

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ
Государственное автономное образовательное учреждение
дополнительного профессионального образования города Москвы
«МОСКОВСКИЙ ЦЕНТР РАЗВИТИЯ КАДРОВОГО ПОТЕНЦИАЛА
ОБРАЗОВАНИЯ»

УПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВЫХ, ИНТЕРАКТИВНЫХ И
ДИСТАНЦИОННЫХ ТЕХНОЛОГИЙ ОБРАЗОВАНИЯ



УТВЕРЖДАЮ
Директор ГАОУ ДПО МЦРКПО

 Рытов А.И.

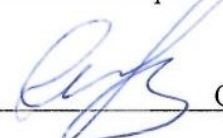
«31» _____ июля _____ 2020 г.

Дополнительная профессиональная программа
(повышение квалификации)

Организация защиты детей от информации,
причиняющей вред здоровью, развитию детей,
не соответствующей задачам образования

Рег. номер _____ 686 _____

Начальник организационного отдела


_____ С.Г. Садчикова

Разработчики курса:

Сорокин П.А.,

Самсолюк А.С.,

Новиков К.А.

Одобрено на заседании Управления развития
цифровых, интерактивных и дистанционных
технологий образования
Протокол № 2 от 29.07.2020 г.

Начальник управления  Ю.В. Федорова

Направление: IT и средовые компетенции
Уровень: базовый

Москва, 2020

Раздел 1. «Характеристика программы»

1.1. Цель реализации программы

Совершенствование профессиональных компетенций слушателей в области организация защиты детей от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования.

Совершенствуемые / новые компетенции

№	Компетенции	Направление подготовки 44.03.01 Педагогическое образование (Бакалавр)
		Код компетенции
1.	Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики	ОПК-1

1.2. Планируемые результаты обучения

№	Знать/Уметь	Направление подготовки 44.03.01 Педагогическое образование (Бакалавр)
		Код компетенции
1.	Знать: признаки социальных угроз для несовершеннолетних в сети Интернет. Уметь: выявлять социальные угрозы для несовершеннолетних в сети Интернет.	ОПК-1
2.	Знать: алгоритмы и механизмы организации профилактики вовлечения детей в деструктивную деятельность в сети Интернет. Уметь: применять алгоритмы и механизмы организации профилактики вовлечения детей в деструктивную деятельность в сети Интернет.	ОПК-1

2.	<p>Знать: нормативную базу в области обеспечения защиты детей от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования; компетенции организаций, задействованных в процессе обеспечения информационной безопасности детей.</p> <p>Уметь: определить компетенции организаций, задействованных в процессе обеспечения информационной безопасности детей; направить обращения в организации, задействованные в процессе обеспечения информационной безопасности детей.</p>	ОПК-1
----	---	-------

1.3. Категория обучающихся: уровень образования - высшее образование, область профессиональной деятельности – основное общее, среднее общее образование.

1.4. Форма обучения: очная с использованием дистанционных образовательных технологий.

1.5. Срок обучения: 16 часов.

Раздел 2. «Содержание программы»

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Внеаудиторные учебные занятия, самостоятельная работа		Форма контроля	Трудоемкость
		Лекции	Интерактивные занятия		
1.	Современная государственная политика в области образования. Нормативные документы, регламентирующие безопасность детей при работе с компьютерной техникой и в сети Интернет	2	2	Практическая работа № 1, 2, 3, 4,	4
2.	Социальные информационные угрозы: феномен скулшутинга (Колумбайн), деструктивные ARG, кибербуллинг (сетевая травля)	2	2,5	Практическая работа № 5, 6, 7, 8	4,5

3.	Социальные информационные угрозы: игровая зависимость и зависимость от азартных онлайн-игр, сетевой груминг (педофилия в Интернете), АУЕ* ¹	2	2,5	Практическая работа № 9, 10, 11, 12, 13	4,5
4.	Образовательные ресурсы по безопасному использованию ресурсов в сети Интернет для участников образовательного процесса	2			2
	Итоговая аттестация		1	Зачет Итоговое тестирование	1
	Итого	5	11		16

2.2. Учебная программа

Наименование темы	Виды учебных занятий, учебных работ	Основное содержание
Тема 1. Современная государственная политика в области образования. Нормативные документы, регламентирующие безопасность детей при работе с компьютерной техникой и в сети Интернет	Лекция, 2 часа	Государственная программа города Москвы «Развитие образования города («Столичное образование»)). Приоритетные задачи московской системы образования. Ценностные основания системных изменений в столичном образовании. Основные механизмы повышения эффективности системы образования Москвы (Рейтинг вклада школ в качественное образование, «Надежная школа», аттестационная справка директора и др.). Городские проекты. Результаты системы образования города Москвы. ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и развитию»; ФЗ РФ «Об информации, информационных технологиях и о защите информации», ФЗ РФ «Об образовании в Российской Федерации»; Методические рекомендации по ограничению в образовательных организациях доступа, обучающихся к видам информации; «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях».

¹ Запрещена на территории РФ

	<p>Практическая работа, 2 часа</p>	<p><i>Практическая работа №1.</i> «Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: скулшутинг, ARG, груминг, АУЕ*²»</p> <p><i>Практическая работа №2.</i> «Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: кибербуллинг»</p> <p><i>Практическая работа №3.</i> «Определение с точки зрения четырех ролей: классный руководитель, родители, жертва, одноклассники верной и неверной линии поведения в ситуации возникновения эпизода кибербуллинга»</p> <p><i>Практическая работа №4.</i> «Распределение предложенных кейсов в соответствии с компетенциями органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей»</p>
<p>Тема 2. Социальные информационные угрозы: феномен скулшутинга (Колумбайн), деструктивные ARG, кибербуллинг (сетевая травля)</p>	<p>Лекция, 2 часа</p>	<p>Феномен скулшутинга (Колумбайн) Признаки и методология профайлинга социальных сетей несовершеннолетних на основе актуальных данных государственных и негосударственных структур безопасности для выявления признаков субкультуры «школьных стрелков». Анализ данных и вопросы профилактики. Деструктивные ARG (феномен доведения до самоубийства с использованием игротехник и коммуникации в соцсети). «Сообщества смерти» и их администраторы. Признаки, особенности. Эволюция и технологические аспекты деструктивных игротехник («Синий кит», «Момо», «Красная сова» и т.д.) Кибербуллинг (сетевая травля). Особенности социально-психологического и технологического характера. Рассмотрение актуальных междисциплинарных разработок в вопросах профилактики и действий в условиях ЧП. Анализ механизмов социальных сетей Вконтакте, Facebook, Youtube, TikTok, Instagram для технологической работы в ситуациях с кибербуллингом с точки зрения родительской и преподавательской аудитории.</p>

² Запрещена на территории РФ

	<p>Практическая работа, 2,5 часа</p>	<p><i>Практическая работа №5.</i> «Определение технологии, методики и инструментов превентивной работы с актуальными информационными угрозами, доступные руководителям образовательных учреждений, педагогам, родителям и несовершеннолетним. <i>Практическая работа №6.</i> «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Феномен скулшутинга (Колумбайн)» <i>Практическая работа №7.</i> «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Деструктивные ARG» <i>Практическая работа №8.</i> «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Кибербуллинг»</p>
<p>Тема 3. Социальные информационные угрозы: игровая зависимость и зависимость от азартных онлайн-игр, сетевой груминг (педофилия в Интернете), АУЕ*³</p>	<p>Лекция, 2 часа</p>	<p>Игровая зависимость и зависимость от азартных онлайн-игр. Анализ данных ВОЗ и актуальных мировых тенденций, рассмотрение феномена игровой аддикции, с точки зрения проблем социализации современных несовершеннолетних, угроз для здоровья и безопасности. Сетевой груминг (педофилия в Интернете). Рассмотрение специфики современной коммуникации преступников в сети Даркнет. Форумы и признаки специфической субкультуры педофилов. Форматы мониторинга и предупреждения опасных ситуаций с несовершеннолетними. АУЕ*. Запрещенная организация и околоскриминальная субкультура. На основе данных ЦИСМ (Росмолодежь) и ряда других экспертных организаций рассмотрение актуальных информационных аспектов данной проблематики. Рассмотрение вопросов профилактики вовлечения детей и молодежи в преступную и околопреступную коммуникацию. Овершаринг. Рассмотрение современных трендов и взаимосвязи между открытым доступом к персональным данным и возможными угрозами жизни, здоровью и безопасности несовершеннолетнего на основе актуальных исследований. Обзор законодательства.</p>
	<p>Практическая работа, 2,5 часа</p>	<p><i>Практическая работа №9.</i> «Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры» <i>Практическая работа №10.</i> «Игровая зависимость и зависимость от азартных онлайн-игр: определение ТОП-5 современных компьютерных онлайн игр» <i>Практическая работа №11.</i> «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Сетевой груминг»</p>

³ Запрещена на территории РФ

		<p><i>Практическая работа №12.</i> «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «АУЕ*⁴»</p> <p><i>Практическая работа №13.</i> «Определение типа информационной угрозы в отношении несовершеннолетнего на основе анализа предложенных кейсов: «Овершаринг»</p>
<p>Тема 4. Образовательные ресурсы по безопасному использованию ресурсов в сети Интернет для участников образовательного процесса</p>	<p>Лекция, 2 часа</p>	<p>Образовательные программы ведущих ИТ-компаний по безопасному использованию ресурсов в сети Интернет в повседневной жизни и в образовательных организациях. Актуальные разработки от компаний Amazon, Google, Facebook, Mail.ru, Apple и др. по теме информационной гигиены и безопасности для аудитории взрослых и несовершеннолетних.</p> <p>Рекомендации для взаимодействия с несовершеннолетними по вопросам информационной безопасности, в соответствии с тремя возрастными группами: начальная школа (1-4 класс), основная школа (5-9 класс), средняя школа (10-11 классы).</p> <p>Актуальный опыт государственных и общественных структур:</p> <ul style="list-style-type: none"> – Роскомнадзор – Комиссия по безопасности, спорту и молодежной политике Московской городской думы – ООПН “Безопасная столица” – Координационный совет негосударственной сферы безопасности – Лига безопасного интернета – Родит – Фонд развития Интернет – Фонд “Дружественный рунет” – Центр безопасного интернета в России – «Защита детей в интернете» от Лаборатории Касперского https://kids.kaspersky.ru/
<p>Итоговая аттестация</p>	<p>Интерактивное занятие, 1 час</p>	<p>Зачет как совокупность успешно выполненных практических работ и участие в дискуссиях на Круглых столах курса.</p> <p>Итоговое тестирование на платформе https://moodle.mioo.ru/course/view.php?id=1277</p>

⁴ Запрещена на территории РФ

Раздел 3. «Формы аттестации и оценочные материалы»

Оценка качества освоения программы осуществляется в форме текущей и итоговой аттестации.

Текущая аттестация:

- участие в дискуссиях и выполнении практических работ. Дискуссии и практические работы реализуются с фиксацией результатов на Форуме курса повышения квалификации, а также на дополнительных образовательных электронных ресурсах, используемых в курсе. Оценивание зачет / незачет. Зачет ставится, если обучающийся принял участие в дискуссии и в выполнении практических заданий.
- выполнение Практических работ № 1-13. Зачет ставится, если критерии оценивания выполнены. Описание практических работ и их критерии оценивания в **Приложении 1**.

Итоговая аттестация – осуществляется на основании совокупности успешно выполненных практических работ, оцененных «зачет» и результата итогового тестирования (примеры вопросов итогового тестирования в **Приложении 2**).

Обучающийся считается сдавшим зачет (аттестованным), если:

- получил положительные оценки и(или) отзывы не менее чем на 70% практических работ, выполненных в процессе обучения.
- результат итогового тестирования – 60% и более процентов правильных ответов.

Практические работы при качественном выполнении могут быть использованы обучающимися в качестве материала (образовательного продукта), применяемого в педагогической практике. Основным продуктом, планируемым в результате обучения на курсе – сценарий образовательного мероприятия, направленный на профилактические меры по защите детей от видов информации, распространяемой посредством сети Интернет,

причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях. Все практические задания обучающихся выполняют и сдают в удобное время в рамках учебной программы через модули дистанционной поддержки курса на платформе moodle.mioo.ru.

Перечень практических заданий

Проверяемые практические работы	
Практическая работа № 1	Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: скулшутинг, ARG, груминг, АУЕ* ⁵ .
Практическая работа № 2	Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: кибербуллинг.
Практическая работа № 3	Определение с точки зрения четырех ролей: классный руководитель, родители, жертва, одноклассники верную и неверную линию поведения в ситуации возникновения эпизода кибербуллинга.
Практическая работа № 4	Распределение предложенных кейсов в соответствии с компетенциями органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей.
Практическая работа № 5	Определение технологии, методики и инструментов превентивной работы с актуальными информационными угрозами, доступные руководителям образовательных учреждений, педагогам, родителям и несовершеннолетним.
Практическая работа № 6	Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Феномен скулшутинга (Колумбайн)»
Практическая работа № 7	Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Деструктивные ARG»
Практическая работа № 8	Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Кибербуллинг»
Практическая работа № 9	Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры

⁵ Запрещена на территории РФ

Практическая работа № 10	Игровая зависимость и зависимость от азартных онлайн-игр: определение ТОП-5 современных компьютерных онлайн игр
Практическая работа № 11	Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Сетевой груминг»
Практическая работа № 12	Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «АУЕ* ⁶ »
Практическая работа № 13	Определение типа информационной угрозы в отношении несовершеннолетнего на основе анализа предложенных кейсов: «Овершаринг».

Соответствие практических заданий заявленным компетенциям

№	Знать	Направление подготовки 44.04.01 Педагогическое образование (магистратура) Код компетенции	Контроль
1.	Признаки социальных угроз для несовершеннолетних в сети Интернет.	ОПК-1	Практическая работа № 1, 2, 13
2.	Алгоритмы и механизмы организации профилактики вовлечения детей в деструктивную деятельность в сети Интернет.	ОПК-1	Практическая работа № 3, 5, 6, 7, 8, 9, 10, 11, 12
3.	Нормативную базу в области обеспечения защиты детей от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования; компетенции организаций, задействованных в процессе обеспечения информационной безопасности детей.		Практическая работа № 4
№	Уметь		Контроль
1.	Выявлять социальные угрозы для несовершеннолетних в сети Интернет.	ОПК-1	Практическая работа № 1, 2, 13
2.	Применять алгоритмы и механизмы организации профилактики вовлечения детей в деструктивную деятельность в сети Интернет.	ОПК-1	Практическая работа № 3, 5, 6, 7, 8, 9, 10, 11, 12

⁶ Запрещена на территории РФ

3.	Определить компетенции организаций, задействованных в процессе обеспечения информационной безопасности детей; направить обращения в организации, задействованные в процессе обеспечения информационной безопасности детей.		<i>Практическая работа № 4</i>
----	--	--	--------------------------------

Раздел 4. «Организационно-педагогические условия реализации программы»

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Нормативные документы

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 31.07.2020) "[Об образовании в Российской Федерации](#)", (дата обращения 28.07.2020)
2. Федеральный закон от 29.12.2010 N 436-ФЗ "[О защите детей от информации, причиняющей вред их здоровью и развитию](#)"
3. [Концепция информационной безопасности детей](#), утвержденной распоряжением Правительства РФ от 02.12.2015 N 2471. (дата обращения 28.07.2020)
4. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)», приложение к приказу Минтруда РФ № 544н от 18.10.2013г., URL http://www.consultant.ru/document/cons_doc_LAW_155553/cca в системе [Департамента образования города Москвы. Москва, 2008](#) (дата обращения 28.07.2020)
5. Постановление Главного государственного санитарного врача РФ от 29 декабря 2010 г. N 189 "Об утверждении СанПиН 2.4.2.2821-10 "Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях" (с изменениями и дополнениями). Система ГАРАНТ: <http://base.garant.ru/12183577/#ixzz5r69ysA2h> (дата обращения 28.07.2020).

Основная литература:

1. Малюк А.А. Глобальная культура кибербезопасности // Горячая линия - Телеком. М., 2017. С. 308.
2. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.
3. ЛеФевер Л. Искусство объяснять. Как сделать так, чтобы вас понимали с полуслова; пер. с англ. Москва: Манн, Иванов и Фербер, 2018.
4. Международная информационная безопасность: Теория и практика: В трех томах: Учебник для вузов / Под общ. ред. А.В.Крутских. — М.: Издательство «Аспект Пресс», 2019.
5. Хломов К.Д., Давыдов Д.Г., Бочавер А.А. Кибербуллинг в опыте российских подростков. [Электронный ресурс] // Психология и право. 2019(9). No 2. С. 276-295. doi: 10.17759/psylaw.2019090219.

Интернет ресурсы:

1. Журнал для педагогов, психологов и родителей «Дети в информационном обществе». <http://detionline.com/journal> (дата обращения 28.07.2020).
2. Методическое пособие «Интернет: возможности, компетенции, безопасность». Солдатова Г., Зотова Е., Лебешева М., Шляпников В. <http://detionline.com/internet-project/training-aids> (дата обращения 28.07.2020).
3. «Урок полезного и безопасного Интернета» от компании МТС. <http://detionline.com/mts/lessons> (дата обращения 28.07.2020).
4. «Защита детей в интернете» от компании Касперского <https://kids.kaspersky.ru/> (дата обращения 28.07.2020).
5. Видеоурок «Безопасность в Интернете» от компании Касперского <https://урокцифры.рф/teachers.html> (дата обращения 28.07.2020).

6. Интернет и безопасность. Онлайн курс для детей и взрослых.
<https://sites.google.com/site/kyrsbez/home> (дата обращения 28.07.2020).
7. Think with Google. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн. URL:
<https://www.thinkwithgoogle.com/intl/ru-ru/insights-trends/user-insights/novoe-pokolenie-internet-polzovatelei-issledovanie-privyчек-i-povedeniia-rossiiskoi-molodezhi-onlain/> (дата обращения 28.07.2020).
8. Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей результаты всероссийского исследования [Электронный ресурс]. М., Фонд Развития Интернет, 2013. 144 с. URL: <http://detionline.com/assets/files/research/DigitalLiteracy.pdf> (дата обращения 28.07.2020).
9. PricewaterhouseCoopers: аналитический обзор по теме информационной безопасности (2018)
<https://www.pwc.ru/ru/publications/global-information-security-survey-2018.html> (дата обращения 28.07.2020).
10. «Исследования» от Mail.ru Group <https://corp.mail.ru/ru/press/infograph/>
11. Мальцева В.А. Защита детей от кибербуллинга. вопросы уголовно-правового регулирования // научная электронная библиотека «Киберленинка» (Cyberleninka) (2019) <https://cyberleninka.ru/article/n/zaschita-detey-ot-kiberbullinga-voprosy-ugolovno-pravovogo-regulirovaniya> (дата обращения 28.07.2020)

4.2. Материально-технические условия реализации программы

1. Компьютер у каждого обучающегося.
2. Доступ в Интернет.
3. Учебные материалы, размещенные в информационной среде
<https://moodle.mioo.ru/course/view.php?id=1338>

Описание практических работ

Практическая работа №1. «Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: скулшутинг, ARG, груминг, АУЕ*».

<p>Алгоритм выполнения</p>	<ul style="list-style-type: none"> • Работая в группах в интерактивном пространстве Miro проводится анализ профилей несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по четырем видам информационных угроз: скулшутинг, вовлечение подростков в деструктивные игротехники, на примере игротехники «Синий кит», онлайн-груминг, вовлечение несовершеннолетних в запрещенные организации, на примере АУЕ*⁷) из социальных сетей (Вконтакте, Facebook, Instagram, TikTok и др.). <p>Критерии анализа:</p> <ul style="list-style-type: none"> - визуальные образы - текстовая информация - сообщества, подписки, друзья <ul style="list-style-type: none"> • Определить тип информационной угрозы в отношении несовершеннолетнего • Предположить возможные предпосылки вовлечения несовершеннолетнего в опасные сообщества/деятельность
<p>Критерии оценивания</p>	<ul style="list-style-type: none"> • Выявлены типы социальных информационных угроз
<p>Оценка</p>	<p>Зачет / Незачет</p>

⁷ Запрещена на территории РФ

Практическая работа №2. «Определение типа информационных угроз на основе анализа предложенных кейсов в отношении несовершеннолетнего: кибербуллинг».

Алгоритм выполнения	<ul style="list-style-type: none"> • Проанализировать публикации и диалоги несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме кибербуллинга) в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). • При помощи интерактивного сервиса Mentimeter выдвинуть предположение об угрозе, с которой столкнулся несовершеннолетний.
Критерии оценивания	<ul style="list-style-type: none"> • Выявлены типы социальных информационных угроз • Файл с выполненным заданием опубликован в учебном курсе.
Оценка	Зачет / Незачет

Практическая работа №3. «Определение с точки зрения четырех ролей: классный руководитель, родители, жертва, одноклассники верную и неверную линию поведения в ситуации возникновения эпизода кибербуллинга»

Алгоритм выполнения	<ul style="list-style-type: none"> • Работая в группах в интерактивном пространстве Miro необходимо распределить предложенные варианты поведения каждой аудитории на два кластера: «верная линия поведения» и «неверная линия поведения».
Критерии оценивания	<ul style="list-style-type: none"> • Выработана верная линия поведения в случае возникновения эпизода кибербуллинга с точки зрения четырех ролей: классного руководителя, родителя, жертвы, одноклассников.
Оценка	Зачет / Незачет

Практическая работа №4. «Распределение предложенных кейсов в соответствии с компетенциями органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей»

Алгоритм выполнения	<ul style="list-style-type: none"> • В интерактивном пространстве LearningApps распределить предложенные кейсы в соответствии с компетенциями представленных органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей.
Критерии оценивания	<ul style="list-style-type: none"> • Предложенные кейсы верно распределены в соответствии с компетенциями органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей.
Оценка	Зачет / Незачет

Практическая работа №5. «Определение технологии, методики и инструментов превентивной работы с актуальными информационными угрозами, доступные руководителям образовательных учреждений, педагогам, родителям и несовершеннолетним»

Алгоритм выполнения	<ul style="list-style-type: none"> • Используя методику «мозгового штурма» работая в группах выделить ТОП-5 информационных угроз для несовершеннолетних в социальных сетях с позиции руководителя образовательной организации, педагога, родителя и несовершеннолетнего • Используя инструмент общего интерактивного онлайн голосования выделить угрозу ТОП-1 с точки зрения каждой роли • Используя методику «мозгового штурма» работая в группах предложить технологии, методики и
---------------------	---

	<p>инструменты превентивной работы с выбранной угрозой.</p> <ul style="list-style-type: none"> Используя инструмент общего интерактивного онлайн голосования оценить эффективность набора предложенных решений в позиции каждой роли.
Критерии оценивания	<ul style="list-style-type: none"> Выявлены ТОП-5 информационных угроз для несовершеннолетних в социальных сетях с позиции руководителя образовательной организации, педагога, родителя и несовершеннолетнего Предложены технологии, методики и инструменты превентивной работы с предложенными угрозами.
Оценка	Зачет / Незачет

Практическая работа №6. «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Феномен скулшутинга (Колумбайн)»»

Алгоритм выполнения	<ul style="list-style-type: none"> Основываясь на материалах лекционного блока проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме скулшутинга) в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). Определить набор тревожных признаков и маркеров, свидетельствующих о возможном увлечении несовершеннолетнего тематикой скулшутинга
Критерии оценивания	<ul style="list-style-type: none"> В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

Практическая работа №7. «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Деструктивные ARG»»

Алгоритм выполнения	<ul style="list-style-type: none"> • Основываясь на материалах лекционного блока проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме деструктивных игротехник (ARG), на примере игротехники «Синий кит») в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). • Определить набор тревожных признаков и маркеров, свидетельствующих о возможном вовлечении несовершеннолетнего в деструктивную игротехнику (ARG).
Критерии оценивания	<ul style="list-style-type: none"> • В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

Практическая работа №8. «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Кибербуллинг»

Алгоритм выполнения	<ul style="list-style-type: none"> • Основываясь на материалах лекционного блока проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме кибербуллинга) в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). • Определить набор тревожных признаков и маркеров, свидетельствующих о вовлечении детей в ситуацию кибербуллинга в качестве жертвы, агрессора, пассивного наблюдателя.
Критерии оценивания	<ul style="list-style-type: none"> • В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

Практическая работа №9. «Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры («Игровая зависимость и зависимость от азартных онлайн-игр»»)

Алгоритм выполнения	<ul style="list-style-type: none">• При помощи преподавателей разобрать принципы и механизмы создания моделей компьютерных игр и азартных онлайн-игр
Критерии оценивания	<ul style="list-style-type: none">• Активное участие в интерактивном практическом задании• Правильные и своевременные ответы на вопросы преподавателя
Оценка	Зачет / Незачет

Практическая работа №10. «Определение ТОП-5 современных компьютерных онлайн игр («Игровая зависимость и зависимость от азартных онлайн-игр»»)

Алгоритм выполнения	<ul style="list-style-type: none">• При помощи интерактивной платформы Kahoot сопоставить скриншот (снимок экрана) из компьютерной игры (Minecraft, Counter-Strike, Dota 2, FIFA, World of Tanks) с названием игры.
Критерии оценивания	<ul style="list-style-type: none">• Верное выполнение упражнения
Оценка	Зачет / Незачет

Практическая работа №11. «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «Сетевой груминг»»

Алгоритм выполнения	<ul style="list-style-type: none"> • Основываясь на материалах лекционного блока проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме онлайн-груминга,) в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). • Определить набор тревожных признаков и маркеров, свидетельствующих о возможном общении ребенка с сетевым педофилом.
Критерии оценивания	<ul style="list-style-type: none"> • В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

Практическая работа №12. «Анализ предложенных кейсов и выявление признаков социальной информационной угрозы «АУЕ*»»

Алгоритм выполнения	<ul style="list-style-type: none"> • Основываясь на материалах лекционного блока проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей по теме вовлечения несовершеннолетних в запрещенные на территории РФ организации, на примере АУЕ*) в социальных сетях (Вконтакте, Facebook, Instagram, TikTok и др.). • • Определить набор тревожных признаков и маркеров, свидетельствующих о возможном увлечении несовершеннолетнего тематикой АУЕ*⁸
Критерии оценивания	<ul style="list-style-type: none"> • В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

⁸ Запрещена на территории РФ

Практическая работа №13. «Определение типа информационной угрозы в отношении несовершеннолетнего на основе анализа предложенных кейсов: «Овершаринг»»

Алгоритм выполнения	<ul style="list-style-type: none">• Работая в группа в интерактивном пространстве Miro проводится анализ профилей, публикаций несовершеннолетних (разработанных на основе реальных практик и кейсов для тренировочных целей тематике овершаринг) из социальных сетей (Вконтакте, Facebook, Instagram, TikTok и др.).• Критерии анализа:<ul style="list-style-type: none">- визуальные образы- текстовая информация- геометки, хэштеги• Определить тип информационной угрозы в отношении несовершеннолетнего• Предположить возможную зону риска, в которой находится несовершеннолетний
Критерии оценивания	<ul style="list-style-type: none">• Верно определён тип социальной информационной угрозы• В предложенных кейсах выявлены признаки социальной информационной угрозы
Оценка	Зачет / Незачет

Примеры вопросов входного и итогового тестирования

В каком нормативном документе дано определение информационной безопасности детей?

- a) ФЗ РФ «Об информации, информационных технологиях и о защите информации»
- b) ФЗ РФ «Об образовании в Российской Федерации»
- c) ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и развитию»
- d) Семейный кодекс РФ

Какое действие в сети Интернет педагогу следует классифицировать как кибербуллинг?

- a) массовая публикация унижительных сообщений на странице ребенка в социальных сетях
- b) дизлайк под видео со дня рождения ребенка
- c) удаление ребенка из списка друзей
- d) отклонение запроса ребенка на добавление в друзья

В ответ на какое увлечение учеников педагогу следует отреагировать настороженно и провести мониторинг социальных сетей с целью выяснить, нет ли среди учащихся класса тех, кто увлечен сообществами по теме «стрельба в школе»?

- a) повышенный интерес к начальной военной подготовке
- b) ношение футболок с надписью Natural Selection
- c) изображение акул и касаток на одежде

d) массовое ношение красных ниток на запястье

В Ребенок в общении с преподавателем демонстрирует увлечение криминальной субкультурой. С уважением высказывается о преступниках и открыто демонстрирует пренебрежение к любым законам и правилам. Как действовать?

a) Довести информацию до родителей и руководства школы

b) Заявить в полицию, пусть проведут служебный мониторинг и проверку

c) Постараться в доверительном общении выяснить больше информации о круге общения и действиях школьника

d) Потребовать назвать старших «авторитетов», при необходимости связаться с ними и получить дополнительную информацию о новом увлечении обучающегося.

Что в поведении ученика педагогу следует квалифицировать как тенденцию к развитию зависимости от онлайн-казино?

a) постоянные попытки взять реванш

b) попытки занять деньги на обед у одноклассников

c) эмоциональное возбуждение во время онлайн-игры на переменах

d) частые обсуждения игр с друзьями

d) сказать ученику, что это неприлично

Какое сочетание цифр активно используется в сетевых сообществах, посвященных деструктивной ARG «Синий кит»?

a) 15.88

b) 4.20

c) 18.88

d) 6.66