

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное учреждение
РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ

Центр развития высшего и среднего профессионального образования



УТВЕРЖДЕНО:

Вице-президент РАО,
доктор психологических наук,
академик РАО

 /В.С. Басюк/

« 29 » сентября 202 6 г.

Дополнительная профессиональная программа повышения квалификации

**«Гибридные угрозы в образовательной среде: управленческие
механизмы и устойчивость образовательной организации»**

(16 академических часов)

Авторы-составители:

Карпович Олег Геннадьевич,
член-корреспондент РАО, доктор
юридических наук, доктор политических
наук, профессор.

Савина Юлия Григорьевна, кандидат
педагогических наук, доцент.

Москва, 2026

Раздел 1. Характеристика программы

1.1. Цель реализации программы.

Совершенствование профессиональных компетенций руководителей образовательных организаций высшего и среднего профессионального образования в области выявления, оценки и нейтрализации гибридных вызовов в образовательной среде, а также формирование навыков проектирования управленческих решений, обеспечивающих устойчивость образовательной среды и непрерывность образовательного процесса.

Планируемые результаты обучения

Планируемые результаты обучения (ВО)

Трудовая функция	Трудовое действие	Знать	Уметь
Реализация стратегических целей и задач, программ развития образовательной организации (А/01.9 – ВО)	Диагностика рисков и уязвимостей образовательной среды	Методы и технологии оценки рисков и управления ими; законодательство РФ в сфере образования, стратегического планирования и проектного управления; приоритетные направления федеральной и региональной политики в сфере ВО; типологию гибридных угроз (информационно-психологические, ценностно-смысловые, организационные, технологические) и индикаторы риска в образовательной среде ВО.	Вырабатывать варианты решений и оценивать риски; учитывать требования законодательства РФ и отраслевых стандартов при управлении рисками; определять приоритетные направления развития ОО и готовить программные документы; определять качественные и количественные плановые показатели; использовать технологии проектирования и прогнозирования; составлять карту рисков; расставлять приоритеты рисков с учётом специфики ОО.

Обеспечение соблюдения законности и правопорядка, антикоррупционной и антитеррористической политики (А/08.9 – ВО);	Организация системы защиты и реагирования на инциденты гибридных вызовов в образовательной сфере; обеспечение комплексной безопасности ОО; управление разработкой локальных нормативных актов.	Законодательство РФ, регламентирующее образовательную деятельность, охрану труда, безопасность жизнедеятельности; законодательство о противодействии коррупции и антитеррористической деятельности; требования к оформлению и порядку разработки локальных нормативных актов; основания и порядок привлечения к дисциплинарной ответственности; особенности деструктивного поведения обучающихся, подверженных воздействию радикальной идеологии; нормативно-правовую базу противодействия гибридным вызовам; базовые контуры защиты (административный, воспитательный, цифровой, коммуникационный)	Координировать деятельность по профилактике правонарушений и коррупции; определять меры по предотвращению правонарушений; использовать справочно-правовые информационные системы; разрабатывать локальные нормативные акты (регламенты, приказы, дорожные карты); выстраивать алгоритмы реагирования на типовые инциденты; проектировать сценарии кризисных коммуникаций; обеспечивать взаимодействие с родителями (законными представителями) обучающихся по вопросам профилактики деструктивного поведения.
Взаимодействие с государственными органами, органами местного самоуправления, работодателями, профессиональными сообществами (А/09.9 – ВО)	Организация взаимодействия и внедрения решений	Структуру и компетенцию органов государственной власти и местного самоуправления, порядок межведомственного взаимодействия; законодательство РФ в сфере образования; основы правового регулирования государственно-частного партнёрства; основы делового	Выбирать оптимальные формы сотрудничества с работодателями и профессиональными сообществами; вести переговоры и деловую переписку с соблюдением норм делового этикета; использовать законные способы защиты интересов

		этикета и делового общения, включая сетевую коммуникацию посредством ИКТ; основы функционирования государственных информационных систем; эффективные формы коммуникации и партнёрства; модели сетевого взаимодействия по вопросам устойчивости образовательной среды; функционал сетевых инновационных площадок РАО; механизмы апробации и тиражирования решений.	ОО в органах власти; организовывать использование ИТ для обеспечения информационной открытости ОО; организовывать подготовку презентационных и информационно-аналитических материалов; организовывать межведомственное взаимодействие; формировать рабочие группы; планировать мероприятия с измеримыми результатами.
--	--	--	--

Планируемые результаты обучения (СПО)

Трудовая функция	Трудовое действие	Знать	Уметь
Реализация стратегических целей и задач, программ развития образовательной организации (С/02.7 – СПО)	Диагностика рисков и уязвимостей образовательной среды	Методы и технологии оценки рисков и управления ими; законодательство РФ в сфере образования, стратегического планирования и проектного управления; приоритетные направления федеральной и региональной политики в сфере СПО; типологию гибридных угроз (информационно-психологические, ценностно-смысловые, организационные,	Вырабатывать варианты решений и оценивать риски; учитывать требования законодательства РФ и отраслевых стандартов при управлении рисками; определять приоритетные направления развития ОО и готовить программные документы; определять качественные и количественные

		технологические) и индикаторы риска в образовательной среде ВО/СПО.	плановые показатели; использовать технологии проектирования и прогнозирования; составлять карту рисков; расставлять приоритеты рисков с учётом специфики ОО.
Руководство деятельностью по профилактике деструктивного поведения, формированию психологической, антитеррористической и информационной безопасности (В/02.6 – СПО)	Организация системы защиты и реагирования на инциденты гибридных вызовов в образовательной сфере; обеспечение комплексной безопасности ОО; управление разработкой локальных нормативных актов.	Законодательство РФ, регламентирующее образовательную деятельность, охрану труда, безопасность жизнедеятельности; законодательство о противодействии коррупции и антитеррористической деятельности; требования к оформлению и порядку разработки локальных нормативных актов; основания и порядок привлечения к дисциплинарной ответственности; особенности деструктивного поведения обучающихся, подверженных воздействию радикальной идеологии; нормативно-правовую базу противодействия гибридным вызовам; базовые контуры защиты (административный, воспитательный, цифровой, коммуникационный)	Координировать деятельность по профилактике правонарушений и коррупции; определять меры по предотвращению правонарушений; использовать справочно-правовые информационные системы; разрабатывать локальные нормативные акты (регламенты, приказы, дорожные карты); выстраивать алгоритмы реагирования на типовые инциденты; проектировать сценарии кризисных коммуникаций; обеспечивать взаимодействие с родителями (законными представителями) обучающихся по вопросам профилактики деструктивного поведения.
Взаимодействие с государственными органами, органами местного	Организация взаимодействия и внедрения решений	Структуру и компетенцию органов государственной власти и местного	Выбирать оптимальные формы сотрудничества

самоуправления, работодателями, профессиональными сообществами (С/03.7 – СПО)		самоуправления, порядок межведомственного взаимодействия; законодательство РФ в сфере образования; основы правового регулирования государственно-частного партнёрства; основы делового этикета и делового общения, включая сетевую коммуникацию посредством ИКТ; основы функционирования государственных информационных систем; эффективные формы коммуникации и партнёрства; модели сетевого взаимодействия по вопросам устойчивости образовательной среды; функционал сетевых инновационных площадок РАО; механизмы апробации и тиражирования решений.	с работодателями и профессиональными сообществами; вести переговоры и деловую переписку с соблюдением норм делового этикета; использовать законные способы защиты интересов ОО в органах власти; организовывать использование ИТ для обеспечения информационной открытости ОО; организовывать подготовку презентационных и информационно-аналитических материалов; организовывать межведомственное взаимодействие; формировать рабочие группы; планировать мероприятия с измеримыми результатами.
---	--	--	---

1.2. Категория слушателей: руководители образовательных организаций (ректоры, директора), заместители руководителей (проректоры, заместители директоров) по учебно-методической, воспитательной, цифровой работе вузов и колледжей.

1.3. Уровень образования слушателей: высшее образование (специалитет, магистратура).

1.4. Форма обучения: очно-заочная с применением дистанционных образовательных технологий (ДОТ).

1.5. Срок освоения программы: 16 академических часов.

Раздел 2. Содержание программы

2.1. Учебный (тематический) план

№ п/п	Наименование модулей (разделов), тем	Всего часов	Виды учебных занятий, учебных работ			Формы контроля
			Лекции	Семинары	Самост. работа	
1.	Теоретические и правовые основы противодействия гибридным вызовам и угрозам в сфере образования	4	2	2	–	Текущий контроль: тест (10 вопросов), выполнение письменного задания (подбор 2–3 нормативных документов, формулировка 1–2 рисков).
2.	Типология и специфика проявления гибридных угроз в образовательной среде (ВО/СПО)	4	1	2	1	Текущий контроль: заполнение оценочного листа уязвимостей (10–15 пунктов), карты рисков (3–5 позиций) с обоснованием.
3.	Методы и инструменты противодействия гибридным вызовам в сфере образования	6	1	4	1	Текущий контроль: составление регламента реагирования и дорожная карта (8–10 мероприятий с ответственными, сроками и КПЭ).
4.	Итоговая аттестация	2	–	2	–	Защита педагогического продукта (карта рисков, регламент, дорожная карта, коммуникационный план), публичное выступление (5–

						7 минут) с презентацией (7–10 слайдов)
Итого:		16	4	10	2	

2.3. Календарный учебный график

№ п/п	Наименование модулей (разделов), вид аттестации	Всего (ч)	Учебные недели		
			1 неделя (ч)	2 неделя (ч)	3 неделя (ч)
I.	Раздел 1. «Теоретические и правовые основы противодействия гибридным вызовам и угрозам в сфере образования»	4	4	–	–
II.	Раздел 2. «Типология и специфика проявления гибридных угроз в образовательной среде (ВО/СПО)»	4	–	4	–
III	Раздел 3. Методы и инструменты противодействия гибридным вызовам в сфере образования	6	–	2	4
IV	Итоговая аттестация (конференция, защита мини-проекта)	2	–	–	2
Итого		16	4	6	6

Раздел 3. Формы аттестации и оценочные материалы

3.1. Текущая аттестация

Текущая аттестация проводится по итогам освоения каждого модуля и включает формы контроля, установленные учебным (тематическим) планом (п. 2.1).

3.2. Итоговая аттестация

Форма итоговой аттестации	Конференция с защитой мини-проекта «Пакет управленческих решений по противодействию гибридным угрозам для (название своей организации)» (публичное выступление 5-7 минут + презентация 7-10 слайдов)
Требования к итоговой аттестации	Педагогический продукт должен включать: 1) карту рисков-вызовов (3-5 позиций) с типом угрозы, индикатором, уровнем, зоной ответственности и последствиями; 2) регламент реагирования (1-2 страницы) с алгоритмом действий, ролями, сроками и каналами коммуникации; 3) дорожную карту (8-10 мероприятий на 3-6 месяцев) с ответственными, сроками и показателями (ключевые показатели эффективности (КПЭ)); 4) коммуникационный план с шаблонами 3-4 типовых сообщений для внутренней аудитории, студентов, родителей и СМИ; 5) публичное выступление с логикой «проблема – решение – результат» и ответами на вопросы комиссии.
Критерии оценивания	- Реализуемость решений (учёт ресурсов и специфики ОО) – до 1 балла. - Нормативная корректность (соответствие нормативными документам и установленными полномочиям ОО) – до 1 балла. - Измеримость результатов (чёткие ключевые показатели эффективности (КПЭ), сроки, ответственные) – до 1 балла. - Учёт специфики ВО/СПО (возрастные группы, модели управления, цифровая зрелость) – до 1 балла. - Качество публичного выступления (логика, ясность, ответы на вопросы) – до 1 балла.
Оценка	Зачтено/не зачтено

Перевод баллов в оценку: 4-5 баллов – зачтено; 3 балла – зачтено при условии доработки по замечаниям комиссии; менее 3 баллов – не зачтено (требуется повторная защита с доработкой).

Список тем для мини-проектов (на выбор слушателя)

1. «Проектирование контура защиты воспитательной среды колледжа от ценностно-смысловых угроз».
2. «Алгоритм реагирования вуза на информационные атаки в социальных сетях».
3. «Дорожная карта повышения устойчивости цифровой среды колледжа к технологическим угрозам».
4. «Организация межведомственного взаимодействия по противодействию гибридным вызовам в сфере образования на региональном уровне».
5. «Модель взаимодействия вузов и колледжей для обмена лучшими практиками устойчивости к противодействию гибридных вызовов в сфере образования».
6. «Принципы построения системы кризисных коммуникаций как элемента управленческой устойчивости образовательной организации».

7. «План кризисных коммуникаций образовательной организации (педагогический/организационный продукт): методология проектирования и управленческая логика реализации (на примере вуза/колледжа)».

8. «Регламент мониторинга рисков гибридных вызовов для образовательной организации».

9. «Карта рисков гибридных вызовов и меры защиты молодёжных пространств в колледже».

10. «Проект приказа о создании рабочей группы по противодействию гибридным вызовам в образовательной организации (с обоснованием и мерами противодействия)».

11. «Интеграция механизмов защиты в систему управления качеством образовательной организации».

12. Проектирование контура защиты воспитательной среды ОО от ценностно-смысловых угроз».

13. «Алгоритм реагирования ОО на информационные угрозы в родительских чатах и социальных сетях».

14. «Карта рисков гибридных вызовов и меры защиты воспитательной среды ОО».

3.3. Оценочные материалы

3.3.1. Раздел 1. «Теоретические и правовые основы противодействия гибридным вызовам и угрозам в сфере образования».

Форма контроля по плану: тест (10 вопросов), выполнение письменного задания (подбор 2–3 нормативных документов, формулировка 1–2 рисков).

Тест с выбором одного правильного ответа

Инструкция: выберите один верный вариант.

1. Какой признак наиболее точно характеризует «гибридность» угрозы в образовательной среде?

А) Угроза исходит только из внешнего источника.

Б) Угроза сочетает информационные, ценностно-смысловые, организационные и технологические компоненты.

В) Угроза проявляется исключительно в цифровой среде.

Г) Угроза может быть устранена только силовыми методами.

Правильный ответ: Б.

2. Какой документ имеет прямое отношение к формированию устойчивости образовательной среды к деструктивному информационному воздействию?

А) Локальный акт о порядке проведения промежуточной аттестации.

Б) Стратегия национальной безопасности РФ.

В) Положение о студенческом самоуправлении.

Г) Регламент работы библиотеки.

Правильный ответ: Б.

3. Что из перечисленного относится к ценностно-смысловым угрозам?

А) DDoS-атака на сайт вуза.

Б) Распространение фейков о расписании экзаменов.

В) Продвижение в молодёжной среде установок, разрушающих традиционные ценности и социальную сплочённость.

Г) Сбой системы электронного документооборота.

Правильный ответ: В.

5. Какой функциональный контур защиты включает разработку регламентов, приказов и дорожных карт?

А) Воспитательный.

Б) Цифровой.

В) Административный.

Г) Коммуникационный.

Правильный ответ: В.

6. Что относится к технологическим угрозам в образовательной среде?

А) Массовая рассылка фейка о закрытии вуза.

Б) Продвижение деструктивной идеологии в студенческих чатах.

В) Кибератака, утечка данных, компрометация цифровых сервисов.

Г) «Тихий саботаж» при внедрении новой системы.

Правильный ответ: В.

7. Какой принцип лежит в основе матрицы оценки уровня риска?

А) Вероятность × Стоимость.

Б) Вероятность × Последствия.

В) Частота × Длительность.

Г) Ущерб × Время реакции.

Правильный ответ: Б.

8. Какой индикатор риска соответствует организационной угрозе?

А) Рост числа жалоб в студенческих чатах.

Б) Появление материалов с деструктивной идеологией.

В) Увеличение конфликтов между подразделениями, срывы сроков согласований.

Г) Аномальная активность в учётных записях.

Правильный ответ: В.

9. Что является ключевым отличием гибридных угроз от установленных законом угроз безопасности?

А) Гибридные угрозы всегда исходят из-за рубежа.

Б) Гибридные угрозы сочетают разнородные компоненты, взаимно усиливающие друг друга.

В) Гибридные угрозы действуют только в цифровой среде.

Г) Гибридные угрозы не подпадают под действие законодательства РФ.

Правильный ответ: Б.

10. Какой документ определяет требования к антитеррористической защищённости образовательных организаций?

- А) Постановление Правительства РФ от 02.08.2019 № 1006.
 Б) ФЗ-273 «Об образовании в РФ».
 В) Указ Президента РФ от 05.12.2016 № 646.
 Г) Распоряжение Правительства РФ от 29.05.2015 № 996-р.

Правильный ответ: А.

Критерии оценивания:

Количество правильных ответов	Оценка
9-10	«Отлично»
7-8	«Хорошо»
5-6	«Удовлетворительно»
менее 5	«Неудовлетворительно»

Письменное задание: подбор нормативных документов и формулировка рисков

Инструкция: выберите 2-3 нормативных документа из области деятельности своей организации (ВО или СПО), регулирующих вопросы безопасности и противодействия деструктивным влияниям в сфере образования. Для каждого документа кратко укажите, какие риски он позволяет нейтрализовать. Сформулируйте 1-2 риска, которые подлежат выявлению и нейтрализации в вашей образовательной организации.

Шаблон выполнения:

№	Нормативный документ (название, дата, номер)	Риски, нейтрализуемые документом	Риск для вашей ОО (формулировка)
1			
2			
3			

Пример выполнения:

№	Нормативный документ (название, дата, номер)	Риски, нейтрализуемые документом	Риск для вашей ОО (формулировка)
1	ФЗ-273 «Об образовании в РФ», ст. 43 — обязанности и ответственность обучающихся	Нарушение дисциплины, деструктивное поведение в образовательной среде	Рост конфликтов в учебных группах, связанных с распространением манипулятивного контента в чатах
2	Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности РФ»	Информационно-психологическое воздействие на молодёжь, подрыв ценностных основ	Низкая устойчивость студентов к информационно-психологическим манипуляциям из внешних источников

Критерии оценивания:

- Выбрано не менее 2 нормативных документов, релевантных деятельности ОО (ВО/СПО) – 1 балл.
- Для каждого документа корректно указаны нейтрализуемые риски – 1 балл.
- Сформулированы 1–2 риска, специфичные для конкретной ОО, с привязкой к типологии гибридных угроз – 1 балл.

Перевод баллов: 3 балла – зачтено; 2 балла – зачтено при условии доработки; менее 2 – не зачтено.

Вопросы для устной проверки и дискуссии

1. Какие признаки отличают гибридные угрозы от установленных в соответствии с законом угроз безопасности? Приведите 2–3 критерия.
2. Назовите 3 ключевых документа (ФЗ, стратегия, приказ), которые регулируют вопросы безопасности и противодействия деструктивным влияниям в сфере образования, и кратко укажите, какие риски они позволяют нейтрализовать.
3. Как понятие «гибридность» отражается в структуре угроз (информационные, ценностные, организационные, технологические компоненты)?

3.3.2. Раздел 2. «Типология и специфика проявления гибридных угроз в образовательной среде (ВО/СПО)».

Форма контроля по плану: заполнение оценочного листа уязвимостей (10–15 пунктов), карты рисков (3–5 позиций с обоснованием).

Заполнение оценочного листа уязвимостей
по функциональным контурам защиты (10–15 пунктов)

Формат: таблица.

Инструкция: заполните оценочный лист уязвимостей по 4 функциональным контурам защиты (административный, воспитательный, цифровой, коммуникационный). Для каждой уязвимости укажите контур защиты, уровень риска (В/С/Н), меру/решение, ответственного и срок. Объём — не менее 10 пунктов (по 2–4 на каждый контур).

Шаблон заполнения:

Функциональный контур	Уязвимость	Уровень риска (В/С/Н)	Мера/решение	Ответственный	Срок
Административный					
Воспитательный					
Цифровой					
Коммуникационный					
Воспитательный					

Образец заполнения (фрагмент):

Функциональный контур	Уязвимость	Уровень риска (В/С/Н)	Мера/решение	Ответственный	Срок
Административный	Нет регламента реагирования на инциденты гибридных вызовов	В	Разработать и утвердить регламент	Проректор по безопасности	До 30.09.2026
Воспитательный	Не все кураторы обучены распознаванию ценностно-смысловых угроз	С	Провести обучение кураторов, выдать чек-лист	Куратор воспитательной работы	До 15.10.2026
Цифровой	Мониторинг студенческих чатов фрагментарный, нет единого реестра чатов	С	Сформировать реестр чатов, настроить регулярный мониторинг	ИТ-служба	До 20.10.2026
Коммуникационный	Нет шаблонов кризисных	В	Подготовить 4 шаблона (сотрудники,	Пресс-служба	До 25.10.2026

	сообщений для разных аудиторий		студенты, родители, СМИ)		
--	--------------------------------------	--	--------------------------------	--	--

Критерии: не менее 10 строк (по всем 4 контурам), по каждой заполнены все столбцы, уровни риска обоснованы – «зачтено». Если заполнено менее 8 строк или есть грубые несоответствия (пустой «срок», не указан «ответственный») — «не зачтено».

Заполнение карты рисков-вызовов (3-5 позиций с обоснованием).

Инструкция: заполните карту рисков-вызовов из 3–5 позиций. Для каждой позиции укажите: тип угрозы, индикатор риска, уровень угрозы (высокий/средний/низкий), зону ответственности, возможные последствия. Добавьте краткое обоснование выбора (1–2 предложения на позицию) с учётом специфики вашей ОО (ВО/СПО), возрастных групп, цифровой зрелости и модели управления.

Критерии оценивания (4 балла):

Критерий	Балл
Все 3–5 позиций карты рисков содержат корректный тип угрозы, понятный индикатор, обоснованный уровень и зону ответственности.	1
Оценочный лист заполнен не менее чем на 10 пунктов, по каждому указаны уязвимость, контур защиты и мера/решение.	1
Обоснования выбора рисков учитывают специфику ОО (ВО/СПО), возрастные группы, цифровую зрелость и модели управления.	1
Отсутствие грубых ошибок в типологии угроз (например, смешение разных типов без дифференциации).	1

Перевод баллов: 3–4 балла — зачтено; менее 3 баллов — не зачтено (требуется доработка с повторной сдачей).

Шаблон карты рисков:

№	Тип угрозы	Индикатор риска	Уровень угрозы (В/С/Н)	Зона ответственности	Возможные последствия	Обоснование выбора
1						

№	Тип угрозы	Индикатор риска	Уровень угрозы (В/С/Н)	Зона ответственности	Возможные последствия	Обоснование выбора
2						
3						

Образец заполнения (фрагмент, колледж СПО):

№	Тип угрозы	Индикатор риска	Уровень угрозы	Зона ответственности	Возможные последствия	Обоснование выбора
1	Информационно-психологическая	Распространение фейка о «закрытии колледжа» в студенческих чатах; рост негативных публикаций в соцсетях за неделю	Высокий	ИТ-служба, кураторы	Массовые пропуски занятий, паника среди родителей, репутационный ущерб	Колледж характеризуется высокой плотностью неформальных коммуникаций в мессенджерах; возрастная группа (15–18 лет) имеет повышенную восприимчивость к эмоционально окрашенным фейкам
	Ценностно-смысловая	Появление в чатах материалов с деструктивной идеологией; рост вовлечённости студентов в «токсичные» сообщества	Высокий	Отдел воспитательной работы	Снижение устойчивости к манипуляциям, эскалация конфликтов на ценностной почве	Опрос кураторов показал, что менее 50% обучены распознаванию ценностно-смысловых угроз; низкая цифровая грамотность части студентов
	Организационная	Увеличение конфликтов между подразделениями, срывы сроков согласования решений по безопасности	Средний	Руководство ОО, юридический отдел	Хаотичные действия при инциденте, юридические риски, невозможность оценки эффективности мер	В локальных актах не прописаны процедуры межведомственного взаимодействия при инцидентах; отсутствует утверждённая дорожная карта

Критерии оценивания (4 балла):

Критерий	Балл
Все 3–5 позиций карты рисков содержат корректный тип угрозы, понятный индикатор, обоснованный уровень и зону ответственности.	1
Оценочный лист заполнен не менее чем на 10 пунктов, по каждому указаны уязвимость, контур защиты и мера/решение.	1
Обоснования выбора рисков учитывают специфику ОО (ВО/СПО), возрастные группы, цифровую зрелость и модели управления.	1
Отсутствие грубых ошибок в типологии угроз (например, смешение разных типов без дифференциации).	1

Перевод баллов:

3–4 балла — зачтено; менее 3 — не зачтено (требуется доработка с повторной сдачей).

Вопросы для устной проверки и дискуссии

- Приведите по 1 примеру для каждого типа гибридных угроз (информационно-психологические, ценностно-смысловые, организационные, технологические) применительно к образовательной организации.
- По каким индикаторам можно выявить ценностно-смысловые угрозы в студенческой среде? Назовите 3–4 маркера.
- Как связаны функциональные контуры защиты (административный, воспитательный, цифровой, коммуникационный) с типами угроз? Приведите по одному примеру соответствия.
- Объясните, как контент-анализ коммуникаций может применяться для экспресс-диагностики уязвимостей ОО.
- Как специфика колледжа (СПО) влияет на проявление гибридных угроз по сравнению с вузом (ВО)? Назовите 2–3 отличия.

3.3.3. Раздел 3. «Методы и инструменты противодействия гибридным вызовам в сфере образования».

Форма контроля по плану: составление регламента реагирования и дорожной карты (8–10 мероприятий с ответственными, сроками и КПЭ).

Практико-ориентированная контрольная работа: разработка черновиков кризисных сообщений.

Задание. Вы – руководитель образовательной организации. В студенческих чатах массово распространяется фейк о якобы «закрытии вуза» и «переводе всех студентов на платное обучение». Подготовьте черновик первого официального сообщения для внутренней аудитории (сотрудники) и для студентов/родителей. В каждом сообщении – не более 120–150 слов.

Требования к содержанию:

- факт (что произошло / что известно);
- источник информации и степень достоверности;
- что уже сделано / делается сейчас;
- дальнейшие шаги и сроки;
- куда обращаться за уточнениями (единый контакт).

Образец сообщения для сотрудников (внутренняя аудитория):

«Уважаемые коллеги! В студенческих чатах и социальных сетях распространяется недостоверная информация о якобы планируемом закрытии колледжа и переводе всех студентов на платное обучение. Данная информация не соответствует действительности, источник не является официальным. На данный момент руководство колледжа подготовило официальное опровержение, которое будет опубликовано на сайте и в официальных соцсетях в течение 1 часа. Кураторам необходимо довести достоверную информацию до учебных групп и пресекать распространение фейка. Официальные разъяснения для студентов и родителей будут направлены до 15:00 текущего дня. Вопросы направлять по единому каналу: тел. 8 (XXX) XXX-XX-XX, Морозова А.Л.»

Образец сообщения для студентов и родителей:

«Уважаемые студенты и родители! Обращаем ваше внимание: в неофициальных чатах распространяется ложная информация о закрытии колледжа и переводе на платное обучение. Эта информация не имеет никаких оснований. Колледж работает в штатном режиме, обучение продолжается согласно учебному плану. Распространение недостоверной информации может быть связано с попыткой дестабилизации. Просим не передавать непроверенные сведения и руководствоваться только официальными источниками: сайт колледжа и официальная страница в VK. Все вопросы – по единому телефону 8 (XXX) XXX-XX-XX или на почту.»

Критерии оценки:

- Соответствие аудитории (отдельный текст для сотрудников и для студентов/родителей) – 1 балл.

- Наличие всех 5 пунктов содержания – 1 балл.
- Отсутствие паники и двусмысленностей, нейтральный тон, опора на факты – 1 балл.
- Чёткие сроки/ответственные и канал связи – 1 балл.

Перевод баллов: 4 балла – «зачтено»; 3 балла – «частично зачтено» (доработка по замечаниям); менее 3 – «не зачтено».

Разработка регламента реагирования на гибридные вызовы (1–2 страницы).

Инструкция: подготовьте проект регламента реагирования образовательной организации на инциденты гибридных вызовов. Объём – не более 2 страниц.

Регламент должен включать:

1. Общие положения – назначение, область применения, нормативная база.
2. Классификация инцидентов – по типам угроз (информационно-психологические, ценностно-смысловые, организационные, технологические) и уровням тяжести.
3. Роли и зоны ответственности – кто принимает решение, кто реагирует, кто информирует.
4. Алгоритм реагирования – пошаговые действия при инциденте (первые 24-48 часов), каналы коммуникации.
5. Порядок согласования и публикации сообщений – единый контакт, шаблоны для разных аудиторий.
6. Механизмы обратной связи и корректировки – оценка эффективности реагирования, актуализация регламента.

Образец фрагмента регламента (алгоритм реагирования):

Алгоритм реагирования на типовой инцидент (массовая рассылка фейка в студенческих чатах):

Шаг 1 (0–2 часа). Идентификация инцидента: ответственный ИТ-специалист фиксирует факт распространения деструктивного контента, делает скриншоты, определяет охват. Кураторы групп опрашиваются о наличии фейка в курируемых чатах. Ответственный: начальник ИТ-отдела.

Шаг 2 (2–4 часа). Оповещение рабочей группы: руководитель ОО или заместитель созывает экстренное совещание (очно или онлайн). Определяется уровень угрозы по матрице «Вероятность × Последствия». Принимается решение о формате реагирования. Ответственный: руководитель рабочей группы.

Шаг 3 (4–8 часов). Публикация официального сообщения: пресс-служба выпускает опровержение по утверждённым шаблонам для сотрудников, студентов/родителей и (при необходимости) СМИ. Сообщение публикуется на сайте, в официальных соцсетях, рассылается кураторам. Ответственный: руководитель пресс-службы.

Шаг 4 (24–48 часов). Мониторинг реакции: ИТ-служба отслеживает динамику распространения фейка, кураторы фиксируют реакцию студентов. При необходимости готовится повторное сообщение. Ответственный: начальник ИТ-отдела.

Критерии оценивания:

Наличие всех 6 ключевых разделов – 1 балл.

Алгоритм реагирования содержит конкретные шаги, сроки и ответственных – 1 балл.

Учёт специфики ОО (ВО/СПО) и нормативной базы – 1 балл.

Регламент реализуем (реалистичные сроки, назначены ответственные, определены каналы коммуникации) – 1 балл.

Перевод баллов: 3–4 балла – зачтено; 2 балла – зачтено при доработке; менее 2 – не зачтено.

Разработка дорожной карты мероприятий (8–10 мероприятий с ответственными, сроками и КПЭ).

Инструкция: на основе карты рисков (из Модуля 2) составьте дорожную карту мероприятий на 3–6 месяцев. Включите мероприятия по всем 4 функциональным контурам защиты. Для каждого мероприятия укажите: название, контур, цель, ответственного, срок и КПЭ (измеримый результат).

Шаблон дорожной карты:

№	Название мероприятия	Контур	Цель	Ответственный	Срок	КПЭ
1						
2						

Образец заполнения (фрагмент, колледж СПО):

№	Название мероприятия	Контур	Цель	Ответственный	Срок	КПЭ
	Разработать и утвердить регламент реагирования на гибридные вызовы	Административный	Формализация процедур реагирования; снижение юридических рисков	Волков Д.А., юристконсульт	До 30.09.2026	1 документ, согласован с юристом, утверждён приказом директора
2	Провести инструктаж руководителей подразделений по новому регламенту	Административный	Обеспечение единого понимания процедур реагирования	Волков Д.А., юристконсульт	До 10.10.2026	Инструктаж проведён, протокол заседания, явка не менее 90% руководителей
3	Провести обучение кураторов по распознаванию ценностно-смысловых угроз (16 ак. часов)	Воспитательный	Повышение устойчивости воспитательной среды; формирование навыков распознавания манипулятивного контента	Морозова А.Л., куратор воспитательной работы	До 15.10.2026	Обучено не менее 80% кураторов; средний балл итогового тестирования не ниже 75%
4	Внедрить ежемесячный мониторинг маркеров деструктивного поведения студентов	Воспитательный	Своевременное выявление и профилактика деструктивных явлений	Морозова А.Л.; педагог-психолог	До 01.11.2026, далее ежемесячно	1 отчёт в месяц; анализ динамики за квартал
5	Сформировать реестр студенческих чатов и настроить регулярный мониторинг	Цифровой	Снижение рисков распространения деструктивного контента	Петров И.С., начальник ИТ-отдела	До 05.09.2026, далее еженедельно	Реестр из не менее 25 чатов; еженедельный отчёт мониторинга

№	Название мероприятия	Контур	Цель	Ответственный	Срок	КПЭ
6	Разработать алгоритм реагирования куратора при выявлении деструктивного контента в чатах	Цифровой	Обеспечение регламентированного и оперативного реагирования	Петров И.С., Морозова А.Л.	До 20.09.2026	1 утверждённый алгоритм; доведён до всех кураторов (под подпись)
7	Внедрить двухфакторную аутентификацию для корпоративных учётных записей	Цифровой	Защита учётных данных от несанкционированного доступа	Петров И.С., начальник ИТ-отдела	До 15.11.2026	2ФА включена для 100% корпоративных аккаунтов
8	Подготовить 4 шаблона кризисных сообщений (сотрудники, студенты, родители, СМИ)	Коммуникационный	Сокращение времени реакции на инциденты; предотвращение дезинформации	Кузнецова М.П., руководитель пресс-службы	До 25.10.2026	4 документа, согласованы с юристом, утверждены приказом
9	Утвердить порядок согласования и публикации сообщений при инцидентах	Коммуникационный	Исключение неуполномоченных источников; единый канал коммуникации	Кузнецова М.П., руководитель пресс-службы	До 25.10.2026	1 документ; определён единый контакт; утверждён приказом
10	Провести комплексные учения по реагированию на гибридную угрозу	Все контуры	Практическая отработка регламентов и шаблонов; проверка готовности рабочей группы	Смирнова Е.В., заместитель директора	До 20.12.2026	1 проведённое учение; отчёт с оценкой времени реакции; протокол разбора

Критерии оценивания:

- Дорожная карта содержит 8-10 мероприятий, охватывающих все 4 контура защиты – 1 балл.

- Для каждого мероприятия указаны ответственный, срок и КПЭ (конкретный, измеримый, достижимый, релевантный, ограниченный по времени) – 1 балл.
 - Мероприятия логически связаны с картой рисков из Модуля 2 – 1 балл.
 - Сроки реалистичны (не более 6 месяцев), ответственные назначены по зонам компетенций – 1 балл.
- Перевод баллов: 3-4 балла – зачтено; 2 балла – зачтено при доработке; менее 2 – не зачтено.

Вопросы для устной проверки и дискуссии

1. Опишите алгоритм реагирования на типовой инцидент: массовая рассылка фейка о вузе в студенческих чатах. Укажите первые 3 шага, ответственных и каналы коммуникации.
2. Что должно входить в регламент реагирования на гибридные вызовы? Перечислите 5-6 ключевых разделов.
3. Как в дорожной карте мероприятий обеспечить измеримость результатов? Приведите пример КПЭ для одного мероприятия.
4. Какие шаблоны сообщений должны быть в коммуникационном плане для кризисных ситуаций? Назовите 4 типа адресатов и по одной цели сообщения для каждого.
5. Как организовать межведомственное взаимодействие при серьёзном инциденте (например, кибератака с утечкой данных)? Укажите 2-3 внешних партнёра и формат взаимодействия.
6. Как интегрировать меры защиты в систему управления качеством ОО? Приведите 1-2 практических механизма.

3.3.4. Итоговая аттестация

Форма контроля по плану: защита педагогического продукта (карта рисков, регламент, дорожная карта, коммуникационный план), публичное выступление (5–7 минут) с презентацией (7–10 слайдов).

Кейс-задание для мини-проекта

Ситуация. «В ОО в течение недели фиксируется рост конфликтов в группах, увеличение числа пропусков и появление в чатах мемов с агрессивной риторикой. По данным мониторинга, в одном из чатов распространяются материалы, дискредитирующие преподавателей и администрацию».

Задание:

1. Составьте карту рисков (3-5 позиций): тип угрозы, индикатор, уровень (высокий/средний/низкий), зона ответственности, последствия.
2. Предложите 3-4 первоочередных шага (алгоритм на первые 24-48 часов).
3. Сформулируйте 1 мероприятие на 3 месяца с КПЭ (сроки, ответственный, целевой показатель).

Критерии оценки:

- Полнота карты рисков (все 5 элементов на каждую позицию) – 1 балл.
- Реалистичность и последовательность первых шагов – 1 балл.
- Корректность КПЭ (конкретный, измеримый, достижимый, релевантный, ограниченный по времени) – 1 балл.
- Учёт специфики СПО (возраст, модели управления, цифровая зрелость) – 1 балл.

Оценка: 4 балла – «зачтено»; 3 балла – «частично зачтено»; менее 3 – «не зачтено».

Требования к итоговому педагогическому продукту и критерии оценивания

Педагогический продукт включает:

1. Карту рисков-вызовов (3-5 позиций) с типом угрозы, индикатором, уровнем, зоной ответственности и последствиями.
2. Регламент реагирования (1-2 страницы) с алгоритмом действий, ролями, сроками и каналами коммуникации.
3. Дорожную карту (8-10 мероприятий на 3-6 месяцев) с ответственными, сроками и КПЭ.
4. Коммуникационный план с шаблонами 3-4 типовых сообщений для внутренней аудитории, студентов, родителей и СМИ.
5. Публичное выступление с логикой «проблема – решение – результат» и ответами на вопросы комиссии (5-7 минут, презентация 7-10 слайдов).

Критерии оценивания (5 баллов):

Критерий	Балл
Реализуемость решений (учёт ресурсов и специфики ОО)	до 1

Критерий	Балл
Нормативная корректность (соответствие нормативным документам и полномочиям ОО)	до 1
Измеримость результатов (чёткие КПЭ, сроки, ответственные)	до 1
Учёт специфики ВО/СПО (возрастные группы, модели управления, цифровая зрелость)	до 1
Качество публичного выступления (логика, ясность, ответы на вопросы)	до 1

Перевод баллов: 4-5 баллов – «зачтено»; 3 балла – «зачтено при условии доработки по замечаниям комиссии»; менее 3 – «не зачтено» (требуется повторная защита с доработкой).

3.3.15. Вопросы для защиты мини-проекта (практико-ориентированные)

- Обоснуйте выбор именно этих 3-5 рисков в вашей карте: почему они приоритетны для вашей ОО?
- Чем ваш регламент реагирования отличается от типовых решений? В чём специфика под вашу ОО?
- Как вы планируете контролировать выполнение дорожной карты и корректировать её при изменении угроз?

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Учебно-методическое обеспечение и информационное обеспечение программы (литература)

Нормативно-правовые документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). — URL: <http://www.pravo.gov.ru> (дата обращения: 20.08.2026). — Текст: электронный.

2. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»: редакция от 24.07.2025. — URL: <http://www.pravo.gov.ru> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* базовый документ, определяющий правовые рамки деятельности образовательных организаций и допустимые меры по обеспечению безопасности образовательной среды. Используется в модуле «Нормативные основы противодействия гибридным угрозам».

3. Федеральный закон от 30.12.2020 № 489-ФЗ «О молодежной политике в Российской Федерации» (ред. от 23.07.2025). — URL: http://www.consultant.ru/document/cons_doc_LAW_368861/ (дата обращения: 20.08.2026). — Текст: электронный. закрепляет патриотическое воспитание молодёжи и духовно-нравственное *Пояснение:* воспитание молодёжи как основные направления молодежной политики. Определяет полномочия органов публичной власти по формированию у молодых граждан мировоззрения на основе традиционных ценностей, защите исторической памяти, противодействию деструктивным явлениям. Используется в модуле «Воспитательный контур» и при разработке мер по устойчивости образовательной среды

4. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». — URL: <http://publication.pravo.gov.ru/Document/View/0001201612060002> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* формирует системные подходы к защите в информационной сфере, что важно для понимания цифровых компонентов гибридных угроз и мер реагирования в образовательной среде.

5. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». — URL: <http://publication.pravo.gov.ru/Document/View/000120210703000> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* задаёт стратегический контекст обеспечения безопасности, включая социокультурные и информационные аспекты, релевантные для противодействия гибридным вызовам.

6. Указ Президента Российской Федерации от 09.11.2022 № 809 (ред. от 04.03.2026 № 136) «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». — URL: <http://www.kremlin.ru/acts/bank/48502> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* документ стратегического планирования в сфере национальной безопасности, определяющий цели

и задачи защиты традиционных ценностей. Закрепляет воспитание в духе уважения к традиционным ценностям как ключевой инструмент государственной политики в области образования; содержит задачу противодействия распространению деструктивной идеологии и защиты от внешнего деструктивного информационно-психологического воздействия. Используется в модуле «Воспитательный контур: ценностно-смысловые угрозы и устойчивость образовательной среды».

7. Распоряжение Правительства Российской Федерации от 29.05.2015 № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года». — URL: http://www.consultant.ru/document/cons_doc_LAW_180933/ (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* определяет приоритеты государственной политики в области воспитания и социализации, основные направления развития институтов воспитания. Закрепляет духовно-нравственное воспитание на основе традиционных ценностей, развитие инструментов медиации для разрешения конфликтов в образовательной среде, повышение информационной безопасности детей. Используется при формировании воспитательного контура защиты и разработке дорожной карты мероприятий.

8. Распоряжение Правительства Российской Федерации от 17.08.2024 № 2233-р «Об утверждении Стратегии реализации молодёжной политики в Российской Федерации на период до 2030 года». — URL: <http://www.consultant.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* устанавливает долгосрочные ориентиры молодёжной политики, включая патриотическое и духовно-нравственное воспитание, профилактику негативных социальных явлений в молодёжной среде, формирование устойчивости к деструктивным информационно-психологическим воздействиям. Используется при формировании дорожной карты мероприятий и обосновании воспитательных мер.

9. Приказ Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам». — URL: <https://docs.cntd.ru/document/1312587284> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* регламентирует реализацию программ ДПО, включая требования к структуре, планированию и оценке результатов. Необходим для обоснования организационно-педагогических условий программы.

10. Приказ Минтруда России от 18.10.2013 № 544н (ред. от 05.08.2016) «Об утверждении профессионального стандарта "Педагог

(педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)»». — URL: https://www.consultant.ru/document/cons_doc_LAW_155553 (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение*: определяет трудовые функции педагога, в том числе связанные с обеспечением безопасной и психологически комфортной образовательной среды, профилактикой деструктивных явлений.

11. Постановление Правительства Российской Федерации от 02.08.2019 № 1006 (ред. от 05.03.2022 № 289) «Об утверждении требований к антитеррористической защищённости объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства, и формы паспорта безопасности этих объектов (территорий)». — URL: http://www.consultant.ru/document/cons_doc_LAW_331342/ (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение*: устанавливает обязательные требования к антитеррористической защищённости образовательных организаций и форму паспорта безопасности.

12. Распоряжение Правительства Российской Федерации от 24.06.2023 № 1667-р «Об утверждении комплекса мер по профилактике негативных социальных явлений в детской и молодёжной среде на 2023–2025 годы». — URL: <http://www.consultant.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение*: содержит системные меры по профилактике деструктивного поведения, травли, вовлечения молодёжи в опасные онлайн-сообщества. Непосредственно перекликается с задачами программы по выявлению и нейтрализации ценностно-смысловых угроз в образовательной среде. Используется в модуле «Воспитательный контур» и при разработке чек-листов экспресс-диагностики.

13. Письмо Минобрнауки России от 10.12.2024 № МН-6/2820 «О направлении методических рекомендаций по обеспечению комплексной безопасности в образовательных организациях». — URL: <https://edu.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение*: содержит типовые алгоритмы действий, распределение ролей, порядок реагирования и взаимодействия с внешними структурами; используются как основа для адаптации регламентов под конкретную образовательную организацию.

14. Письмо Минкомсвязи России от 10.04.2020 № ЛБ-С-088-8929 «О мерах по обеспечению информационной безопасности детей при использовании ресурсов сети "Интернет"». — URL: <https://digital.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение*: определяет

меры защиты несовершеннолетних от деструктивного контента и информационных угроз в цифровой среде.

15. Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)» (утв. ФСТЭК России 17.05.2023). — URL: <https://www.garant.ru/products/ipo/prime/doc/406855550/> (дата обращения: 20.08.2026). — Текст: электронный. *Пояснение:* описывает этапы мониторинга, оценки критичности и принятия решений по устранению уязвимостей — обеспечивает переход от диагностики угроз к конкретным управленческим действиям.

16. Локальные нормативные акты образовательных организаций (положения о комплексной безопасности, паспорт безопасности, инструкции по действиям в ЧС, правила внутреннего распорядка, положение о службе медиации). *Пояснение:* практический уровень реализации мер безопасности; в рамках программы разбираются как кейс-материалы: слушатели адаптируют шаблоны под специфику своей организации. Включают:

- Положение о комплексной безопасности — ключевой локальный акт, закрепляющий общую политику организации: приоритетные направления безопасности (антитеррористическая защищённость, пожарная, электробезопасность, охрана труда, информационная), распределение ответственности, планируемые мероприятия;

- Паспорт безопасности объекта (территории) — документ, разрабатываемый организацией по форме, утверждённой Постановлением Правительства РФ № 1006, согласовываемый с территориальными органами ФСБ, Росгвардии, МЧС;

- Инструкции по действиям в ЧС — пошаговые регламенты действий сотрудников и обучающихся при пожаре, угрозе взрыва, стихийном бедствии, химической угрозе и т.п., с прилагаемыми планами эвакуации;

- Правила внутреннего распорядка — отдельно для обучающихся (поведение, права, обязанности, правила на уроках и мероприятиях) и для работников (режим труда и отдыха, дисциплинарные требования);

- Положение о службе медиации (примирения) — определяет цели, задачи, порядок работы службы, права и обязанности участников, процедуры урегулирования конфликтов.

Основная литература:

1. Карпович, О. Г. Гибридные войны : учебник / О. Г. Карпович, А. А. Гришанов, В. Б. Козюлин, В. В. Комлева, С. А. Кондаков, А. А. Крутько, А. Ж. Мартиросян, А. В. Моисеев, А. Ш. Ногмова, Д. И. Савельев, Р. Н. Шангараев ; Дипломатическая академия МИД России. — 2-е изд., испр. и доп. — Москва : Сам Полиграфист, 2025. — 910 с. — ISBN 978-5-00227-592-2. —

URL: <https://elibrary.ru/item.asp?id=88778524> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный.

2. Карпович, О. Г. Гибридные угрозы в образовательной среде: вопросы противодействия / О. Г. Карпович // Национальная оборона. — 2026. — URL: <https://oborona.ru/product/zhurnal-nacionalnaya-oborona/gibridnye-ugrozy-v-obrazovatelnoj-srede-voprosy-protivodejstviya-47685.shtml> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* раскрыты роль образовательного сообщества в противодействии гибридным вызовам, ценностно-воспитательные механизмы, подходы к формированию устойчивости образовательной среды; используется для обоснования методологии программы и формулирования целевых результатов.

3. Бартош, А. А., Гибридная война : учебное пособие / А. А. Бартош. - Москва : КноРус, 2024. -305 с. - ISBN 978-5-406-12912-8. - URL: <https://book.ru/book/953119> (обращения: 20.08.2026). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

4. Худякова, Т. Л. Диагностика психологической безопасности образовательной среды в условиях внедрения цифровых образовательных технологий : учебно-методическое пособие / Т. Л. Худякова, Л. Н. Гридяева, Ю. В. Клепач, В. Р. Петросянц. — Воронеж : ВГПУ, 2022. — 80 с. — URL: <https://e.lanbook.com/book/317741> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* включает анкету из трёх блоков (контентно-технические, коммуникационные, личностные риски и риски здоровья); используется практических занятиях как готовый инструмент диагностики. готовый инструмент диагностики.

5. Баева, И. А. Психологическая безопасность образовательной среды: становление направления и перспективы развития / И. А. Баева // Экстремальная психология и безопасность личности. — 2024. — Т. 1, № 3. — С. 5–19. — DOI: 10.17759/epps.2024010301. — URL: https://psyjournals.ru/journals/epps/archive/2024_n3/Baeva?ysclid=mt7e3eep1a110040717 (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* методика экспресс-оценки отношения участников к среде, удовлетворённости её характеристиками и уровня защищённости от угроз; применяется для интерпретации результатов диагностики и связи выявленных рисков с воспитательными мерами.

6. Баева, И. А. Психологическая безопасность в образовании: монография / И. А. Баева. — СПб. : Союз, 2002. — 271 с. — ISBN 5-94033-148-3. — URL: <https://www.academia.edu/35689297/> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный.

Пояснение: базовая монография, в которой предложена концепция психологической безопасности образовательной среды и методика её оценки.

7. Формирование и поддержание психологической безопасности образовательной среды : учебно-методическое пособие / под ред. О. А. Ульяниной. — М. : МГППУ, 2022. — 180 с. — ISBN 978-5-907672-02-4. — URL: <https://mgppu.ru/resources/files/ucheb-metod%20pos/%D0%A4%D0%BE%D1%80%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%B8%20%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BF%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D1%81%D1%80%D0%B5%D0%B4%D1%8B.pdf?ysclid=mt7e5fko1h144435952> (дата обращения: 20.08.2026). — Режим доступа: свободный. — Текст: электронный. *Пояснение:* учебно-методическое пособие, в котором рассмотрены условия формирования психологически безопасной образовательной среды (социально-психологический климат, принципы диалогического воспитания) и предложены диагностические инструменты для её непрерывного мониторинга; предназначено для педагогов-психологов, педагогических работников и администрации образовательных организаций.

Дополнительная литература:

1. Бухарин, С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов. - Москва : Академический Проект, 2020. - 382 с. - ISBN 978-5-8291-3190-6. - URL: <https://e.lanbook.com/book/132794> (дата обращения: 20.08.2026). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

2. Карпович О. Г. Когнитивные войны в контексте стратегических коммуникации : монография / О. Г. Карпович, Р.Н. Шангараев ; ДА МИД России. - Москва : Сам Полиграфист, 2024. - 268 с. - URL: <https://elib.dipacademy.ru/MegaPro/Download/ToView/1330?idb=books>. (дата обращения: 20.08.2026). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

3. Терновская, Л. О. Война и мир в гибридном измерении : монография / Л.О. Терновская. - Москва : ИНФРА-М, 2024. - 368 с. - ISBN 978-5-16-015800-6. - URL: <https://znanium.com/catalog/product/2104845> (дата обращения:

20.08.2026). - Режим доступа: для авторизир. пользователей . - Текст : электронный.

4. Боев, В. Д. Моделирование в среде AnyLogic : учебное пособие для вузов / В. Д. Боев. - Москва : Юрайт, 2024. - 298 с. - ISBN 978-5-534-02560-6. - URL: <https://urait.ru/bcode/562671> (дата обращения: 20.08.2026). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

5. Искусственный интеллект, аналитика и новые технологии : практическое руководство / К. Андерсон, Н. Давар, Р. Д'Авени [и др.]. - Москва : Альпина Паблишер, 2022. - 200 с. - ISBN 978-5-9614-4791-0. - URL: <https://znanium.ru/catalog/product/2138146> (дата обращения: 20.08.2026). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

6. Методические рекомендации по формированию психологически безопасной образовательной среды / авторский коллектив ХМАО — Югры. — Ханты-Мансийск, 2023. — 124 с. — URL: <https://admhmansy.ru/> (дата обращения: 20.08.2026). — Режим доступа: свободный. — Текст: электронный. *Пояснение:* включают алгоритмы действий педагога-психолога при выявлении травли и деструктивного поведения, положения о службе медиации, чек-листы фиксации инцидентов; используются как шаблоны для адаптации под образовательную организацию.

7. Материалы Центра развития ВО и СПО РАО : методические рекомендации, дорожные карты, типологии угроз, кейсы пилотных площадок. — Москва : РАО, 2024–2026. — URL: <https://rusacademedu.ru/> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* прикладные решения и лучшие практики; применяются в модулях по управленческим решениям и устойчивости образовательной организации, разборе реальных кейсов и адаптации дорожных карт.

8. Сборники научно-практических конференций РАО по вопросам безопасности и устойчивости образовательной среды (2023–2026 гг.). — Москва : РАО, 2023–2026. — URL: <https://elibrary.ru/> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* содержат актуальные кейсы, примеры локальных регламентов, метрики эффективности; используются для итоговой мини-защиты проектных решений слушателей.

9. Гайдамакин, Н. А. Метод экспресс-анализа событий, связанных с воздействиями на файлы, предназначенный для расследования инцидентов информационной безопасности / Н. А. Гайдамакин, Р. В. Гибилинда, Н. И. Синадский // Вестник СибГУТИ. — 2020. — № 4. — С. 3–10. — URL: <https://vestnik.sibsutis.ru/jour/article/view/31/31> (дата обращения: 20.08.2026).

— Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* предложен метод быстрой обработки больших массивов событий ИБ за счёт шаблонов — напрямую перекликается с идеей экспресс-диагностики гибридных угроз.

10. Звягин, А. А. Россия в гибридной войне. Информационно-психологическая безопасность: монография / А. А. Звягин, Б. А. Артамонов, И. А. Мельников. — Москва : ИНФРА-М, 2024. — 329 с. — ISBN 978-5-16-019200-1. — URL: <https://znanium.com/catalog/document?id=440608> (дата обращения: 20.08.2026). — Режим доступа: для авторизир. пользователей. — Текст: электронный. *Пояснение:* предложена основа для формирования ментального механизма противодействия угрозам информационно-психологической войны и норм информационной гигиены.

Интернет-ресурсы:

1. Электронная библиотека Российской академии образования — URL: <https://rusacademedu.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* доступ к методическим рекомендациям, материалам пилотных инновационных площадок, типологиям угроз и дорожным картам; поиск актуальных материалов для адаптации в рамках программы.

2. Официальный сайт Министерства науки и высшего образования Российской Федерации — URL: <https://minobrnauki.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* мониторинг актуальных приказов, писем и методических рекомендаций по безопасности образовательной среды.

3. Официальный сайт Министерства просвещения Российской Федерации — URL: <https://edu.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* нормативные документы и методические рекомендации по безопасности образовательной среды.

4. Банк документов Министерства просвещения Российской Федерации — URL: <https://docs.edu.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* поиск конкретных приказов и писем по теме программы.

5. Официальный сайт Рособнадзора — URL: <https://obrnadzor.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* разъяснения и требования надзорного органа к организации комплексной безопасности.

6. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации — URL: <https://digital.gov.ru/> (дата обращения: 20.08.2026). — Текст: электронный.

Назначение: материалы по информационной безопасности и цифровым угрозам.

7. Электронная система образования — URL: <https://edsoo.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* нормативные и методические материалы по ФГОС и безопасным образовательным практикам.

8. Справочно-правовая система «КонсультантПлюс» — URL: <https://www.consultant.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* актуальные редакции нормативных актов, письма ведомств, судебная практика по вопросам безопасности в образовательных организациях.

9. Справочно-правовая система «Гарант» — URL: <https://www.consultant.ru/> (дата обращения: 20.08.2026). — Текст: электронный. *Назначение:* публикации нормативных актов, писем и методических рекомендаций по безопасности в образовательных организациях.

10. Электронные библиотеки вузов — доступ к программам повышения квалификации, учебно-методическим комплексам по противодействию гибридным угрозам. — Текст: электронный. *Назначение:* изучение примеров реализации программ и методических решений.

4.2. Материально-технические условия реализации программы

Практические занятия проводятся в учебных аудиториях, оснащённых мультимедийным оборудованием (проектор, экран, ноутбук, акустическая система), либо в компьютерных классах с доступом к сети Интернет (одно рабочее место на слушателя, группа не более 20 человек).

Для групповой работы предусмотрены зоны для дискуссий и проектной деятельности с возможностью перемещения мебели для организации работы в малых группах.

Для проведения занятий по диагностике гибридных угроз используется комплект печатных и электронных анкет, чек-листов и бланков фиксации инцидентов.

При заочной форме обучения с использованием дистанционных образовательных технологий применяется образовательная платформа на базе СДО MOODLE, которая обеспечивает:

- организацию и информационную поддержку учебного процесса с применением дистанционных технологий;
- управление пользователями всех категорий;

- хранение, обновление и систематизацию учебно-методических ресурсов;
- взаимодействие участников дистанционного учебного процесса; дистанционный мониторинг учебного процесса.

Основные компоненты ЭИОС, обеспечивающие учебно-методическое содержание учебного процесса:

- электронные учебно-методические комплексы;
- электронные образовательные и информационные ресурсы;
- фонды оценочных средств в электронном виде.

Для лиц с ограниченными возможностями здоровья (ОВЗ) обеспечиваются специальные условия: адаптированные учебные материалы с увеличенным шрифтом, возможность использования специальных технических средств обучения, индивидуальный график консультаций. Не менее 30% материалов представлены в формате, адаптированном для лиц с ОВЗ.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

4.3. Кадровые условия реализации программы

Требования к квалификации педагогов:

- Образование: высшее, соответствующее профилю программы (педагогика, психология, управление в образовании, безопасность жизнедеятельности, информационная безопасность и смежные направления).
- Опыт работы: не менее 3 лет в системе образования или в сфере обеспечения безопасности образовательных организаций; наличие опыта реализации программ повышения квалификации либо участия в методических и проектных работах по тематике безопасности образовательной среды.
- Уровень профессиональной квалификации: соответствие требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (в том числе профессиональный стандарт «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», иные релевантные стандарты).
- Дополнительные требования: не менее 70% преподавательского состава должны иметь опыт работы в мультикультурной или многоуровневой образовательной среде; не менее одного преподавателя должен иметь профильное образование в области информационной безопасности.

Для проведения отдельных модулей могут привлекаться внешние эксперты:

- представители органов управления образованием (по вопросам нормативно-правового обеспечения комплексной безопасности);
- специалисты по информационной безопасности (по вопросам цифровых компонентов гибридных угроз);
- психологи и медиаторы (по вопросам психологической безопасности и разрешения конфликтов);
- представители надзорных органов (по вопросам соблюдения требований антитеррористической защищённости и пожарной безопасности).

Качественный состав:

Категория	Требования	Количество
Руководитель программы	Кандидат или доктор наук, опыт научной и методической работы по тематике безопасности образовательной среды не менее 5 лет	1 чел.
Преподаватели теоретических модулей	Высшее образование (педагогика, психология, управление в образовании), опыт работы по профилю не менее 3 лет	не менее 2 чел.
Преподаватели практических модулей	Высшее образование (информационная безопасность, безопасность жизнедеятельности), опыт практической работы не менее 3 лет	не менее 1 чел.
Внешние эксперты	Специалисты органов управления образованием, информационной безопасности, психологи	не менее 2 чел.