

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

Федеральное государственное автономное образовательное учреждение
дополнительного профессионального образования

**«Академия реализации государственной политики
и профессионального развития работников образования
Министерства просвещения Российской Федерации»
(ФГАОУ ДПО «Академия Минпросвещения России»)**

«УТВЕРЖДАЮ»

Начальник управления по развитию
дополнительного профессионального
образования

Т.В. Расташанская

2021 г.



**Дополнительная профессиональная программа
(повышение квалификации)**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ:
СОЦИАЛЬНЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ**

Авторский коллектив:
ФГАОУ ДПО «Академия
Минпросвещения России»
Федорова Ю.В.,
Невская О.В.

ГАОУ ДПО «Корпоративный университет»
Новиков К.А.

Раздел 1. «Характеристика программы»

1.1. Цель реализации программы: совершенствование профессиональных компетенций слушателей в области информационной безопасности детей.

1.2. Планируемые результаты обучения

А. Руководители

Должностные обязанности (По ЕКС)	Планируемые результаты обучения
<p>Определяет стратегию, цели и задачи развития образовательного учреждения, принимает решения о программном планировании его работы, участии образовательного учреждения в различных программах и проектах, обеспечивает соблюдение требований, предъявляемых к условиям образовательного процесса, образовательным программам, результатам деятельности образовательного учреждения и к качеству образования, непрерывное повышение качества образования в образовательном учреждении.</p>	<p>Знать:</p> <ul style="list-style-type: none"> - приоритетные направления развития образовательной системы Российской Федерации; - действующие нормативные документы в области информационной безопасности детей; - управленческие подходы по организации защиты детей от информационных угроз. <p>Уметь:</p> <ul style="list-style-type: none"> - организовывать деятельность по выявлению и защите детей от основных социальных угроз; - организовывать деятельность по защите детей от возникающих угроз при работе с персональными устройствами; - организовывать деятельность по защите детей от фишинга; - организовывать деятельность по защите детей от угроз, связанных с кибербуллингом; - организовывать деятельность по защите детей от угроз, связанных с экстремизмом, группами смерти и АУЕ*

Б. Учителя

Трудовые действия (Профессиональный стандарт «Педагог»)	Знать	Уметь

* Запрещенная на территории РФ

Регулирование поведения обучающихся для обеспечения безопасной образовательной среды (воспитательная деятельность)	<ul style="list-style-type: none"> - приоритетные направления развития образовательной системы Российской Федерации; - действующие нормативные документы в области информационной безопасности детей; - основные информационные угрозы; - основные механизмы защиты детей от информационных угроз. 	<ul style="list-style-type: none"> - применять механизмы выявления и защиты детей от основных социальных угроз; - применять механизмы выявления и защиты детей от возникающих угроз при работе с персональными устройствами; - применять механизмы выявления и защиты детей от фишинга; - применять механизмы выявления и защиты от угроз, связанных с кибербуллингом; - применять механизмы выявления и защиты детей от угроз, связанных с экстремизмом, группами смерти и АУЕ*
--	--	---

1.3. Категория слушателей: руководители образовательных организаций, педагогические работники реализующие программы общего образования, среднего профессионального образования.

1.4. Форма обучения: очно-заочная /очная/ заочная с применением электронного обучения, дистанционных образовательных технологий.

1.5. Срок освоения программы: 48 часов.

Раздел 2. «Содержание программы»

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Самостоятельная работа	Формы контроля
			Лекции	Интерактивные занятия		
1. Инвариантная часть «Государственная политика в образовании»						

* Запрещенная на территории РФ

1.1	Государственная политика в сфере общего образования Российской Федерации. Нормативное регулирование в области информационной безопасности детей	2			2	
1.2	Цифровая трансформация образования	2			2	Тестирование
2. Вариативная часть для руководителей						
2.1	Модуль 1. Планирование и организация деятельности по защите детей от социальных угроз сети Интернет	9	4	3	2	
2.1.1	Планирование и организация деятельности по обеспечению информационной безопасности в образовательной организации.	2	1		1	
2.1.2	Планирование и организация деятельности по выявлению признаков коллективной интернет-истерии	2	1	1		
2.1.3	Планирование и организация деятельности по предотвращению ситуаций, связанных со скулшутингом	2	1	1		
2.1.4	Планирование и организация деятельности по	3	1	1	1	Практическая работа № 1

	выявлению признаков опасного досуга учащихся					
2.2	Модуль 2. Планирование и организация деятельности по выявлению технологических угроз сети Интернет	7	3	2	2	
2.2.1	Планирование и организация деятельности по защите от вредоносных программ	3	1	1	1	
2.2.2	Планирование и организация деятельности по внедрению в практику образовательной организации правил сетевой гигиены	2	1		1	
2.2.3	Планирование и организация деятельности по Безопасному использованию интеллектуальной собственности и предотвращению нарушений авторского права	2	1	1		Практическая работа № 2
2.3	Модуль 3. Планирование и организация деятельности по защите от психологических и техно-психологических угроз сети Интернет	6	3	1	2	
2.3.1	Планирование и организация деятельности по	2	1		1	

	профилактике онлайн-игровой зависимости					
2.3.2	Планирование и организация деятельности по профилактике в образовательной организации фрейпинга, скама, угроз псевдоблаготворительности	2	1		1	
2.3.3	Планирование и организация деятельности по защите детей от фишинга	2	1	1		Практическая работа № 3
2.4	Модуль 4. Планирование и организация деятельности по защите детей от социально-технологических угроз сети Интернет	11	5	3	3	
2.4.1	Планирование и организация деятельности по Предотвращению вовлечения детей в незаконную деятельность в сети Darknet	2	1		1	
2.4.2	Планирование и организация деятельности по защите детей от опасностей, связанных с наркоторговлей в Darknet	4	2	2		
2.4.3	Планирование и организация деятельности по обеспечению безопасной работы учеников и	2	1		1	

	педагогов в соцсетях					
2.4.4	Планирование и организация деятельности по профилактике кибербуллинга	3	1	1	1	Практическая работа № 4
2.5	Модуль 5. Планирование и организация деятельности по защите детей от социально-психологических угроз сети Интернет	9	4	1	4	
2.5.1	Планирование и организация деятельности по профилактике экстремизма	2	1		1	
2.5.2	Планирование и организация деятельности по защите детей от опасностей, связанных с группами смерти и ARG	2	1		1	
2.5.3	Планирование и организация деятельности по профилактике вовлечения детей в АУЕ* и другие неконформистские субкультуры	2	1		1	
2.5.4	Планирование и организация деятельности по защите детей от груминга и секстинга	3	1	1	1	Практическая работа № 5

* Запрещенная на территории РФ

	Итоговая аттестация	2			2	Зачет
	Итого:	48	19	10	19	
3. Вариативная часть для учителей						
3.1	Модуль 1. Социальные угрозы сети Интернет	9	4	3	2	
3.1.1	Информационная безопасность.	2	1		1	
3.1.2	Коллективная интернет-истерия	2	1	1		
3.1.3	Скулшутинг	2	1	1		
3.1.4	Опасный досуг	3	1	1	1	Практическая работа № 1
3.2	Модуль 2. Технологические угрозы сети Интернет	7	3	2	2	
3.2.1	Вредоносные программы	3	1	1	1	
3.2.2	Сетевая гигиена	2	1		1	
3.2.3	Безопасное использование авторского контента	2	1	1		Практическая работа № 2
3.3	Модуль 3. Психологические и техно-психологические угрозы сети Интернет	6	3	1	2	
3.3.1	Феномен онлайн-игровой зависимости	2	1		1	
3.3.2	Фрейпинг, скам, псевдоблаготворительность	2	1		1	
3.3.3	Фишинг	2	1	1		Практическая работа № 3
3.4	Модуль 4. Социально-технологические угрозы сети Интернет	11	5	3	3	
3.4.1	Что такое Darknet	2	1		1	
3.4.2	Наркоторговля в Darknet	4	2	2		

3.4.3	Правила безопасности соцсетей	2	1		1	
3.4.4	Кибербуллинг	3	1	1	1	Практическая работа № 4
3.5	Модуль 5. Социально-психологические угрозы сети Интернет	9	4	1	4	
3.5.1	Экстремизм	2	1		1	
3.5.2	Группы смерти и ARG	2	1		1	
3.5.3	АУЕ* и неконформистские субкультуры	2	1		1	
3.5.4	Грумминг и секстинг	3	1	1	1	Практическая работа № 5
	Итоговая аттестация	2			2	Зачет
	Итого:	48	19	10	19	

2.2. Рабочая программа

Инвариантная часть «Государственная политика в образовании»

1.1. Государственная политика в сфере общего образования Российской Федерации. Нормативное регулирование в области информационной безопасности детей

Самостоятельная работа (2 ч.). Образовательное законодательство Российской Федерации. Цели и ключевые задачи Российской Федерации в сфере образования. Показатели федеральных проектов. Механизмы достижения поставленных целей. Единая система научно-методического сопровождения педагогических работников и управленческих кадров.

Законодательные и нормативные акты Российской Федерации в области информационной безопасности.

1.2. Цифровая трансформация образования

Самостоятельная работа (2 ч.). Национальная цель «Цифровая трансформация». Суть цифровой трансформации образования. Технологическое обновление и новая дидактика образования, персонализации образовательного процесса на основе использования растущего потенциала

* Запрещенная на территории РФ

цифровых технологий. Актуальные навыки и практики преподавания в цифровую эпоху. Анализ мер, реализуемых Правительством Российской Федерации в рамках федерального проекта «Цифровая образовательная среда» национального проекта «Образование»: цели, задачи, основные мероприятия и результаты реализации. Выполнение тестовых заданий.

2. Вариативная часть для руководителей

2.1. Модуль 1. Планирование и организация деятельности по защите детей от социальных угроз сети Интернет

2.1.1. Планирование и организация деятельности по обеспечению информационной безопасности в образовательной организации

Лекция (1 ч.). Организация работы по использованию алгоритма безопасного использования сети Интернет: Актуальные угрозы информационной безопасности и защита информации при организации урока. Проведение аудита сайта на предмет возможности его использования в образовательной деятельности. Анализ типовых ошибок, меры по их предотвращению, устранению и защите образовательной организации от угроз сети Интернет.

Самостоятельная работа (1 ч.). Изучение учебных материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.1.2. Планирование и организация деятельности по выявлению признаков коллективной интернет-истерии

Лекция (1 ч.). Тренды, челленджи, флешмобы, опасный досуг. Подростковый суицид как соцсетевой феномен. Особенности социально-психологического и технологического характера. Анализ механизмов социальных платформ (МойМир, Вконтакте и пр.) для организации технологической работы в ситуациях потенциальных или актуальных угроз с точки зрения родительской и преподавательской аудитории.

Интерактивное занятие (1 ч.). Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

2.1.3. Планирование и организация деятельности по предотвращению ситуаций, связанных со скулшутингом

Лекция (1 ч.). Организация работы по анализу признаков возникновения ситуаций школьной стрельбы (скулшутинга): методология проверки аккаунтов несовершеннолетних в социальных сетях для выявления признаков субкультуры «школьных стрелков». Анализ данных, поведенческих признаков и вопросы профилактики.

Интерактивное занятие (1 ч.). Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы

путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

2.1.4. Планирование и организация деятельности по выявлению признаков опасного досуга учащихся

Лекция (1 ч.). Планирование и организация мероприятий по выявлению ситуаций с опасным досугом, руферов, зацеперов и т.п. Признаки и методология проверки аккаунтов несовершеннолетних в социальных сетях для выявления признаков субкультуры руферов, зацеперов и т.п.

Интерактивное занятие (1 ч.). Практическая работа № 1. (Выполняется онлайн на интерактивном занятии). Организация деятельности по анализу ситуаций и выявлению признаков *интернет*-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.2. Модуль 2. Планирование и организация деятельности по выявлению технологических угроз сети Интернет

2.2.1. Планирование и организация деятельности по защите от вредоносных программ

Лекция (1 ч.). Организация защиты от вредоносного ПО – вирусы, черви, трояны, бэкдоры, руткиты, ботнеты, макровирусы и т.п., - принципы работы, назначение, векторы атаки. Спам и навязчивая реклама как разновидность вредоносного ПО. Квалифицированные хакерские атаки, вирусы-шифровальщики.

Интерактивное занятие (1 ч.). Организация противодействия распространённым ошибкам, создающим уязвимости для кибератак. Распространенные ошибки, приводящие к уязвимостям подключенных к сети Интернет устройств. Ответственность за нарушение правил сбора, хранения, использования и удаления охраняемой законом информации.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.2.2. Планирование и организация деятельности по внедрению в практику образовательной организации правил сетевой гигиены

Лекция (1 ч.). Применение в образовательной организации практических рекомендаций по защите от современных угроз – алгоритмов безопасного использования сети Интернет:

- как использовать устройства при выходе в сеть Интернет;

- меры предосторожности при использовании электронной почты, мессенджеров и смс
- правила подключения к публичным wi-fi сетям;
- безопасное скачивание файлов;
- настройка безопасного поиска в поисковых системах, оценка и поиск безопасных сайтов через поисковые системы;
- удаление истории и файлов cookie из браузера;
- принцип организации резервного копирования ценной информации.

Как работает stalking – поиск максимального количества информации человека по открытым источникам.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.2.3. Планирование и организация деятельности по Безопасному использованию интеллектуальной собственности и предотвращению нарушений авторского права

Лекция (1 ч.). Применимость в образовательной деятельности права на использование чужого контента, цитирование, консервативное авторское право, современные лицензиары, свободная лицензия, Creative Commons, правила использования свободной лицензии в образовании, виды лицензий.

Интерактивное занятие (1 ч.). Практическая работа № 2. (Выполняется онлайн на интерактивном занятии). Организация работы по применению в образовательной организации алгоритма обеспечения максимальной защиты персональных устройств. Ассоциирование логотипов свободных лицензий с соответствующими им лицензионными условиями.

2.3. Модуль 3. Планирование и организация деятельности по защите от психологических и техно-психологических угроз сети Интернет

2.3.1. Планирование и организация деятельности по профилактике онлайн-игровой зависимости

Лекция (1 ч.). Организация в образовательной организации работы по выявлению механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры. Профилактика игровой зависимости и зависимости от азартных онлайн-игр: умение распознавать ТОП-5 современных компьютерных онлайн-игр. Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.3.2. Планирование и организация деятельности по профилактике в образовательной организации фрейпинга, скама, угроз псевдоблаготворительности

Лекция (1 ч.). Организация выявления в условиях образовательной организации программных инструментов, предназначенных для кибермошенничества. Методы психологического манипулирования и технологическое обеспечение мошенничества. Способы выявления. Анализ собственной устойчивости к скаму и психоманипулированию при помощи тестов ситуаций.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.3.3. Планирование и организация деятельности по защите детей от фишинга

Лекция (1 ч.). Организация распознавания разных видов и типов фишинга. Статистика – сегодня фишинг — наиболее часто встречающееся киберпреступление. Смычка технологии и психологии, проблема цитирования в интернете как важный маркер психологической устойчивости пользователей.

Интерактивное занятие (1 ч.). Практическая работа № 3. (Выполняется онлайн на интерактивном занятии). Организация определения безопасных ресурсов среди представленных фишинговых электронных писем и сайтов.

2.4. Модуль 4. Планирование и организация деятельности по защите детей от социально-технологических угроз сети Интернет

2.4.1. Планирование и организация деятельности по Предотвращению вовлечения детей в незаконную деятельность в сети

Лекция (1 ч.). Организация работы по знакомству педагогов с опасными проявлениями анонимной сети Darknet. Принципы функционирования и угрозы криптосетей, методы и инструменты вовлечения детей в опасные сообщества сети Darknet.

Как устроена и функционирует анонимная сеть Darknet, какие угрозы и опасные маркеры содержит. Что такое Tor. Криптовалюта как феномен теневого рынка. Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

2.4.2. Планирование и организация деятельности по защите детей от опасностей, связанных с наркоторговлей в Darknet
Лекция (2 ч.). Торговля наркотиками в сети Darknet. Классификация ПАВ. Вовлечение подростков в употребление и распространение ПАВ. Организация распознавания членами школьной команды речевых маркеров и невербальных признаков причастности к субкультуре потребителей ПАВ. Статистика распространения и употребления ПАВ.

Интерактивное занятие (2 ч.). Организация в образовательной организации работы по распознаванию педагогами признаков употребления психоактивных веществ. Обучающиеся анализируют видеоролики, фиксируют характерные признаки в поведении людей, предполагают вещество, под действием которого находятся герои роликов и предлагают возможные сценарии своего поведения в аналогичной ситуации. Анализ диалогов школьников, в которых содержатся тревожные речевые маркеры. Сортировка жаргонных фраз.

2.4.3. Планирование и организация деятельности по обеспечению правил безопасности соцсетей

Лекция (1 ч.). Овершаринг. Современные тренды и взаимосвязи между открытым доступом к персональным данным и возможными угрозами жизни, здоровью и безопасности несовершеннолетнего на основе актуальных исследований. Организация работы по определению признаков овершаринга на примере предложенных профайлов. Критерии допустимости раскрытия личной информации.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

2.4.4. Планирование и организация деятельности по профилактике кибербуллинга

Лекция (1 ч.). Кибербуллинг (троллинг, моббинг и т.п.). Организация определения педагогами причины и механики возникновения, ролей. Коллективный зритель как главный травмирующий фактор – принципиальное отличие кибербуллинга от буллинга. Организация реагирования, возможности и инструменты противодействия.

Интерактивное занятие (1 ч.). Практическая работа № 4. (Выполняется онлайн на интерактивном занятии). Планирование сценариев противодействия кибербуллингу в образовательной организации с позиций ключевых социальных ролей участников.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

2.5. Модуль 5. Планирование и организация деятельности по защите детей от социально-психологических угроз сети Интернет

2.5.1. Планирование и организация деятельности по защите детей от экстремизма.

Лекция (1 ч.). Экстремизм и хулиганство. Наличие идеологической или религиозной подоплеки. Признаки вовлечения школьника в экстремистское сообщество. Ответственность. Религиозные и политические радикальные группы. Христианские ортодоксальные секты, исламские фундаменталисты, ячейки радикальных суннитских джамаатов на территории России и бывшего СНГ. Планирование и организация действий по использованию алгоритма корректного и эффективного реагирования на угрозу, сопровождение ситуации педагогическим коллективом и управленческой командой, взаимодействие с правоохранительными структурами.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

2.5.2. Планирование и организация деятельности по защите детей от опасностей, связанных с группами смерти и ARG.

Лекция (1 ч.). Деструктивные ARG (феномен доведения до самоубийства с использованием игротехник и коммуникации в соцсети). «Группы смерти» и их администраторы. Признаки, особенности. Эволюция и технологические аспекты деструктивных игротехник («Синий кит», «Момо», «Красная сова» и т.д.). Организация выявления в образовательной организации признаков вовлечения ребенка в участие в ARG по комплексу признаков на его странице в соцсети.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

2.5.3. Планирование и организация деятельности по профилактике вовлечения детей в АУЕ* и другие неконформистские субкультуры

Лекция (1 ч.). «АУЕ*». Запрещенная околोकриминальная субкультура. Организация профилактических мероприятий, противостоящих угрозе вовлечения детей и молодежи в квазикриминальную субкультуру,

* Запрещенная на территории РФ

особенности идеологического контекста и фактического функционирования. Анализ предложенных ситуаций и выявление признаков принадлежности к «АУЕ*».

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

2.5.4. Планирование и организация деятельности по защите детей от груминга и секстинга

Лекция (1 ч.). Груминг и секстинг, Субкультура педофилов: методики и способы «обработки» детей. Организация профилактических мероприятий, противостоящих угрозе вовлечения несовершеннолетних в коммуникацию с педофилами. Форматы мониторинга и предупреждения опасных ситуаций с несовершеннолетними.

Интерактивное занятие (1 ч.). Практическая работа № 5. (Выполняется онлайн на интерактивном занятии). Организация работы по определению типа информационной угрозы на примере представленных материалов (экстремизм, группы смерти, АУЕ*).

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

Итоговая аттестация

Самостоятельная работа (2 ч.).

3. Вариативная часть для учителей

3.1. Модуль 1. Социальные угрозы сети Интернет

3.1.1. Информационная безопасность

Лекция (1 ч.). Алгоритмы безопасного использования сети Интернет: Актуальные угрозы информационной безопасности и защита информации при организации урока. Аудит сайта на предмет возможности его использования в образовательной деятельности. Анализ типовых ошибок, меры по их предотвращению, устранению и защите образовательной организации от угроз сети Интернет.

Самостоятельная работа (1 ч.). Изучение учебных материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.1.2. Коллективная интернет-истерия

Лекция (1 ч.). Тренды, челленджи, флешмобы, опасный досуг. Подростковый суицид как соцсетевой феномен. Особенности социально-психологического и технологического характера. Анализ механизмов социальных платформ

(МойМир, Вконтакте и пр.) для технологической работы в ситуациях потенциальных или актуальных угроз с точки зрения родительской и преподавательской аудитории.

Интерактивное занятие (1 ч.). Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

3.1.3. Скулшутинг

Лекция (1 ч.). Школьная стрельба (скулшутинг): признаки и методология проверки аккаунтов несовершеннолетних в социальных сетях для выявления признаков субкультуры «школьных стрелков». Анализ данных, поведенческих признаков и вопросы профилактики.

Интерактивное занятие (1 ч.). Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

3.1.4. Опасный досуг

Лекция (1 ч.). Опасный досуг, руферы, зацеперы и т.п. Признаки и методология проверки аккаунтов несовершеннолетних в социальных сетях для выявления признаков субкультуры руферов, зацеперов и т.п.

Интерактивное занятие (1 ч.). Практическая работа № 1. (Выполняется онлайн на интерактивном занятии). Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.2. Модуль 2. Технологические угрозы сети Интернет

3.2.1. Вредоносные программы

Лекция – (1 ч.). Виды вредоносного ПО – вирусы, черви, трояны, бэкдоры, руткиты, ботнеты, макровирусы и т.п., - принципы работы, назначение, векторы атаки. Спам и навязчивая реклама как разновидность вредоносного ПО. Квалифицированные хакерские атаки, вирусы-шифровальщики.

Интерактивное занятие (1 ч.). Определение мер противодействия распространённым ошибкам, создающим уязвимости для кибератак. Распространенные ошибки, приводящие к уязвимостям подключенных к сети Интернет устройств. Ответственность за нарушение правил сбора, хранения, использования и удаления охраняемой законом информации.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.2.2. Сетевая гигиена

Лекция (1 ч.). Практические рекомендации по защите от современных угроз – алгоритмы безопасного использования сети Интернет:

- как использовать устройства при выходе в сеть Интернет;
- меры предосторожности при использовании электронной почты, мессенджеров и смс
- правила подключения к публичным wi-fi сетям;
- безопасное скачивание файлов;
- настройка безопасного поиска в поисковых системах, оценка и поиск безопасных сайтов через поисковые системы;
- удаление истории и файлов cookie из браузера;
- принцип организации резервного копирования ценной информации.

Практика сталкеринга – поиска максимального количества информации человека по открытым источникам

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.2.3. Безопасное использование авторского контента

Лекция (1 ч.). Право на использование чужого контента, цитирование, консервативное авторское право, современные лицензиары, свободная лицензия, Creative Commons, правила использования свободной лицензии в образовании, виды лицензий.

Интерактивное занятие (1 ч.). Практическая работа № 2. (Выполняется онлайн на интерактивном занятии). Алгоритм обеспечения максимальной защиты персональных устройств. Ассоциирование логотипов свободных лицензий с соответствующими им лицензионными условиями.

3.3. Модуль 3. Психологические и техно-психологические угрозы сети Интернет

3.3.1. Феномен онлайн-игровой зависимости

Лекция (1 ч.). Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры. Игровая зависимость и зависимость от азартных онлайн-игр: умение распознавать ТОП-5 современных компьютерных онлайн-игр. Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.3.2. Фрейпинг, скам, псевдоблаготворительность.

Лекция (1 ч.). Виды программных инструментов, предназначенных для кибермошенничества. Методы психологического манипулирования и технологическое обеспечение мошенничества. Способы выявления. Анализ собственной устойчивости к скаму и психоманипулированию при помощи тестов ситуаций.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.3.3. Фишинг

Лекция (1 ч.). Виды и типы фишинга. Статистика – сегодня фишинг — наиболее часто встречающееся киберпреступление. Смычка технологии и психологии, проблема цитирования в интернете как важный маркер психологической устойчивости пользователей.

Интерактивное занятие (1 ч.). Практическая работа № 3. (Выполняется онлайн на интерактивном занятии). Определение безопасного ресурса среди представленных фишинговых электронных писем и сайтов.

3.4. Модуль 4. Социально-технологические угрозы сети Интернет

3.4.1. Что такое Darknet

Лекция (1 ч.). Что такое анонимная сеть Darknet. Принципы функционирования и угрозы криптосетей, методы и инструменты вовлечения детей в опасные сообщества сети Darknet.

Как устроена и функционирует анонимная сеть Darknet, какие угрозы и опасные маркеры содержит. Что такое Tor. Криптовалюта как феномен теневого рынка. Анализ предложенных ситуаций и выявление признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде.

3.4.2. Наркотоорговля в Darknet

Лекция (2 ч.). Торговля наркотиками в сети Darknet. Классификация ПАВ. Вовлечение подростков в употребление и распространение ПАВ. Речевые маркеры и невербальные признаки причастности к субкультуре потребителей ПАВ. Статистика распространения и употребления ПАВ.

Интерактивное занятие (2 ч.). Анализ признаков употребления психоактивных веществ. Обучающиеся анализируют видеоролики, фиксируют характерные признаки в поведении людей, предполагают вещество, под действием которого находятся герои роликов и предлагают возможные сценарии своего поведения в аналогичной ситуации. Анализ диалогов школьников, в которых содержатся тревожные речевые маркеры. Сортировка жаргонных фраз.

3.4.3. Правила безопасности соцсетей

Лекция (1 ч.). Овершаринг. Современные тренды и взаимосвязи между открытым доступом к персональным данным и возможными угрозами жизни, здоровью и безопасности несовершеннолетнего на основе актуальных исследований. Определение признаков овершаринга в предложенных профайлах. Критерии допустимости раскрытия личной информации.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

3.4.4. Кибербуллинг

Лекция (1 ч.). Кибербуллинг (троллинг, моббинг и т.п.). Определения, причины и механика возникновения, роли. Коллективный зритель как главный травмирующий фактор – принципиальное отличие кибербуллинга от буллинга. Особенности реагирования, возможности и инструменты противодействия.

Интерактивное занятие (1 ч.). Практическая работа № 4. (Выполняется онлайн на интерактивном занятии). Формирование собственных сценариев противодействия возникшему кибербуллингу с позиций ключевых социальных ролей участников.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

3.5. Модуль 5. Социально-психологические угрозы

3.5.1. Экстремизм

Лекция (1 ч.). Экстремизм и хулиганство. Наличие идеологической или религиозной подоплеки. Признаки вовлечения школьника в экстремистское сообщество. Ответственность. Религиозные и политические радикальные группы. Христианские ортодоксальные секты, исламские фундаменталисты, ячейки радикальных суннитских джамаатов на территории России и бывшего СНГ. Разработка алгоритма корректного и эффективного реагирования на

угрозу, сопровождение ситуации педагогическим коллективом, взаимодействие с правоохранительными структурами.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

3.5.2. Группы смерти и ARG

Лекция (1 ч.). Деструктивные ARG (феномен доведения до самоубийства с использованием игротехник и коммуникации в соцсети). «Группы смерти» и их администраторы. Признаки, особенности. Эволюция и технологические аспекты деструктивных игротехник («Синий кит», «Момо», «Красная сова» и т.д.). Выявление признаков вовлечения ребенка в участие в ARG по комплексу признаков на его странице в соцсети.

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

3.5.3. АУЕ* и неконформистские субкультуры

Лекция (1 ч.). «АУЕ*». Запрещенная околोकриминальная субкультура. Профилактика вовлечения детей и молодежи в квазикриминальную субкультуру, особенности идеологического контекста и фактического функционирования. Анализ предложенных ситуаций и выявление признаков принадлежности к «АУЕ*».

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

3.5.4. Груминг и секстинг

Лекция (1 ч.). Груминг и секстинг, Субкультура педофилов: методики и способы «обработки» детей. Профилактика вовлечения несовершеннолетних в коммуникацию с педофилами. Форматы мониторинга и предупреждения опасных ситуаций с несовершеннолетними.

Интерактивное занятие (1 ч.). Практическая работа № 5. (Выполняется онлайн на интерактивном занятии). Определение типа информационной угрозы на основе проанализированных материалов.

* Запрещена на территории РФ

Самостоятельная работа (1 ч.). Изучение материалов по теме. Ответы на вопросы для самопроверки. Выполнение тренировочных заданий в цифровой среде.

Итоговая аттестация

Самостоятельная работа (2 ч.).

Раздел 3. Формы аттестации и оценочные материалы

Инвариантный модуль.

Условия успешного завершения курса: выполнение всех предусмотренных программой практических работ, тестов, не менее 60% правильно выполненных заданий итоговой аттестации.

1. Инвариантная часть «Государственная политика в образовании»

Освоение раздела завершается тестированием. Тест включает 15 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 60% заданий, соответственно набрано не менее 9 баллов.

Примеры тестовых заданий.

Расставьте в иерархической последовательности нижеприведенные документы:

- 1) Федеральный закон «Об образовании в Российской Федерации».
- 2) Национальная доктрина образования в Российской Федерации.
- 3) Конституция Российской Федерации.
- 4) Указ «О национальных целях развития Российской Федерации на период до 2030 г.»

Основными принципами цифровой дидактики выступают (выбор всех правильных вариантов):

- 1) Персонализация образовательного процесса.
- 2) Многоступенчатый мониторинг достижений ребенка.
- 3) Сохранение традиционной роли учителя.

А. Для руководителей

Модуль 1. Планирование и организация деятельности по защите детей от социальных угроз сети Интернет

Практическая работа № 1. Организация деятельности по анализу ситуаций и выявлению признаков интернет-угрозы. Определение типа информационной угрозы путем анализа предложенных ситуаций. Определение технологии, методики и инструментов предотвращения информационных угроз.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

<p>Алгоритм выполнения</p>	<p>Проанализировать профили несовершеннолетних (разработанных на основе реальных данных и ситуаций), выявить подозрительные признаки и отнести выявленные признаки к одной из социальных угроз</p> <p>Критерии анализа:</p> <ul style="list-style-type: none"> • визуальные образы • текстовая информация • сообщества, подписки, друзья <p>Определить тип информационной угрозы в отношении несовершеннолетнего</p> <p>Предположить возможные предпосылки вовлечения несовершеннолетнего в опасные сообщества/деятельность.</p> <p>Составить примерный план работы педагогического коллектива с профилями несовершеннолетних в социальных сетях</p> <p>Проверить правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Ответы на задание сообщить преподавателю или разместить в группе поддержки курса в Telegram</p>
<p>Критерии оценивания</p>	<p>Опасные признаки выявлены.</p> <p>Тип угрозы определен.</p> <p>План работы составлен.</p> <p>Ответы размещены в группе поддержки курса в Telegram</p>
<p>Оценка</p>	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Какие рекомендации по информационной безопасности руководитель может дать родителям (законным представителям) детей 9-12 лет? (выбор одного правильного ответа):

- 1) регулярно разговаривайте с ребенком о том, что происходит в его «онлайн-жизни»
- 2) установите систему «Родительского контроля» на устройствах, с которых ребенок будет выходить в Интернет
- 3) установите программу-шпион на устройствах ребенка для скрытого наблюдения за его действиями в интернете
- 4) запретите ребенку иметь аккаунты в социальных сетях

В ответ на какое увлечение учеников в школе руководителю образовательной организации следует отреагировать настороженно и поручить провести мониторинг социальных сетей с целью выяснить, нет ли среди учащихся тех, кто увлечен сообществами по теме «Колумбайн»? (выбор одного правильного ответа):

- 1) предпочтение в одежде длинных темных плащей;
- 2) предпочтение одежды с символикой акул и касаток;
- 3) появление значков Columbian;
- 4) предпочтение играть в онлайн-игре на стороне террористов.

Модуль 2. Планирование и организация деятельности по выявлению технологических угроз сети Интернет

Практическая работа № 2. Организация работы по применению в образовательной организации алгоритма обеспечения максимальной защиты персональных устройств.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	Составьте план внедрения алгоритма обеспечения максимальной защиты персональных устройств учеников и педагогического состава школы, для этого предварительно выполните следующие действия по защите собственного устройства: Проанализируйте установки своего смартфона/ компьютера по подключению к Wi-fi сетям
---------------------	---

	<p>Установите наиболее безопасные опции подключения</p> <p>Выясните, каким антивирусным ПО вы пользуетесь. Настройте брандмауэр и встроенный антивирус.</p> <p>Изучите историю браузера в своем устройстве (смартфоне или ПК). Почистите историю поисковых запросов и куки</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Выполнены все этапы работы: настроено безопасное подключение к Wi-fi, очищены куки и история браузера, план работы составлен.</p> <p>Отчет о выполнении задания размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Как обеспечить защиту школьников от всех технологических угроз сети Интернет? (выбор одного правильного ответа):

- 1) Установить на все устройства комплексные системы защиты с антивирусом, спам-фильтром, сканером трафика, брандмауэром и выставить все установки в режим максимально возможной защиты
- 2) Достаточно поставить антивирус и соблюдать правила цифровой гигиены
- 3) Единственный способ защититься ото всех угроз сети Интернет – никогда не подключаться к сети Интернет. Других гарантированных способов не существует
- 4) Выходить в интернет из внутренних корпоративных сетей – тогда между пользователем и злоумышленниками стоит как минимум IT персонал интранета

Руководитель узнал, что произошла утечка персональных данных: в интернет попала база с фамилиями и номерами телефонов учащихся. В течение дня

ученики получают оскорбительные сообщения и ссылку на «архив с твоими грязными фотографиями». Каковы правильные действия руководителя в этой ситуации? (выбор одного правильного ответа):

- 1). Самостоятельно проверить архив с фотографиями на предмет опасного для детей и\или запрещенного контента, обратиться в полицию.
- 2). Издать приказ по учебному заведению с запретом переходить по ссылке из сообщения.
- 3). Написать в Роскомнадзор с требованием провести проверку информации, размещенной по ссылке и заблокировать ресурс в случае выявления нарушений.
- 4). Организовать проведение классного часа на тему «Азбука защиты от фишинга в сети интернет», рассказать, что чрезвычайно опасно переходить по ссылкам из непрошенных писем.

Модуль 3. Планирование и организация деятельности по защите от психологических и техно-психологических угроз сети Интернет

Практическая работа № 3. Организация определения безопасных ресурсов среди представленных фишинговых электронных писем и сайтов.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

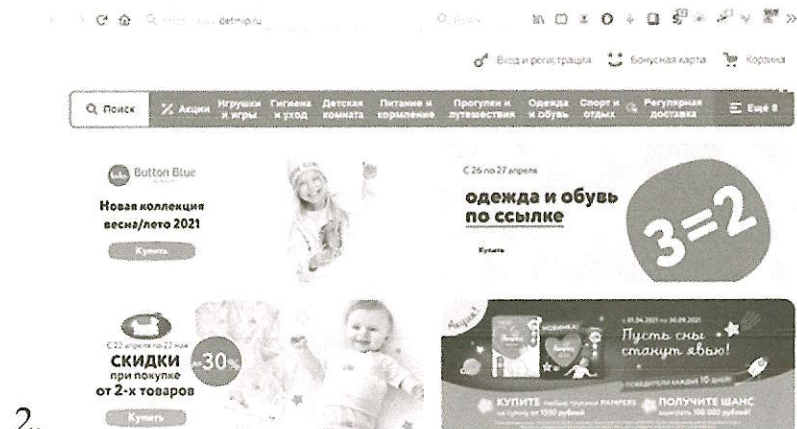
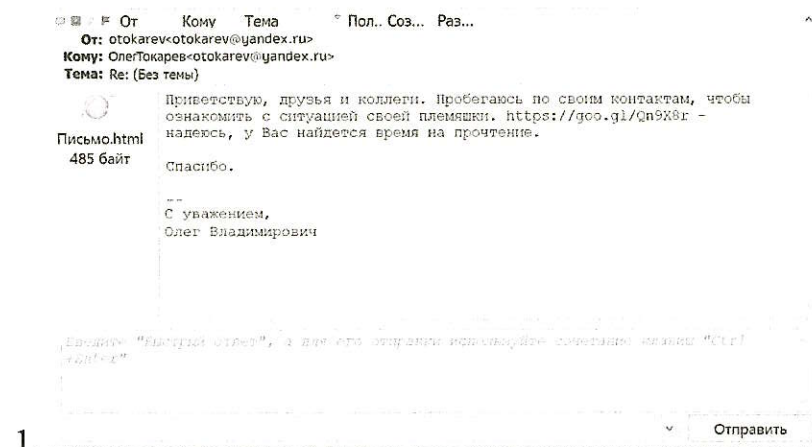
Алгоритм выполнения	<p>Проанализируйте предложенные скриншоты с ресурсами (сайты, электронные сообщения, и пр.); Изучите скриншоты, основываясь на материалах лекций и материалах в цифровой среде, выясните, какие из предложенных ресурсов безопасны</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Составьте план работы по обеспечению использования безопасных ресурсов в школе.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Безопасный ресурс отобран</p> <p>Названы причины, по которым остальные ресурсы представляются опасными.</p>

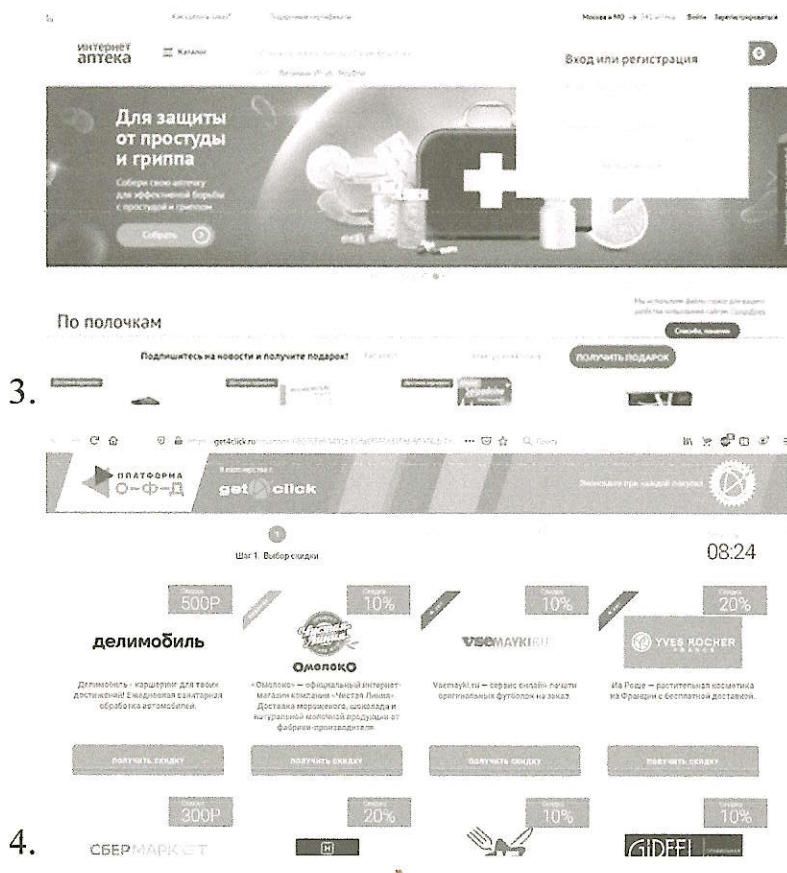
	<p>Составлен план действий по обеспечению использования безопасных ресурсов в школе.</p> <p>Отчет о выполнении задания размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Выберите из четырех предлагаемых скриншотов те, которые, на ваш взгляд небезопасны. (выбор всех правильных ответов):





Выберите лишний элемент среди этапов формирования аддикции к онлайн-играм (выбор одного правильного ответа):

- 1) время, проведенное в игре, увеличивается
- 2) появляются новые интересы, связанные с игрой (фэнтези, аниме, военная техника и т.п.)
- 3) игровая активность формирует новые особенности поведения
- 4) ухудшение эмоционального самочувствия вне игровой активности

Модуль 4. Планирование и организация деятельности по защите детей от социально-технологических угроз сети Интернет

Практическая работа № 4. Планирование сценариев противодействия кибербуллингу в образовательной организации с позиций ключевых социальных ролей участников.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	Классифицировать предложенные решения ситуаций с кибербуллингом с точки зрения четырех основных социальных ролей: жертва, одноклассники, родители, классный руководитель
---------------------	--

	<p>Составить план противодействия кибербуллингу в образовательной организации с учетом разных социальных ролей.</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Все предложенные решения классифицированы в соответствии с одной из социальных ролей.</p> <p>План противодействия кибербуллингу составлен.</p> <p>Отчет о выполнении задания размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Руководитель получил сообщение о том, что кто-то из одиннадцатиклассников, используя школьный компьютер, посещал Darknet. Какие действия помогут руководителю выяснить, кто это был? (выбор одного правильного ответа):

- 1) поручить проанализировать страницы социальных сетей наименее успевающих учеников параллели и найти из них подписчика на сервис Darknet (покупка невозможна без подписки)
- 2) поручить зайти на Darknet.com не позднее двух недель после предполагаемой покупки и выяснить логин пользователя, поочередно запуская ping всех IP-адресов школьных компьютеров; затем выяснить, кто работал за данным компьютером
- 3) определить, на каком школьном компьютере остался анонимный браузер Tor; затем выяснить, кто работал за данным компьютером
- 4) собрать старшеклассников и постараться выяснить данную информацию во время беседы с ними

Какой признак с огромной вероятностью свидетельствует о том, что ребенок покупает наркотики в сети Darknet (выбор одного правильного ответа):

- 1) Использует символику растафарианства, выступает за легализацию марихуаны, слушает раста-рэпы с текстами про марихуану
- 2) У него в пенале были найдены неизвестные таблетки, которые оказались сильными антидепрессантами
- 3) Из его кармана выпал маленький предмет, похожий на комок изоленты, который он очень быстро поднял и спрятал обратно
- 4) На его руке браслет из большого количества маленьких разноразмерных магнитов

Модуль 5. Планирование и организация деятельности по защите детей от социально-психологических угроз сети Интернет

Практическая работа № 5. Организация работы по определению типа информационной угрозы на примере представленных материалов (экстремизм, группы смерти, АУЕ*).

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	<p>Проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов), выявить подозрительные признаки и отнести выявленные признаки к одной из социальных угроз</p> <p>Критерии анализа:</p> <ul style="list-style-type: none">• визуальные образы• текстовая информация• сообщества, подписки, друзья <p>Определить тип информационной угрозы в отношении несовершеннолетнего</p> <p>Предположить возможные предпосылки вовлечения несовершеннолетнего в опасные сообщества/деятельность.</p>
---------------------	--

* Запрещена на территории РФ

	<p>Составить план работы в образовательной организации по предотвращению данных угроз.</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Ответы на задание сообщить преподавателю или разместить в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Опасные признаки выявлены.</p> <p>Тип угрозы определен.</p> <p>План работы составлен.</p> <p>Ответ размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Родители одного из учеников сообщают, что готовы написать заявление в полицию на другого ученика, который вымогает у их сына деньги "на общак" и совершает мелкие кражи. Какое действие руководителя будет наиболее эффективным? (выбор одного правильного ответа):

- 1) Воспитательная беседа с учеником в присутствии его родителей.
- 2) Организация контакта соц.педагога с семьей учащегося в связи с вероятностью вовлечения ребенка в криминальное сообщество, а также информирование директора школы о необходимости обратиться в полицию в связи с субкультурно-обусловленным преступлением.
- 3) Организация классного часа на тему "Блатная жизнь: мифы и реальность" с участием представителя ФСИН
- 4) Самостоятельное обращение в полицию для постановки ученика на учет.

Ученики заметили, что одна из учениц получает сообщения от своего друга из интернета по имени «Теплый мишка». Никто из одноклассников не знаком с ним в реальной жизни, сама ученица на вопросы о нём отвечать отказывается.

Какое действие педагога в этой ситуации будет наиболее адекватным ситуации? (выбор одного правильного ответа):

- 1) Это — педофил, нужно запретить ученице использование средств связи во время учебного процесса, ограничить использование средств связи во время пребывания на территории школы.
- 2) Попытаться выяснить личность "друга" самостоятельно или через заявление в полицию.
- 3) Поговорить с родителями ученицы о социальных угрозах сети Интернет, рассказать о груминге и опасности сетевой педофилии и сообщить о факте соц.педагогу или школьному психологу
- 4) Провести классный час и вынести на обсуждение эту историю, чтобы дружба с "теплым мишкой" стала для ученицы неприглядным фактором

Итоговая аттестация.

Итоговая аттестация проводится в форме зачета. Зачет выставляется при условии выполнения всех предусмотренных программой практических работ, тестов и итогового тестирования.

Время выполнения – 2 ч. Количество попыток – 2.

Тест включает 15 заданий на владение основами информационной безопасности детей. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 60% заданий, соответственно набрано не менее 9 баллов.

Пример задания итогового тестирования.

Что из перечисленного НЕ является формой опасного досуга?

- 1) Руфтинг
- 2) Диггерство
- 3) Стендовая стрельба
- 4) Зацепинг

Какие приоритетные задачи устанавливает Концепция информационной безопасности детей для семьи, государства и организаций, заинтересованных в обеспечении информационной безопасности детей? (выбор всех правильных ответов):

- 1) повышение уровня медиаграмотности детей
- 2) усвоение детьми системы семейных ценностей
- 3) формирование у детей навыков по выбору правильного образовательного профиля
- 4) сохранение конфиденциальности документированной информации

Б. Для педагогов.

Модуль 1. Планирование и организация деятельности по защите детей от социальных угроз сети Интернет

Практическая работа № 1. Анализ предложенных ситуаций и выявление признаков интернет-угрозы (овершаринг, скулшутинг и др.)

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	Проанализировать профили несовершеннолетних (разработанных на основе реальных данных и ситуаций), выявить подозрительные признаки и отнести выявленные признаки к одной из социальных угроз Критерии анализа: <ul style="list-style-type: none">• визуальные образы• текстовая информация• сообщества, подписки, друзья Определить тип информационной угрозы в отношении несовершеннолетнего Предположить возможные предпосылки вовлечения несовершеннолетнего в опасные сообщества/деятельность. Проверить правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ответы на задание сообщить преподавателю или разместить в группе поддержки курса в Telegram
Критерии оценивания	Опасные признаки выявлены. Тип угрозы определен. Ответ размещен в группе поддержки курса в Telegram
Оценка	Зачет / Незачет Зачет выставляется при условии выполнения всех критериев

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1

балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Какие рекомендации по информационной безопасности педагогу целесообразно дать родителям (законным представителям) детей 9-12 лет? (выбор одного правильного ответа):

- 5) регулярно разговаривайте с ребенком о том, что происходит в его «онлайн-жизни»
- 6) установите систему «Родительского контроля» на устройствах, с которых ребенок будет выходить в Интернет
- 7) установите программу-шпион на устройствах ребенка для скрытого наблюдения за его действиями в интернете
- 8) запретите ребенку иметь аккаунты в социальных сетях

В ответ на какое увлечение учеников в классе педагогу следует отреагировать настороженно и провести мониторинг социальных сетей с целью выяснить, нет ли среди учащихся класса тех, кто увлечен сообществами по теме «Колумбайн»? (выбор одного правильного ответа):

- 5) предпочтение в одежде длинных темных плащей;
- 6) предпочтение одежды с символикой акул и касаток;
- 7) появление значков Columbian;
- 8) предпочтение играть в онлайн-игре на стороне террористов.

Модуль 2. Технологические угрозы сети Интернет

Практическая работа № 2. Алгоритм обеспечения максимальной защиты персональных устройств.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	Проанализируйте установки своего смартфона/ компьютера по подключению к Wi-fi сетям Установите наиболее безопасные опции подключения Выясните, каким антивирусным ПО вы пользуетесь. Настройте брандмауэр и встроенный антивирус.
---------------------	---

	<p>Изучите историю браузера в своем устройстве (смартфоне или ПК). Почистите историю поисковых запросов и куки</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Выполнены все этапы работы: настроено безопасное подключение к Wi-fi, очищены куки и история браузера</p> <p>Отчет о выполнении задания размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Как защититься ото всех технологических угроз сети Интернет? (выбор одного правильного ответа):

- 1) Установить на все свои устройства комплексные системы защиты с антивирусом, спам-фильтром, сканером трафика, брандмауэром и выставить все установки в режим максимально возможной защиты
- 2) Достаточно поставить антивирус и соблюдать правила цифровой гигиены
- 3) Единственный способ защититься ото всех угроз сети Интернет – никогда не подключаться к сети Интернет. Других гарантированных способов не существует
- 4) Выходить в интернет из внутренних корпоративных сетей – тогда между пользователем и злоумышленниками стоит как минимум IT персонал интранета

Произошла утечка персональных данных: в интернет попала база с фамилиями и номерами телефонов учащихся. В течение дня ученики получают оскорбительные сообщения и ссылку на «архив с твоими грязными фотографиями». Каковы правильные действия учителя в этой ситуации? (выбор одного правильного ответа):

- 1) Самостоятельно проверить архив с фотографиями на предмет опасного для детей и\или запрещенного контента, обратиться в полицию.
- 2) Издать приказ по учебному заведению с запретом переходить по ссылке из сообщения.
- 3) Написать в Роскомнадзор с требованием провести проверку информации, размещенной по ссылке и заблокировать ресурс в случае выявления нарушений.
- 4) Провести классный час на тему «Азбука защиты от фишинга в сети интернет», рассказать, что чрезвычайно опасно переходить по ссылкам из непрошенных писем.

Модуль 3. Психологические и техно-психологические угрозы сети Интернет

Практическая работа № 3. Определение безопасного ресурса среди представленных фишинговых электронных писем и сайтов.

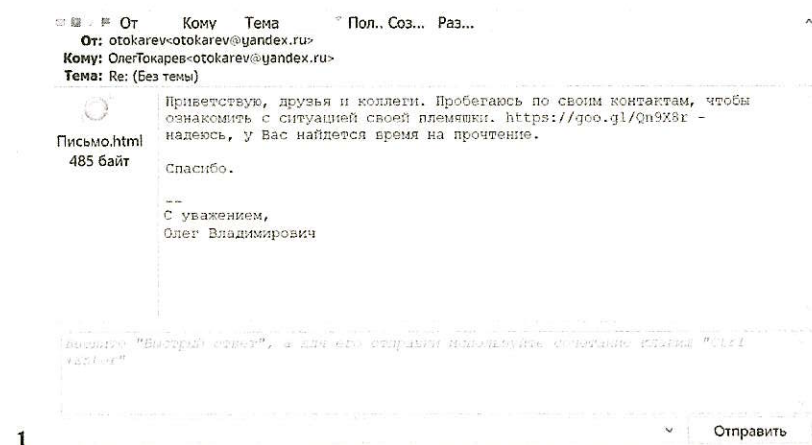
Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	<p>Проанализируйте предложенные скриншоты с ресурсами (сайты, электронные сообщения, и пр.); Изучите скриншоты, основываясь на материалах лекций и материалах в цифровой среде, выясните, какие из предложенных ресурсов безопасны</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Безопасный ресурс отобран</p> <p>Названы причины, по которым остальные ресурсы представляются опасными.</p> <p>Отчет о выполнении задания размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Выберите из четырех предлагаемых скриншотов те, которые, на ваш взгляд небезопасны. (выбор всех правильных ответов):



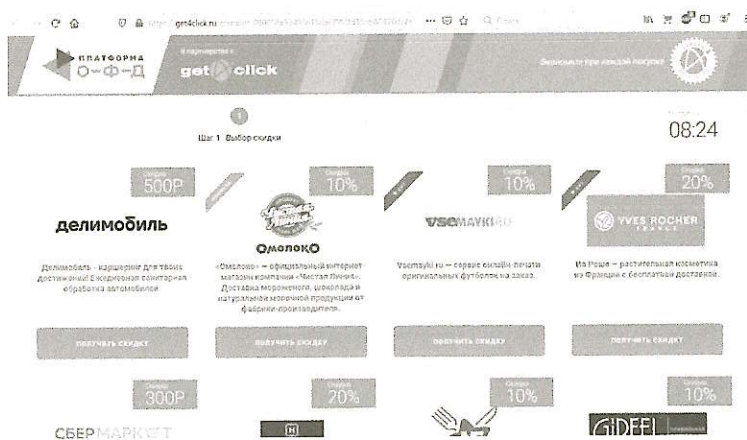
1.



2.



3.



4.

Выберите лишний элемент среди этапов формирования аддикции к онлайн-играм (выбор одного правильного ответа):

- 1) время, проведенное в игре, увеличивается
- 2) появляются новые интересы, связанные с игрой (фэнтези, аниме, военная техника и т.п.)
- 3) игровая активность формирует новые особенности поведения
- 4) ухудшение эмоционального самочувствия вне игровой активности

Модуль 4. Социально-технологические угрозы сети Интернет

Практическая работа № 4. Формирование собственных сценариев противодействия возникшему кибербуллингу с позиций ключевых социальных ролей участников.

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

<p>Алгоритм выполнения</p>	<p>Классифицировать предложенные решения ситуаций с кибербуллингом с точки зрения четырех основных социальных ролей: жертва, одноклассники, родители, классный руководитель</p> <p>Сформировать собственный сценарий противодействия кибербуллингу.</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Отчет о выполнении задания сообщите преподавателю или разместите в группе поддержки курса в Telegram</p>
<p>Критерии оценивания</p>	<p>Все предложенные решения классифицированы в соответствии с одной из социальных ролей.</p>

	Отчет о выполнении задания размещен в группе поддержки курса в Telegram
Оценка	Зачет / Незачет Зачет выставляется при условии выполнения всех критериев

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

Примеры тестовых заданий.

Учитель получил сообщение о том, что кто-то из одиннадцатиклассников, используя школьный компьютер, посещал Darknet. Какие действия помогут педагогу выяснить, кто это был? (выбор одного правильного ответа):

- 1) проанализировать страницы социальных сетей наименее успевающих учеников параллели и найти из них подписчика на сервис Darknet (покупка невозможна без подписки)
- 2) зайти на Darknet.com не позднее двух недель после предполагаемой покупки и выяснить логин пользователя, поочередно запуская ping всех IP-адресов школьных компьютеров; затем выяснить, кто работал за данным компьютером
- 3) определить, на каком школьном компьютере остался анонимный браузер Tor; затем выяснить, кто работал за данным компьютером
- 4) собрать старшеклассников и постараться выяснить данную информацию во время беседы с ними

Какой признак с огромной вероятностью свидетельствует о том, что ребенок покупает наркотики в сети Darknet (выбор одного правильного ответа):

- 1) Использует символику растафарианства, выступает за легализацию марихуаны, слушает раста-рэпы с текстами про марихуану
- 2) У него в пенале были найдены неизвестные таблетки, которые оказались сильными антидепрессантами
- 3) Из его кармана выпал маленький предмет, похожий на комок изоленты, который он очень быстро поднял и спрятал обратно
- 4) На его руке браслет из большого количества маленьких разноразмерных магнитов

Модуль 5. Социально-психологические угрозы сети Интернет

Практическая работа № 5. Определение типа информационной угрозы на основе проанализированных материалов (экстремизм, группы смерти, АУЕ*).

Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде. Ссылку на выполненную работу или скриншот размещают в группу поддержки курса в Telegram.

Алгоритм выполнения	<p>Проанализировать профили несовершеннолетних (разработанных на основе реальных практик и кейсов), выявить подозрительные признаки и отнести выявленные признаки к одной из социальных угроз</p> <p>Критерии анализа:</p> <ul style="list-style-type: none"> • визуальные образы • текстовая информация • сообщества, подписки, друзья <p>Определить тип информационной угрозы в отношении несовершеннолетнего</p> <p>Предположить возможные предпосылки вовлечения несовершеннолетнего в опасные сообщества/деятельность.</p> <p>Проверьте правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.</p> <p>Ответы на задание сообщить преподавателю или разместить в группе поддержки курса в Telegram</p>
Критерии оценивания	<p>Опасные признаки выявлены.</p> <p>Тип угрозы определен.</p> <p>Ответ размещен в группе поддержки курса в Telegram</p>
Оценка	<p>Зачет / Незачет</p> <p>Зачет выставляется при условии выполнения всех критериев</p>

Освоение раздела завершается тестированием. Тест включает 5 вопросов. Количество попыток не ограничено. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 80% заданий, соответственно набрано не менее 4 баллов.

* Запрещена на территории РФ

Примеры тестовых заданий.

Родители одного из учеников сообщают, что готовы написать заявление в полицию на другого ученика, который вымогает у их сына деньги "на общак" и совершает мелкие кражи. Какое действие педагога будет наиболее эффективным? (выбор одного правильного ответа):

- 1) Воспитательная беседа с учеником в присутствии его родителей.
- 2) Организация контакта соц.педагога с семьей учащегося в связи с вероятностью вовлечения ребенка в криминальное сообщество, а также информирование директора школы о необходимости обратиться в полицию в связи с субкультурно-обусловленным преступлением.
- 3) Классный час на тему "Блатная жизнь: мифы и реальность" с участием представителя ФСИН
- 4) Самостоятельное обращение в полицию для постановки ученика на учет.

Ученики заметили, что одна из учениц получает сообщения от своего друга из интернета по имени «Теплый мишка». Никто из одноклассников не знаком с ним в реальной жизни, сама ученица на вопросы о нём отвечать отказывается. Какое действие педагога в этой ситуации будет наиболее адекватным ситуации? (выбор одного правильного ответа):

- 1) Это — педофил, нужно запретить ученице использование средств связи во время учебного процесса, ограничить использование средств связи во время пребывания на территории школы.
- 2) Попытаться выяснить личность "друга" самостоятельно или через заявление в полицию.
- 3) Поговорить с родителями ученицы о социальных угрозах сети Интернет, рассказать о груминге и опасности сетевой педофилии и сообщить о факте соц.педагогу или школьному психологу
- 4) Провести классный час и вынести на обсуждение эту историю, чтобы дружба с "теплым мишкой" стала для ученицы неприглядным фактором

Итоговая аттестация.

Итоговая аттестация проводится в форме зачета. Зачет выставляется при условии выполнения всех предусмотренных программой практических работ, тестов и итогового тестирования.

Время выполнения – 2 ч. Количество попыток – 2.

Тест включает 15 заданий на владение основами информационной безопасности детей. Каждый верный ответ оценивается в 1 балл. Тестирование пройдено успешно, если правильно выполнено не менее 60% заданий, соответственно набрано не менее 9 баллов.

Пример задания итогового тестирования.

Педагог ищет информацию для проведения занятия с детьми. На одном из сайтов он находит список ссылок по нужной теме. Какой из предложенных адресов следует считать наиболее безопасным? (выбор одного правильного ответа):

Что из перечисленного НЕ является формой опасного досуга?

- 1) Руфинг
- 2) Диггерство
- 3) Стендовая стрельба
- 4) Зацепинг

Какие приоритетные задачи устанавливает Концепция информационной безопасности детей для семьи, государства и организаций, заинтересованных в обеспечении информационной безопасности детей? (выбор всех правильных ответов):

- 1) повышение уровня медиаграмотности детей
- 2) усвоение детьми системы семейных ценностей
- 3) формирование у детей навыков по выбору правильного образовательного профиля
- 4) сохранение конфиденциальности документированной информации

Примеры интерактивных заданий (выполняются обучающимися на интерактивных занятиях, размещаются в цифровой среде курса)

1.	Соотнесение предложенных кейсов с компетенциями органов государственной власти и организаций, задействованных в процессе обеспечения информационной безопасности детей.
2.	Умение выявлять опасные и безопасные ресурсы среди представленных сайтов: поддельные электронные письма и веб-страницы.
3.	Выполнение ситуативных заданий по безопасному использованию публичных сетей wi-fi, электронной почты, безопасному поиску в сети и скачиванию файлов, противодействию фишингу.
4.	Определение мер противодействия распространённым ошибкам, приводящим к уязвимости для кибератак
5.	Определение типа информационных угроз в отношении несовершеннолетнего на основе анализа предложенных ситуаций: скулшутинг, ARG, груминг, АУЕ*
6.	Анализ предложенных ситуаций и выявление признаков социальной информационной угрозы «Школьная стрельба (Скулшутинг)».

* Запрещена на территории РФ

7.	Анализ предложенных ситуаций и выявление признаков социально-психологической информационной угрозы «Деструктивные ARG».
8.	Определение технологии, методики и инструментов превентивной работы с актуальными информационными угрозами, доступные руководителям образовательных учреждений, педагогам, родителям и несовершеннолетним.
9.	Анализ предложенных ситуаций и выявление признаков техно-социальной информационной угрозы «Кибербуллинг».
10.	Определение типа информационных угроз на основе анализа предложенных ситуаций в отношении несовершеннолетнего: кибербуллинг.
11.	Определение с точки зрения четырех ролей: классный руководитель, родители, жертва, одноклассники верной и неверной линии поведения в ситуации возникновения кибербуллинга.
12.	Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры
13.	Игровая зависимость и зависимость от азартных онлайн-игр: умение распознавать признаки аддиктивного поведения ребенка в отношении онлайн-игр.
14.	Анализ предложенных ситуаций и выявление признаков социально-психологической информационной угрозы «Груминг»
15.	Анализ предложенных кейсов и выявление признаков социально-психологической информационной угрозы «АУЕ*»
16.	Определение типа информационной угрозы в отношении несовершеннолетнего на основе анализа предложенных ситуаций: «Овершаринг»
17.	Анализ поведенческих признаков употребления психоактивных веществ. Обучающиеся анализируют видеоматериал, фиксируют опасные признаки и предлагают возможную стратегию поведения с человеком
18.	Анализ диалогов школьников. Обучающиеся анализируют диалоги школьников, определяют, о чем идет речь в каждом диалоге, идентифицируют «безопасный» диалог, фиксируют слова-маркеры
19.	Сортировка фраз по 3 группам. Обучающиеся анализируют фразы, определяют, о чем идет речь в каждой фразе, далее группируют фразы по тематическим группам
20.	Признаки употребления ребенком психоактивных веществ. Обучающиеся анализируют фотоматериалы, фиксируют верные варианты и нажимают на кнопку окончания выполнения упражнения

* Запрещена на территории РФ

21.	Профилактика и противодействие угрозам, представленным в видеороликах. Обучающиеся анализируют видеоролики, фиксируют опасные признаки и предлагают 5 наиболее важных управленческих решений по профилактике и противодействию предложенным кейсам
-----	--

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Нормативные документы:

1. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", (дата обращения 21.09.2021).
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".
3. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 31.07.2020) "Об образовании в Российской Федерации", (дата обращения 21.09.2021).
4. Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 "Об утверждении санитарных правил СП 2.4. 3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи".
5. Методические рекомендации по ограничению в образовательных организациях доступа, обучающихся к видам информации.
6. Концепция информационной безопасности детей, утвержденной распоряжением Правительства РФ от 02.12.2015 N 2471. (дата обращения 21.09.2021).
7. Распоряжение Правительства РФ от 02.12.2015 N 2471-р "Об утверждении Концепции информационной безопасности детей" (дата обращения 21.09.2021).
8. 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/ (дата обращения 21.09.2021)

Список основной литературы

1. Бирюков А.А. Информационная безопасность: защита и нападение. Москва: ДМК-Пресс, 2017.
2. 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.
3. Международная информационная безопасность: Теория и практика: В трех томах: Учебник для вузов / Под общ. ред. А.В.Крутских. — М.: Издательство «Аспект Пресс», 2019.
4. Малюк А.А. Глобальная культура кибербезопасности // Горячая линия - Телеком. М., 2017. С. 308.

Список дополнительной литературы

1. 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.
2. С. А. Петренко, В. А. Курбатов. Политики безопасности компании при работе в Интернет. Москва: ДМК-Пресс, 2016

Интернет-ресурсы

1. Курс «Безопасность в интернете» от Яндекса (дата обращения 21.09.2021)
2. Журнал для педагогов, психологов и родителей «Дети в информационном обществе» (дата обращения 21.09.2021)

3. 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)
4. «Урок полезного и безопасного Интернета» от компании МТС. <http://detionline.com/mts/lessons> (дата обращения 21.09.2021)
5. Защита детей. Лаборатория Касперского <https://kids.kaspersky.ru/>
6. 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 21.09.2021)

4.2. Материально-технические условия реализации программы

1. Компьютер у каждого обучающегося.
2. Наушники или колонки, микрофон.
3. Браузер (Яндекс).
4. Доступ в Интернет.
5. Учебные материалы, размещенные в цифровой среде образовательной организации.

Видеозаписи занятий и все учебные материалы размещаются в информационной среде курса: <https://education.apkpro.ru/courses/294>

Информационная поддержка курса осуществляется в мессенджере Telegram. Создается группа для оперативного информирования и размещения результатов практических работ.