная коммуникация	2	Кейс-мастерская	Разработать три варианта одного сообщения для разных возрастов	Адаптирует коммуникацию к возрасту и каналу связи
5.1	Принцип «сначала безопасность — потом детали»	2	Интерактивная лекция	Определить минимальный набор вопросов первичного скрининга	Ставит безопасность ребенка выше сбора подробностей
5.2	Критический уровень риска	2	Кейс-тренинг	Проанализировать ситуации текущего насилия, опасной встречи и угроз жизни	Распознает критические ситуации
5.3	Высокий уровень риска	2	Практикум	Определить срочность случаев груминга, шантажа и угроз публикации	Выявляет ситуации высокого риска
5.4	Средний и консультационный уровни	2	Семинар	Разделить 10 ситуаций по уровням срочности	Дифференцирует уровни риска
5.5	Минимальный скрининг безопасности ребенка	2	Алгоритмический тренажер	Провести скрининг по ситуационной карточке	Быстро определяет уровень срочности и следующий шаг
6.1	Цифровые следы и идентификаторы: платформа, аккаунт, URL, никнейм, ID, время	2	Практикум	Из предложенного кейса выделить сведения, которые необходимо зафиксировать	Определяет минимально необходимые цифровые данные
6.2	Безопасное сохранение переписки, ссылок, угроз и платежной информации	2	Кейс-практикум	Составить карточку первичной фиксации	Корректно фиксирует цифровые сведения

№	Тема занятия	Часы	Форма проведения	Практическое задание	Результат обучения
6.3	Особо чувствительные и сексуализированные материалы с участием ребенка	2	Методический семинар	Определить действия «можно / нельзя» в 10 ситуациях	Не копирует и не распространяет чувствительный контент
6.4	Пароли, двухфакторная аутентификация, приватность и защита аккаунта	2	Цифровой практикум	Разработать чек-лист защиты детского аккаунта	Умеет объяснить базовые меры цифровой защиты
7.1	Что такое маршрутизация. Логика передачи информации	2	Лекция-практикум	Построить цепочку реагирования для типового случая	Понимает последовательность маршрутизации
7.2	Внутришкольный маршрут: педагог, классный руководитель, психолог, социальный педагог, администрация	2	Работа в группах	Распределить функции участников школьной команды	Определяет ответственность специалистов
7.3	Взаимодействие с КЦ 111 и службами защиты ребенка	2	Кейс-семинар	Подготовить краткую информацию для передачи по ситуации	Передает только необходимые сведения
7.4	Ситуации для безотлагательного подключения полиции, медицинской и психологической помощи	2	Ситуационный тренинг	Определить адресата по 10 ситуациям	Выбирает соответствующий маршрут помощи
7.5	Сопровождение ребенка после передачи информации	2	Проектный практикум	Разработать карту маршрутизации своей школы	Организует последующее педагогическое сопровождение
8.1	Основы психологической первой помощи в деятельности педагога	2	Лекция-практикум	Определить действия педагога в первые минуты после обращения	Оказывает базовую эмоциональную поддержку
8.2	Страх, паника, стыд, вина и растерянность ребенка	2	Ролевая тренировка	Подобрать поддерживающие фразы для разных состояний	Реагирует на эмоциональное состояние ребенка
8.3	Признаки риска самоповреждения и алгоритм срочного реагирования	2	Кейс-тренинг	Проанализировать высказывания ребенка и определить уровень риска	Распознает ситуации, требующие срочного подключения специалистов
8.4	Работа с родителями: сообщение о проблеме без обвинения ребенка	2	Ролевая игра	Смоделировать беседу с родителем	Конструктивно взаимодействует с семьей
8.5	Родитель в панике или агрессии. «Безопасный взрослый» и сложные семейные ситуации	2	Кейс-практикум	Разобрать ситуацию, когда информирование конкретного родителя может повысить риск	Выбирает безопасный способ привлечения взрослого
9.1	Цифровая гигиена ребенка и семьи	2	Интерактивный семинар	Разработать семейные цифровые правила	Формирует практические рекомендации
9.2	Приватность, геолокация и персональные данные	2	Цифровой практикум	Провести аудит условного профиля школьника	Выявляет риски избыточного раскрытия данных
9.3	Пароли, коды, фишинг, взлом аккаунтов и мошенничество	2	Практическая лаборатория	Составить памятку «Как защитить аккаунт»	Обучает детей базовой цифровой защите
9.4	Безопасность в онлайн-играх, мессенджерах, чатах и социальных сетях	2	Case-study	Проанализировать цифровой маршрут ребенка и выявить риски	Объясняет детям правила безопасного онлайн-взаимодействия
9.5	ИИ, дипфейки, поддельные изображения и новые формы цифрового мошенничества	2	Дискуссия + проектирование	Разработать 5 рекомендаций по новым ИИ-рискам	Учитывает новые технологические угрозы в профилактике
10.1	Методические принципы обучения детей цифровой безопасности	2	Методический семинар	Сравнить запугивающую и навыко-ориентированную профилактику	Проектирует профилактику без морализаторства и запугивания
10.2	Возрастная дифференциация профилактики: 7–10, 11–14, 15–17 лет	2	Проектный практикум	Подобрать содержание занятия для трех возрастных групп	Адаптирует профилактическую работу к возрасту
10.3	Формы профилактической работы: классный час, кейс, тренинг, дискуссия, проект, родительское собрание	2	Методическая мастерская	Разработать сценарий 30–40-минутного занятия	Создает практико-ориентированное профилактическое занятие
10.4	Самоаудит цифровой безопасности образовательной организации	2	Проектная работа	Заполнить чек-лист самоаудита и определить проблемные зоны школы	Оценивает готовность организации к профилактике и реагированию
11.1	Эмоциональная нагрузка, профессиональные границы и вторичная травматизация	2	Семинар-тренинг	Провести самооценку признаков профессиональной перегрузки	Распознает признаки эмоционального истощения
11.2	Супервизия, командная поддержка и анализ сложного случая	2	Рефлексивный практикум	Разработать личную схему профессиональной поддержки	Использует командные ресурсы и сохраняет профессиональные границы
12.1	Комплексный ситуационный кейс	2	Практический экзамен	Определить риск, срочность, вопросы, маршрут, цифровые сведения и сопровождение	Демонстрирует комплексное применение алгоритма
12.2	Защита итогового практического проекта	2	Защита проекта	Представить локальный алгоритм, профилактическую программу, занятие или методический комплект	Демонстрирует готовность применять материалы курса в образовательной организации

9. МАТРИЦА СООТВЕТСТВИЯ ЦЕЛЕЙ, ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ, РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ОЦЕНИВАНИЯ

№	Задача программы	Формируемая компетенция	Результат обучения	Модули	Оценочное задание	Основные критерии оценивания
1	Сформировать понимание современных цифровых рисков для детей	Диагностико-профилактическая	Определяет основные виды онлайн-рисков и распознает их характерные признаки	1, 2	Анализ ситуационных кейсов	Правильно определен основной риск; выявлены дополнительные риски; названы существенные признаки; отсутствует преждевременная правовая квалификация
2	Научить распознавать кибербуллинг и отличать его от конфликта	Диагностико-профилактическая	Различает единичный конфликт, систематическую травлю и кибербуллинг	2, 10	Кейс «Конфликт или кибербуллинг?»	Установлены признаки систематичности, давления и цифрового канала; определена необходимость школьного реагирования
3	Научить распознавать онлайн-груминг, шантаж и опасное цифровое взаимодействие	Риск-ориентированная	Выявляет признаки установления доверия, секретности, давления, требований и перехода к потенциально опасному контакту	2, 5	Кейс «Друг из игры»	Выделены ключевые признаки; определен уровень риска; предложены безопасные первые действия
4	Сформировать навыки оценки срочности ситуации	Риск-ориентированная	Определяет критический, высокий, средний или консультационный уровень ситуации	5	Алгоритмический тренажер по 10–15 кейсам	Уровень риска определен корректно; решение обосновано; при критическом риске выбран незамедлительный маршрут
5	Сформировать умение проводить минимальный первичный скрининг безопасности	Риск-ориентированная	Устанавливает только сведения, необходимые для понимания текущей безопасности ребенка и дальнейших действий	5	Моделирование первичного разговора	Проверены текущая безопасность, возможность безопасно говорить, наличие угрозы, опасной встречи, шантажа, безопасного взрослого и риска самоповреждения
6	Сформировать навыки безопасной коммуникации с ребенком	Коммуникативная	Ведет разговор без давления, обвинения, стыжения и допроса	4, 8	Рольевая игра «Первые пять минут разговора»	Использует нейтральные вопросы; задает один вопрос за раз; не требует травмирующих подробностей; поддерживает ребенка
7	Научить адаптировать коммуникацию к возрасту ребенка	Коммуникативная	Выбирает соответствующий язык и форму взаимодействия для детей 7–10, 11–14 и 15–17 лет	4, 10	Разработка трех вариантов сообщения	Язык понятен возрасту; отсутствует морализаторство; сохранены смысл и алгоритм безопасности
8	Предупредить повторную травматизацию ребенка	Этическая	Исключает публичный разбор, обвиняющую коммуникацию, повторное требование подробностей и демонстрацию чувствительных материалов	3, 4, 6	Анализ профессиональных ошибок	Определены рискованные действия; предложены безопасные альтернативы; соблюдается достоинство ребенка
9	Сформировать понимание профессиональных границ педагога	Этическая и организационная	Различает педагогическое реагирование и функции следственных, медицинских, психологических и технических специалистов	3	Задание «Можно / нельзя / зависит от ситуации»	Не допускается самостоятельное расследование, поиск нарушителя, контакт с ним, правовая квалификация и цифровая экспертиза
10	Научить соблюдать конфиденциальность	Этическая	Передаст сведения только специалистам, которым они необходимы для защиты ребенка	3, 6, 7	Кейс по передаче конфиденциальной информации	Определен минимально необходимый объем; правильно выбран получатель; исключено публичное распространение
11	Научить безопасно работать с цифровыми сведениями	Цифровая	Фиксирует платформу, аккаунт, ссылку, идентификаторы, время, угрозы и иные необходимые сведения	6	Заполнение карточки первичной фиксации	Зафиксированы необходимые данные; отсутствует избыточный сбор; информация структурирована
12	Предупредить неправомерное обращение с сексуализированным контентом	Цифровая и этическая	Понимает, какие материалы нельзя запрашивать, скачивать, копировать, пересылать или демонстрировать	3, 6	Практикум «Что сохранить — что не сохранять»	Зафиксирован источник/идентификаторы; не предлагается копирование или пересылка чувствительного содержания
13	Сформировать знания о цифровой защите аккаунтов	Цифровая	Объясняет обучающимся и родителям правила приватности, защиты аккаунтов, паролей и двухфакторной аутентификации	6, 9	Разработка чек-листа цифровой защиты	Рекомендации конкретны, понятны, выполнимы и соответствуют возрасту
14	Научить выстраивать школьный маршрут реагирования	Организационная	Определяет последовательность действий педагога, администрации, психологической и социальной службы	7	Разработка карты внутришкольной маршрутизации	Роли распределены; определены последовательность, ответственные и действия при разных уровнях риска
15	Сформировать навыки межведомственного взаимодействия	Организационная	Определяет, в каких ситуациях необходимы КЦ 111, органы внутренних дел, медицинская, психологическая или иная помощь	7, 8	Задание «Кому передать и почему?»	Адресат соответствует характеру риска; срочные ситуации не задерживаются внутри школы; передается минимально необходимая информация
16	Научить сопровождать ребенка после первичного реагирования	Организационная и коммуникативная	Организует дальнейшую педагогическую поддержку после передачи случая профильным специалистам	7, 8	Проект плана сопровождения	Предусмотрены безопасность, психологическая поддержка, недопущение повторной травмы, наблюдение и взаимодействие специалистов

№	Задача программы	Формируемая компетенция	Результат обучения	Модули	Оценочное задание	Основные критерии оценивания
17	Сформировать навыки психологической первой помощи	Коммуникативная	Поддерживает ребенка в состоянии страха, стыда, паники и растерянности в пределах педагогической компетенции	4, 8	Ролевая ситуация	Сохраняется спокойный контакт; признается состояние ребенка; отсутствуют диагнозы и психотерапевтические действия
18	Научить распознавать признаки риска самоповреждения	Риск-ориентированная	Не игнорирует тревожные высказывания и включает срочный алгоритм помощи	5, 8	Ситуационный кейс	Риск распознан; проверена безопасность; предусмотрено незамедлительное подключение соответствующих специалистов
19	Сформировать навыки взаимодействия с родителями	Коммуникативная	Конструктивно сообщает о ситуации и предупреждает обвинение, стыжение и самостоятельное «расследование» родителем	8	Ролевая игра «Разговор с родителем»	Коммуникация спокойная; ребенок не обвиняется; родителю предлагаются конкретные безопасные действия
20	Научить определять безопасного взрослого	Риск-ориентированная и этическая	Учитывает, что не каждый родитель или значимый взрослый автоматически является безопасным для ребенка	8	Анализ сложного семейного кейса	Оценено влияние взрослого на безопасность; исключена передача сведений лицу, способному усилить угрозу
21	Сформировать навыки профилактики онлайн-рисков	Профилактическая	Разрабатывает профилактические мероприятия, ориентированные на формирование навыков, а не запугивание	9, 10	Проект профилактического занятия	Содержание соответствует риску и возрасту; присутствуют алгоритмы действий; исключены травмирующие и морализаторские приемы
22	Научить учитывать возрастные особенности профилактики	Профилактическая и методическая	Дифференцирует профилактический контент для возрастных групп 7–10, 11–14 и 15–17 лет	10	Конструирование трех возрастных вариантов занятия	Соответствие возрасту, уровню самостоятельности, цифровому опыту и типичным рискам
23	Научить организовывать профилактическую работу с родителями	Профилактическая	Разрабатывает рекомендации по семейной цифровой гигиене и доверительной коммуникации	8, 9, 10	Памятка / сценарий родительского собрания	Практичность; отсутствие тотального контроля как основной меры; наличие правил доверительного взаимодействия
24	Сформировать способность к самоаудиту цифровой безопасности школы	Организационно-методическая	Выявляет сильные и проблемные стороны системы профилактики и реагирования образовательной организации	10	Чек-лист самоаудита	Оценены локальные алгоритмы, маршруты, подготовка педагогов, информированность детей и родителей, работа специалистов
25	Сформировать навыки разработки локальных документов	Организационно-методическая	Разрабатывает алгоритм реагирования образовательной организации на онлайн-риски	7, 10, 12	Итоговый проект	Документ содержит уровни риска, последовательность действий, ответственных, маршрутизацию, правила конфиденциальности и сопровождения
26	Сформировать профессиональную устойчивость педагога	Рефлексивная	Распознает признаки эмоциональной перегрузки и соблюдает профессиональные границы	11	Самооценка и рефлексивное задание	Выявлены индивидуальные риски; определены ресурсы поддержки; отсутствует установка на самостоятельное «спасение» ребенка
27	Сформировать культуру профессиональной супервизии	Рефлексивная и командная	Использует консультации специалистов и командный разбор сложных случаев	11	Разработка алгоритма профессиональной поддержки	Определены основания для обращения за помощью; соблюдается конфиденциальность; анализируются действия, а не личность специалиста
28	Проверить интеграцию всех компетенций программы	Комплексная профессиональная компетентность	Применяет полный алгоритм действий при сложной цифровой угрозе	12	Итоговый комплексный кейс	Корректно выполнена последовательность: распознавание → безопасность → коммуникация → уровень риска → фиксация → маршрут → сопровождение
29	Обеспечить перенос результатов обучения в педагогическую практику	Проектировочная	Создает готовый методический продукт для использования в образовательной организации	10, 12	Защита итогового проекта	Практическая применимость, методическая обоснованность, безопасность, соответствие возрасту и возможность внедрения

9.1. Уровни сформированности профессиональных компетенций

Уровень	Характеристика
Высокий	Педагог самостоятельно и обоснованно определяет риск, оценивает срочность, использует безопасную коммуникацию, соблюдает профессиональные границы, правильно фиксирует сведения и выбирает маршрут реагирования.
Достаточный	Основные действия выполняются правильно, но имеются отдельные неточности, которые не создают существенного риска для ребенка.
Базовый	Педагог распознает основную проблему, однако испытывает затруднения при оценке срочности, формулировке вопросов, фиксации сведений или маршрутизации.
Недостаточный	Допускаются действия, способные повысить риск: обвинение ребенка, чрезмерный сбор сведений, неверная оценка срочности, нарушение конфиденциальности, самостоятельное расследование или отсутствие необходимой маршрутизации.

9.2. Рубрика оценки итогового ситуационного кейса

Критерий	Баллы
Правильное определение основного и сопутствующих онлайн-рисков	4
Определение уровня срочности	5
Оценка текущей безопасности ребенка	5
Корректность вопросов педагога	4
Использование поддерживающей коммуникации	4
Соблюдение профессиональных границ	4
Правильность работы с цифровыми сведениями	4
Обоснованность маршрутизации	5
Организация дальнейшего сопровождения	3
Соблюдение конфиденциальности и принципа недопущения повторной травматизации	2
Итого	40

9.3. Рубрика оценки итогового практического проекта

Критерий	Баллы
Актуальность и соответствие проблематике цифровой безопасности ребенка	4
Методическая обоснованность	5
Соответствие возрасту целевой группы	4
Практическая применимость	6
Наличие четкого алгоритма действий	5
Соблюдение принципов безопасности и конфиденциальности	5
Корректность профилактического содержания	4
Возможность использования в образовательной организации	4
Качество представления и защиты проекта	3
Итого	40

10. ОРГАНИЗАЦИЯ УЧЕБНОГО ПРОЦЕССА

Обучение по программе строится на практико-ориентированном, компетентностном и деятельностном подходах. Содержание направлено не только на освоение теоретических знаний о цифровых рисках, но прежде всего на формирование готовности действовать в конкретной профессиональной ситуации.

Основная логика обучения:

ПОНЯТЬ → РАСПОЗНАТЬ → ПРОАНАЛИЗИРОВАТЬ → ПРИНЯТЬ РЕШЕНИЕ → ОТРАБОТАТЬ ДЕЙСТВИЕ → ПОЛУЧИТЬ ОБРАТНУЮ СВЯЗЬ → ПРИМЕНИТЬ В ПРОФЕССИОНАЛЬНОЙ ПРАКТИКЕ

Программа предусматривает сочетание теоретического освоения материала, анализа профессиональных ситуаций, решения учебных кейсов, моделирования разговоров с детьми и родителями, алгоритмических тренажеров, самостоятельной работы, разработки методических продуктов и итогового практического проектирования.

10.1. Принципы организации учебного процесса

Принцип практической направленности. Каждая теоретическая тема завершается практическим действием слушателя: анализом кейса, моделированием разговора, заполнением формы, построением маршрута или разработкой профилактического продукта.

Принцип приоритета безопасности ребенка. Во всех учебных ситуациях первым объектом анализа становится текущая безопасность ребенка. Слушатель учится начинать решение кейса не с поиска виновного или подробностей, а с проверки местонахождения, возможности безопасно говорить, наличия угрозы, опасной встречи и риска самоповреждения.

Принцип «не навреди». При отработке каждого кейса оценивается не только то, что необходимо сделать, но и действия, способные усугубить ситуацию: обвинение ребенка, публичное обсуждение, самостоятельное расследование, требование подробностей, контакт с предполагаемым нарушителем, пересылка чувствительных материалов, обещание негарантированного результата.

Принцип минимально необходимой информации. Педагог получает и фиксирует не максимально возможный, а минимально необходимый объем информации для определения безопасности, срочности, маршрута помощи и передачи соответствующему специалисту.

Принцип возрастной дифференциации. Учебные задания предусматривают работу с возрастными группами 7–10, 11–14 и 15–17 лет с учетом языка общения, уровня самостоятельности, роли родителя или безопасного взрослого и типичных цифровых рисков.

Принцип моделирования профессиональных ситуаций. Слушатель последовательно отрабатывает получение сигнала, установление контакта, первичный разговор, оценку безопасности, определение срочности, фиксацию сведений, выбор маршрута, взаимодействие с ребенком и родителем, дальнейшее сопровождение.

10.2. Формы организации обучения

Интерактивная лекция. Используется для введения ключевых понятий и алгоритмов. Включает проблемный вопрос, краткий теоретический блок, визуальную схему, мини-кейс, обсуждение и проверочный вопрос.

Практический семинар. Предусматривает коллективный анализ онлайн-рисков, признаков опасности, профессиональных ошибок, вариантов маршрутизации и моделей профилактической работы.

Case-study. Кейс строится по схеме: ситуация → признаки → вопросы → оценка риска → действия → маршрут → сопровождение.

Ролевая игра. Используется преимущественно в модулях по коммуникации и взаимодействию с родителями. Основные роли: ребенок, педагог, родитель, педагог-психолог, представитель администрации.

Алгоритмический тренажер. Слушателям предоставляются короткие ситуации, на которые необходимо быстро выбрать профессионально корректное действие и обосновать выбор.

Коммуникативный тренинг. Педагоги отрабатывают начало разговора, нейтральные вопросы, реакцию на страх, молчание, слезы и стыд, завершение разговора и объяснение следующего шага.

Работа в малых группах. Используется для анализа комплексных кейсов, создания карт маршрутизации, подготовки профилактических материалов, анализа школьной системы безопасности и разработки локальных алгоритмов.

Методическая мастерская. Слушатели разрабатывают сценарии классных часов, кейсы для обучающихся, памятки, чек-листы, материалы для родителей, упражнения, алгоритмы действий и формы самоаудита.

Проектная работа. Итоговый профессиональный продукт формируется поэтапно в течение всей программы, а не только на итоговой аттестации.

10.3. Поэтапное формирование итогового проекта

- Модуль 2 - карта цифровых рисков.
- Модуль 4 - набор безопасных формулировок.

- Модуль 5 - алгоритм первичного скрининга.
- Модуль 6 - форма фиксации цифровых сведений.
- Модуль 7 - карта маршрутизации.
- Модуль 9 - профилактические рекомендации.
- Модуль 10 - сценарий профилактического занятия.
- Модуль 12 - объединение элементов в единый итоговый методический продукт.

10.4. Рекомендуемая структура одного 2-часового занятия

Время	Содержание
10 минут	актуализация опыта и постановка проблемы
20 минут	теоретический блок
15 минут	демонстрация алгоритма
30 минут	решение кейса или ролевая работа
15 минут	обсуждение решений
10 минут	работа с чек-листом или памяткой
10 минут	рефлексия и фиксация индивидуального результата

10.5. Роль преподавателя / тренера

- эксперт;
- методист;
- фасилитатор;
- модератор кейс-анализа;
- организатор практической деятельности;
- эксперт итоговых проектов.

При разборе сложных ситуаций преподаватель не стимулирует поиск «виновного», а возвращает обсуждение к профессиональной логике: что представляет угрозу → что необходимо сделать сейчас → кто обладает соответствующими полномочиями → как обеспечить безопасность ребенка.

10.6. Требования к безопасности учебных материалов

При проведении обучения рекомендуется использовать моделируемые, обезличенные или адаптированные ситуации. Не допускается использование:

- реальных интимных материалов несовершеннолетних;
- травмирующих фото и видео;
- персональных данных реальных пострадавших детей;
- материалов, позволяющих идентифицировать конкретного ребенка;
- публичного детального обсуждения личного опыта слушателя без его инициативы.

Учебный кейс должен содержать только ту информацию, которая необходима для выполнения профессионального задания.

11. ВХОДНАЯ ДИАГНОСТИКА И ТЕКУЩИЙ КОНТРОЛЬ

11.1. Входная диагностика

Перед началом программы рекомендуется проведение входной диагностики. Ее цель — определить исходный уровень понимания онлайн-рисков, готовность педагогов к реагированию, типичные ошибочные представления и профессиональные потребности слушателей.

Рекомендуемый формат - 15–20 заданий. Предпочтительно использовать не только вопросы на знание терминологии, но и короткие профессиональные ситуации. Входная диагностика не влияет на итоговую оценку, а используется для определения исходного уровня слушателя.

11.2. Текущий контроль по модулям

Модуль	Форма текущего контроля
Модуль 1	Карта цифровых рисков образовательной организации
Модуль 2	Анализ ситуационного кейса
Модуль 3	Задание «Можно / нельзя / зависит от ситуации»

Модуль	Форма текущего контроля
Модуль 4	Ролевая игра и коммуникативный тренажер
Модуль 5	Определение уровня срочности по ситуационным карточкам
Модуль 6	Заполнение формы минимальной фиксации
Модуль 7	Карта внутришкольной и межведомственной маршрутизации
Модуль 8	Ролевая ситуация «Разговор с родителем»
Модуль 9	Памятка по цифровой гигиене
Модуль 10	Проект профилактического занятия
Модуль 11	Рефлексивная карта профессиональной поддержки
Модуль 12	Итоговый кейс и защита проекта

12. САМОСТОЯТЕЛЬНАЯ РАБОТА

Самостоятельная работа занимает 20 академических часов и направлена на перенос изучаемого содержания в конкретную профессиональную среду слушателя.

Основные виды самостоятельной работы включают анализ профессиональной практики, решение учебных кейсов, разработку памяток, проектирование профилактического занятия, самоаудит образовательной организации и подготовку итогового проекта.

Задание	Часы
Карта цифровых рисков своей образовательной организации	2
Анализ двух ситуационных кейсов	2
Разработка памятки безопасной коммуникации	2
Разработка формы первичного скрининга	2
Карта маршрутизации	3
Чек-лист цифровой гигиены	2
Самоаудит образовательной организации	2
Разработка профилактического занятия	2
Подготовка итогового проекта	3
Итого	20

13. ФОРМИРУЮЩЕЕ И ИТОВОЕ ОЦЕНИВАНИЕ

13.1. Обратная связь в процессе обучения

После практических заданий применяется формирующая обратная связь. Преподаватель оценивает не личность слушателя, а профессиональное действие. Рекомендуемая модель:

15. Что было сделано правильно?
16. Что может создать риск?
17. Что следует изменить?
18. Как выглядит профессионально безопасный вариант?

13.2. Формирующее оценивание

ЗНАЮ → ПОНИМАЮ → ПРИМЕНЯЮ → ОБОСНОВЫВАЮ → ПРОЕКТИРУЮ

Знаю: педагог называет виды онлайн-рисков.

Понимаю: объясняет, почему ситуация является опасной.

Применяю: выбирает корректное действие.

Обосновываю: аргументирует выбранный уровень срочности или маршрут.

Проектирую: разрабатывает собственный алгоритм, занятие, памятку или профилактическую систему.

13.3. Итоговая аттестация

Итоговая аттестация предусматривает три компонента:

Вид контроля	Максимальный балл	Доля
Итоговое тестирование	20	20 %
Комплексный ситуационный кейс	40	40 %
Практический проект	40	40 %
Итого	100	100 %

13.4. Структура итогового тестирования

- 5 заданий на распознавание онлайн-рисков;
- 5 заданий на определение уровня срочности;
- 4 задания на профессиональные границы;
- 3 задания на цифровые сведения и конфиденциальность;
- 3 задания на коммуникацию и маршрутизацию.

Рекомендуемая модель: 1 правильный ответ = 1 балл. Тестирование должно преимущественно проверять выбор профессионально корректного действия, а не механическое запоминание терминов.

13.5. Требования к итоговому проекту

Итоговый проект должен соответствовать проблематике программы, иметь четко определенную целевую группу, содержать конкретный профессиональный алгоритм, учитывать возраст детей, предусматривать безопасную коммуникацию и конфиденциальность, включать практические инструменты и быть пригодным для использования в образовательной организации.

Рекомендуемый объем письменного проекта — 8–15 страниц без учета приложений. К проекту могут прилагаться памятки, чек-листы, схемы, формы, сценарии, алгоритмы и карточки кейсов.

13.6. Интерпретация итогового результата

Результат	Уровень освоения
90–100 баллов	высокий
75–89 баллов	достаточный
70–74 балла	базовый
менее 70 баллов	программа не освоена на требуемом уровне

Минимальный рекомендуемый порог успешного завершения программы — 70 баллов из 100.

14. ПОСТКУРСОВОЕ СОПРОВОЖДЕНИЕ И МОНИТОРИНГ

Посткурсовое сопровождение направлено на поддержку переноса сформированных компетенций в реальную профессиональную деятельность. Рекомендуемая продолжительность сопровождения — до 6 месяцев после окончания программы.

14.1. Основные формы посткурсового сопровождения

- методические консультации по внедрению локальных алгоритмов, профилактической работе и разработке материалов;
- профессиональное сообщество выпускников для обмена методическими материалами и профилактическими практиками;
- разбор обезличенных кейсов без раскрытия персональных данных детей;
- вебинары актуализации с учетом новых социальных сетей, игровых платформ, мошеннических схем, ИИ-инструментов, дипфейков и новых способов социальной инженерии.

14.2. Мониторинг посткурсовых результатов

Через 3–6 месяцев после обучения рекомендуется провести короткий мониторинг. Слушатель отвечает:

- использовал ли материалы программы;
- проводил ли профилактические занятия;
- разработан ли локальный алгоритм;
- проводилась ли работа с родителями;
- возникали ли ситуации онлайн-рисков;
- какие затруднения возникли;
- какие дополнительные материалы необходимы.

15. ПРОФЕССИОНАЛЬНОЕ ПОРТФОЛИО СЛУШАТЕЛЯ

К завершению курса педагог должен иметь собственное профессиональное портфолио цифровой безопасности, включающее:

- карту основных онлайн-рисков;
- алгоритм первичного реагирования;
- перечень безопасных вопросов;
- перечень поддерживающих фраз;
- памятку «что нельзя делать педагогу»;
- карточку первичного скрининга;
- форму минимальной фиксации цифровых сведений;
- карту маршрутизации;
- памятку для родителей;
- памятку для ребенка;
- чек-лист цифровой гигиены;
- сценарий профилактического занятия;
- результаты самоаудита образовательной организации;
- итоговый практический проект.

16. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Основными материалами курса являются:

- Методические указания КЦ 111 по профилактике и реагированию на киберпреступления и онлайн-риски в отношении несовершеннолетних.
- Учебное пособие «Цифровая безопасность ребенка: профилактика и первичное реагирование педагога на киберпреступления и онлайн-риски».
- Матрицы определения онлайн-рисков.
- Учебные кейсы.
- Чек-листы.
- Формы первичной фиксации.
- Карта школьной и межведомственной маршрутизации.
- Памятки для детей, родителей и педагогов.
- Материалы для профилактических занятий.
- Инструменты самооценки педагогов и самоаудита образовательной организации.

Перечень нормативных правовых актов, официальных контактов служб и цифровых платформ подлежит обязательной актуализации перед утверждением и запуском программы.

17. ИТОГОВАЯ МОДЕЛЬ РЕЗУЛЬТАТА ПРОГРАММЫ

Независимо от конкретного модуля в ходе обучения последовательно формируются восемь сквозных профессиональных действий педагога:

РАСПОЗНАТЬ: определить признаки возможной цифровой угрозы.

ПРОВЕРИТЬ БЕЗОПАСНОСТЬ: понять, существует ли непосредственная угроза ребенку.

ПОДДЕРЖАТЬ: сохранить доверительный контакт без обвинения и давления.

ОПРЕДЕЛИТЬ СРОЧНОСТЬ: выбрать соответствующий уровень и скорость реагирования.

НЕ НАВРЕДИТЬ: не проводить расследование, не требовать травмирующих подробностей и не распространять чувствительную информацию.

ЗАФИКСИРОВАТЬ МИНИМУМ: сохранить только те сведения, которые действительно необходимы для помощи.

ПЕРЕДАТЬ ПО МАРШРУТУ: подключить соответствующих специалистов и службы.

СОПРОВОЖДАТЬ И ПРОФИЛАКТИРОВАТЬ: продолжить педагогическую поддержку ребенка и использовать полученный опыт для системной профилактической работы.

17.1. Интегрированная профессиональная последовательность

ЗАМЕТИТЬ СИГНАЛ → РАСПОЗНАТЬ РИСК → УСТАНОВИТЬ БЕЗОПАСНЫЙ КОНТАКТ → ПРОВЕРИТЬ ТЕКУЩУЮ БЕЗОПАСНОСТЬ → ОПРЕДЕЛИТЬ УРОВЕНЬ СРОЧНОСТИ → ОКАЗАТЬ ПЕРВИЧНУЮ ПОДДЕРЖКУ → ЗАФИКСИРОВАТЬ МИНИМАЛЬНО НЕОБХОДИМЫЕ СВЕДЕНИЯ → ПЕРЕДАТЬ ИНФОРМАЦИЮ ПО КОМПЕТЕНЦИИ → ОРГАНИЗОВАТЬ ПЕДАГОГИЧЕСКОЕ СОПРОВОЖДЕНИЕ → ПРОВЕСТИ ПРОФИЛАКТИЧЕСКУЮ РАБОТУ

Именно способность педагога применять данную последовательность в моделируемой и реальной профессиональной ситуации является основным показателем результативности программы повышения квалификации.