Совершенствование компетенций педагогов в области цифровой грамотности и информационной безопасности детей в сети Интернет

Магазейщиков Евгений Александрович,
ФГАОУ ДПО «Академия Минпросвещения России»


С Международным днём безопасного Интернета

Мы не распознаём угрозы,

- Вы получали письма от отправителей, которым вы не давали свой адрес?
- Вам звонили из банка, в котором у вас нет вклада с информацией об операции по вашей карте?
- Вы знаете, что могут означать цифры 4:20 в тетради или в соцсети ребёнка?
- Приходилось ли вам в школе слышать, как дети, общаясь, используют слова «фен», «диспут» или «мяу» в странном контексте?
- Видели ли вы в соцсетях просьбу помочь деньгами от ваших знакомых?

потому что не обращаем внимания на них

Не получится досолить суп, не попробовав

Нельзя выбрать лекарство, не зная, чем болеешь

Невозможно захотеть научиться умению, о котором не знаешь

ЧП предотвратимо, когда вы знаете признаки

Информационная безопасность и ФГОС

Программа развития универсальных учебных действий

Владение основами информационной безопасности, умением безопасного использования средств информационно-коммуникационных технологий (далее - ИКТ) и сети Интернет

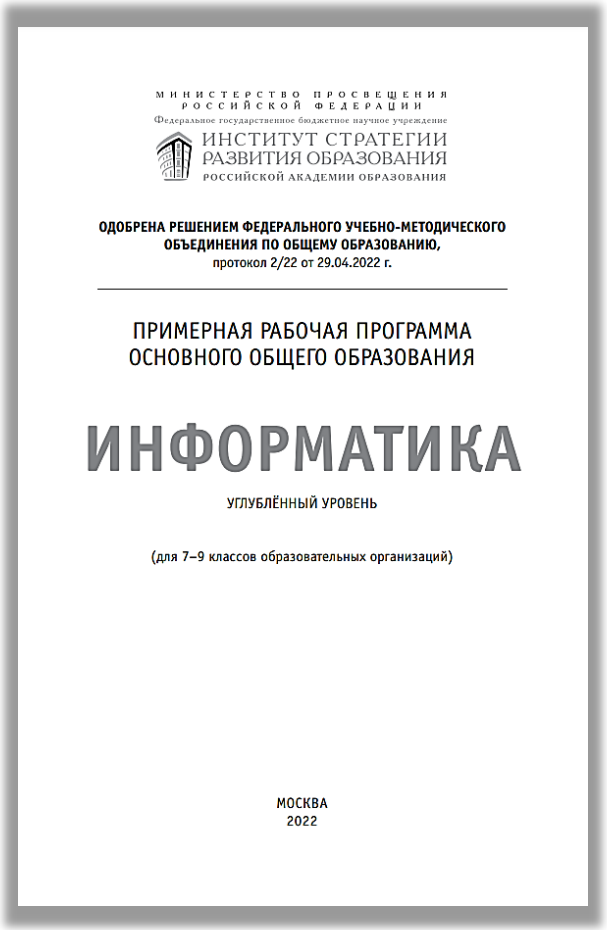
Предметные результаты изучения предметной области «Математика и информатика»

Формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в интернете, умения соблюдать нормы информационной этики и права

Программа воспитания и социализации обучающихся

Формирование и развитие знаний, установок, личностных ориентиров и норм здорового и безопасного образа жизни

Вопросы информационной безопасности в школьном курсе информатики на уровне основного общего образования



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное научное учреждение
ИНСТИТУТ СТРАТЕГИИ РАЗВИТИЯ ОБРАЗОВАНИЯ РОССИЙСКОЙ АКАДЕМИИ ОБРАЗОВАНИЯ

ОДОБРЕНА РЕШЕНИЕМ ФЕДЕРАЛЬНОГО УЧЕБНО-МЕТОДИЧЕСКОГО ОБЪЕДИНЕНИЯ ПО ОБЩЕМУ ОБРАЗОВАНИЮ,
протокол 2/22 от 29.04.2022 г.

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА
ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

ИНФОРМАТИКА

УГЛУБЛЁННЫЙ УРОВЕНЬ

(для 7–9 классов образовательных организаций)

МОСКВА
2022

Цифровая грамотность Глобальная сеть Интернет и стратегии безопасного поведения в ней (10 часов)

- Понятие об информационной безопасности
- Угрозы информационной безопасности при работе в глобальной сети и методы противодействия им
- Правила безопасной аутентификации
- Защита личной информации в сети Интернет
- Предупреждение вовлечения в деструктивные и криминальные формы сетевой активности (кибербуллинг, фишинг и пр.)

Содержание модуля «Информационная безопасность» учебного предмета «Информатика»

- Безопасность общения
- Безопасность устройств
- Безопасность информации

Документы, определяющие информационную защиту детей в сети Интернет

ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и развитию»

Перечень информации, причиняющей вред здоровью и (или) развитию детей, содержится в: Ст. 1.1, Ст. 2.1, 2.2, 2.4, 2.5, 2.6, 2.7, 2.9, Ст. 5, 6, 7, 8, 9, 10, 11.1, 11.2, 12.1-12.5, Ст. 14.1

Концепция информационной безопасности детей, утвержденная правительством РФ

Задачи, которые обозначило Правительство РФ в области информационной защиты детей, содержатся в I,II, III, IV, V разделах

ФЗ РФ «Об образовании в Российской Федерации»

Информация о документах, регулирующих правовые отношения в сфере образования, а также об обязанности образовательной организации создавать безопасные условия обучения учащихся, содержится в: Ст. 4 п. 1, 2, 3.1, Ст. 28 п. 6.2, Ст. 41 п. 1.8, 2, 4.3, Ст. 48 п. 1.4

Опасная информация:

- допускающая насилие и жестокость, вызывающая страх, ужас, панику
- представляющая угрозу жизни и здоровью
- побуждающая детей к самоубийству
- оправдывающая противоправное поведение
- отрицающая семейные ценности, формирующая неуважение к родителям
- вызывающая желание употребить наркотические средства, ПАВ
- пропагандирующая азартные игры
- побуждающая к проституции, содержащая информацию порнографического характера
- пропагандирующая нетрадиционные сексуальные отношения

Защита детей в сети Интернет

Вопрос национальной безопасности

Несмотря на то что этой задаче уделяется все больше внимания на самом высоком уровне, есть объективные проблемы:

Незнание – слабость

Педагоги практически не имеют представления об основных угрозах, с которыми дети могут столкнуться в сети Интернет

Низкая эффективность существующих инструментов

Отсутствует системность и полнота методических пособий и инструкций. Подача материала не предполагает понимание проблемы

Как быть?

Для эффективной профилактики и противодействия основным угрозам в сети Интернет дети и педагоги должны находиться в одном смысловом поле

1. Курс ПК

Информационная безопасность детей: Социальные и технологические аспекты

Программа разработана при участии профильных ведомств

Минцифры России

МВД России

Роскомнадзор

ФСБ России

- охватывает широкий спектр актуальных онлайн-угроз, каждый сегмент снабжён подробным описанием и практическими рекомендациями
- задействованы современные инструменты обучения и обратной связи, знания закрепляются выполнением заданий при помощи специальных образовательных сервисов
- предусмотрено использование современных технологий, способствующих эффективному обучению взрослых

ИНТЕРНЕТ-АГРЕССИЯ

Колумбайн*

Речевые и поведенческие индикаторы, свидетельствующие о намерении устроить «школьную стрельбу». Особенности ведения соцсетей и онлайн-коммуникации

Кибербуллинг

Групповая травля с использованием сети Интернет. Специфика явления, отличие от офлайн-буллинга. Фактор наблюдателя

Субкультура АУЕ*

Особенности распространения идеологии и специфика функционирования субкультуры онлайн в условиях законодательного запрета

Груминг

Сетевые педофилы: методики и способы «обработки» детей. Индикаторы, делающие возможным выявление нездорового интереса к ребенку, специфика мониторинга и предупреждения опасных ситуаций

*Запрещены на территории РФ

ИНТЕРНЕТ-ИСТЕРИЯ

Рискованное поведение

Неадекватная оценка рисков как особенность пубертатного периода. Специфика и возможные способы канализирования и сублимации этой особенности

Суицидальное поведение

Возрастные, психологические и социально обусловленные факторы возникновения суицидальных мыслей, намерений и действий

Флешмобы, челленджи

Феномен спонтанной самоорганизации. Опасные интернет-тренды. Специфика профилактики вовлечения в интернет-истерию

Игры формата ARG

Деструктивные ARG. «Группы смерти» и их администраторы. Эволюция и технологические аспекты деструктивных игротехник

ЗАКРЫТЫЕ СООБЩЕСТВА

Экстремизм

Признаки вовлечения школьника в запрещенные организации сообщества. Тонкости и подводные камни при выявлении признаков угрозы. Эффективная профилактика

Религиозные секты

Христианские ортодоксальные секты, исламские фундаменталисты, ячейки радикальных суннитских джамаатов в РФ и СНГ. Тоталитарно-деструктивные, и коммерческие секты. Эстетические и контркультурные религиозные группы (сатанисты, рериховцы, растафарианцы и т.п.)

Диггерство и зацепинг

Гендерная и возрастная специфика этих видов опасного досуга. Статистика и место в правовом поле. Признаки вовлечения и способы противодействия

Руфинг и роупджампинг

Гендерная и возрастная специфика этих видов опасного досуга. Статистика и место в правовом поле. Признаки вовлечения и способы противодействия

ТЕХНОПСИХОЛОГИ И ПСИХОТЕХНИКИ

Социальная инженерия

Социальная психология на службе интернет-мошенников. Методы манипуляций, при помощи социальных импринтов, отвлечение и рассеивание внимания как инструмент преступника

Вредоносное ПО

Виды вредоносных программ, особенности и специфика их распространения и воздействия на устройства. Организация защиты от вредоносного ПО

Фишинг и его разновидности

Похищение денег с банковских кар и счетов, компрометация учетных данных, её последствия, кража конфиденциального и ценного контента посредством фишинговой атаки жертвы

Скам, псевдо-благотворительность

Интернет-преступления, предполагающие массовость. Технический минимализм. Преступления, эксплуатирующие сочувствие, сопереживание и доброту

ТЁМНАЯ СТОРОНА СЕТИ

Даркнет

«Изнанка» интернета. Криптосети и алгоритм луковой маршрутизации. Скорость распространения и рост охвата пользователей – в мире, в России, среди школьников и студентов. Почему Darknet не получится просто отключить

Наркоторговля в Даркнет

Эволюция криминального рынка по продаже ПАВ. Форумы, ставшие гипермаркетами, и участники, открывшие там магазины. Сложность противодействия. Вовлечение подростков в уголовно-наказуемый бизнес: признаки, способы профилактики

Употребление ПАВ

Смена парадигмы наркопотребления как результат технической революции наркобизнеса. Полинаркомания в школе. Новая атрибутика и символика. Специфика выбора, доставки и потребления ПАВ. Признаки вовлечённости подростка в среду наркопотребителей

Распространение ПАВ

Сравнение употребления наркотиков в мире и в России. Региональная специфика распространенности тех или иных веществ. Скрытая и явная пропаганда наркотиков в современной молодёжной культуре

МЕРЫ ПРОФИЛАКТИКИ

Сетевая гигиена

Базовые правила безопасности. Их применение в образовательной организации. Способы и инструменты защиты учетных данных. Цифровые следы – потенциальная опасность

Феномен сталкеринга

Интернет-профайлинг. Причины и цели навязчивого наблюдения за жертвой в соцсетях, онлайн-преследование

Овершеринг

Современные тренды и взаимосвязи между открытым доступом к персональным данным и возможными угрозами жизни

Онлайн-игровая зависимость

Правовой и медицинский статус явления. Причины и признаки появления зависимости – общественные, социальные, культурные. Формирование аддиктивности как ключевой маркетинговый фактор при разработке онлайн-игр

2. Материалы

Методическая поддержка педагогов после обучения (образовательный контент)

Минцифры России

МВД России

ФСБ России

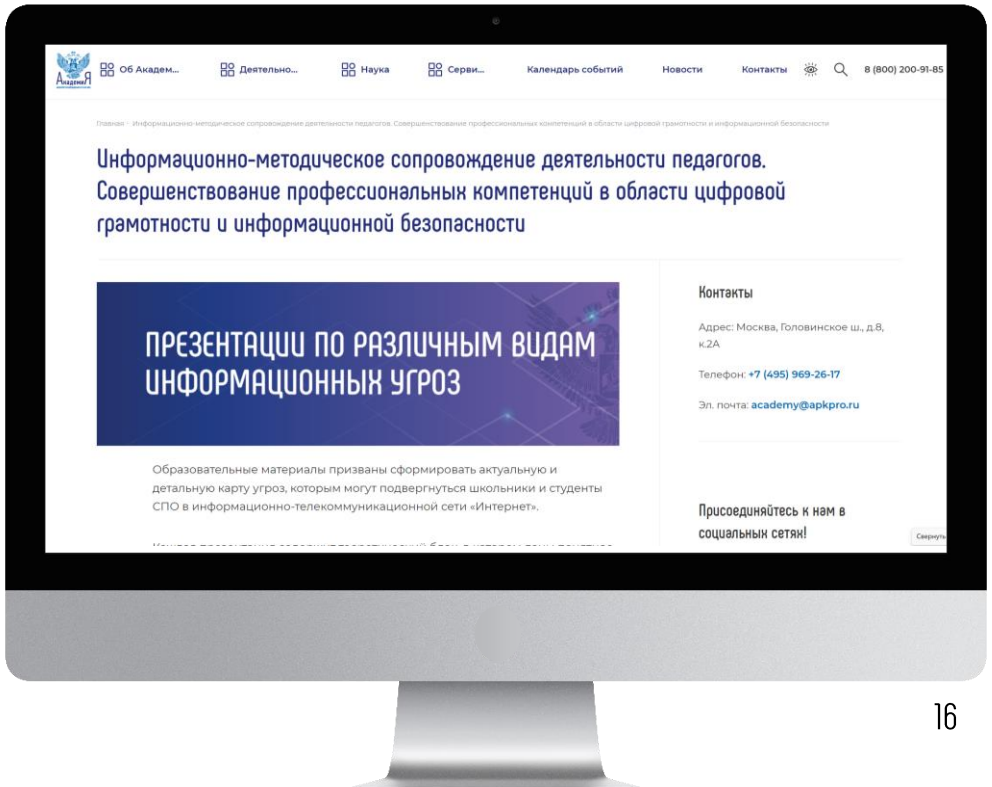
Роскомнадзор

Воронежский государственный медицинский университет имени Н.Н. Бурденко

Изменения в мире IT стремительны. Необходимы механизмы оперативного информирования и актуализации знаний педагогов

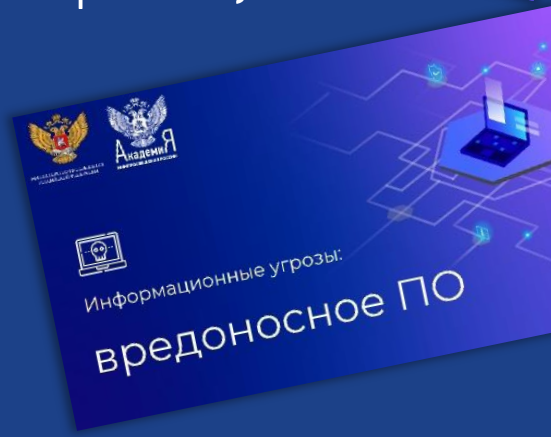
Раздел на сайте Академии: «Информационно-методическое сопровождение деятельности педагогов. Совершенствование профессиональных компетенций в области цифровой грамотности и информационной безопасности»

1. Презентации по различным видам информационных угроз
2. Обучающий раздаточный материал по распознаванию и профилактике информационных угроз
3. Информационно-обучающие видеоролики
4. Практикоориентированные кейсы и сценарии для организации обучения в игровой форме



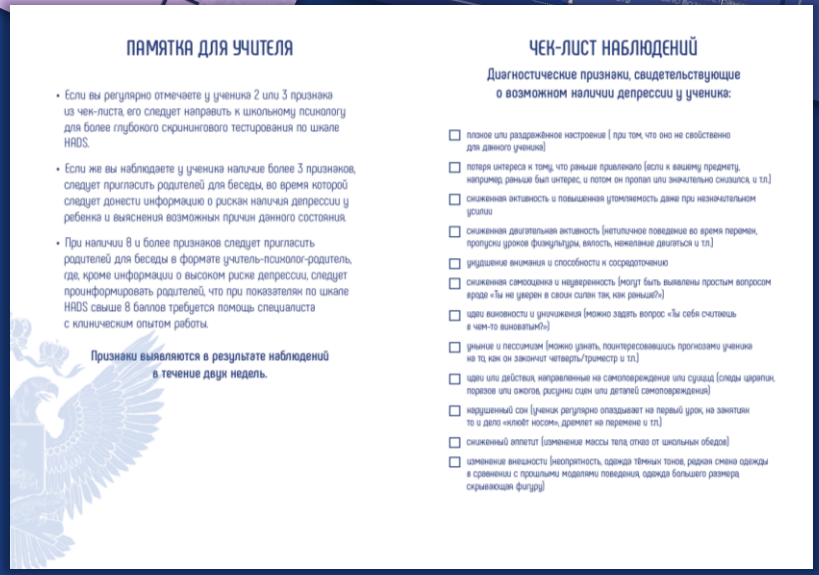
1 Презентации по различным видам информационных угроз

- Кибербуллинг
- Скулшутинг
- Суицидальные сообщества
- Интернет-истерия, рискованное поведение
- Фишинг
- Овершеринг
- АУЕ* (запрещено на территории РФ)
- Груминг
- Вредоносное ПО
- Экстремизм
- Наркоторговля в сети Даркнет



2 Обучающий раздаточный материал по распознаванию и профилактике информационных угроз

- Плакаты
- Настольный календарь
- Карточки для телеграм канала
- Справочники
- Брошюры
- Чек-листы



ПАМЯТКА ДЛЯ УЧИТЕЛЯ

- Если вы регулярно отмечаете у ученика 2 или 3 признака из чек-листа, его следует направить к школьному психологу для более глубокого скринингового тестирования по шкале HADS.
- Если же вы наблюдаете у ученика наличие более 3 признаков, следует пригласить родителей для беседы, во время которой следует донести информацию о рисках наличия депрессии у ребенка и выяснения возможных причин данного состояния.
- При наличии 8 и более признаков следует пригласить родителей для беседы в формате учитель-психолог-родитель, где, кроме информации о высоком риске депрессии, следует проинформировать родителей, что при показателях по шкале HADS свыше 8 баллов требуется помощь специалиста с клиническим опытом работы.

Признаки выявляются в результате наблюдений в течение двух недель.

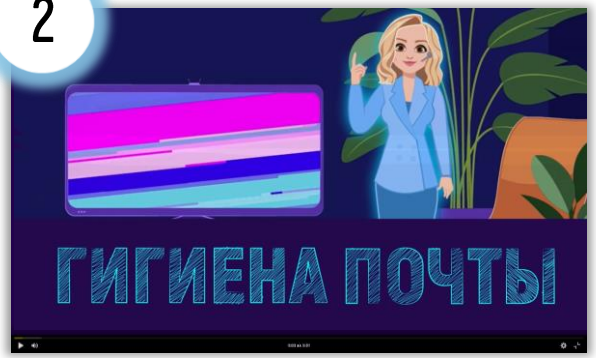
ЧЕК-ЛИСТ НАБЛЮДЕНИЙ

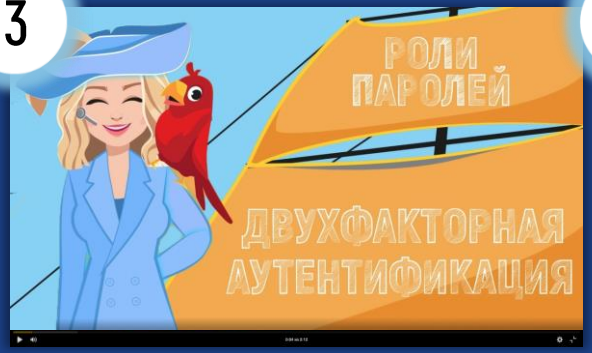
Диагностические признаки, свидетельствующие о возможном наличии депрессии у ученика:

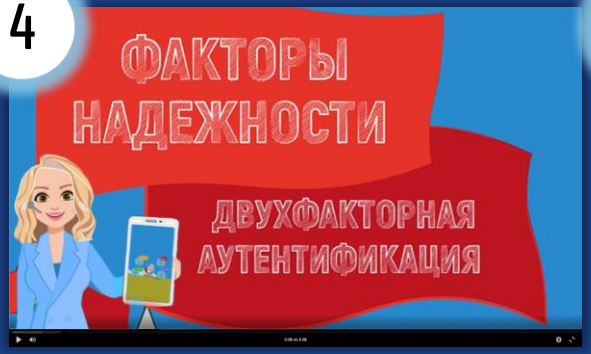
- ☐ плохое или раздражённое настроение (при том, что оно не свойственно для данного ученика)
- ☐ потеря интереса к тому, что раньше привлекало (если к вашему предмету, например, раньше был интерес, и потом он пропал или значительно снизился, и т.п.)
- ☐ сниженная активность и повышенная утомляемость даже при незначительном усилии
- ☐ сниженная двигательная активность (нетипичное поведение во время перемен, пропуски уроков физкультуры, вялость, нежелание двигаться и т.п.)
- ☐ ухудшение внимания и способности к сосредоточению
- ☐ сниженная самооценка и неуверенность (могут быть выявлены простым вопросом вроде «Ты не уверен в своих силах так, как раньше?»)
- ☐ идеи виновности и уничижения (можно задать вопрос «Ты себя считаешь в чем-то виноватым?»)
- ☐ уныние и пессимизм (можно узнать, поинтересовавшись прогнозами ученика на то, как он закончит четверть/триместр и т.п.)
- ☐ идеи или действия, направленные на самоповреждение или суицид (следы царапин, порезов или ожогов, рисунки сцен или деталей самоповреждения)
- ☐ нарушенный сон (ученик регулярно опаздывает на первый урок, на занятиях то и дело «клюёт носом», дремлет на перемене и т.п.)
- ☐ сниженный аппетит (изменение массы тела, отказ от школьных обедов)
- ☐ изменение внешности (неопрятность, одежда тёмных тонов, редкая смена одежды в сравнении с прошлыми моделями поведения, одежда большего размера, скрывающая фигуру)

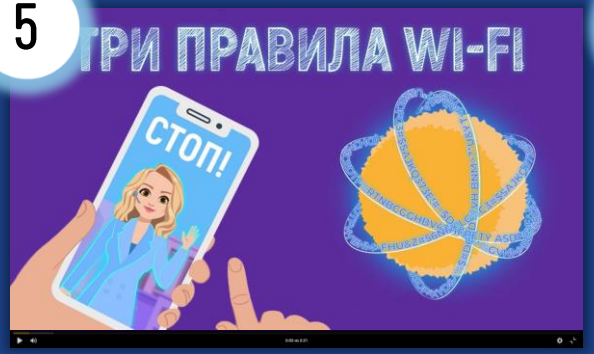
3 Информационно-обучающие видеоролики

1


2


3


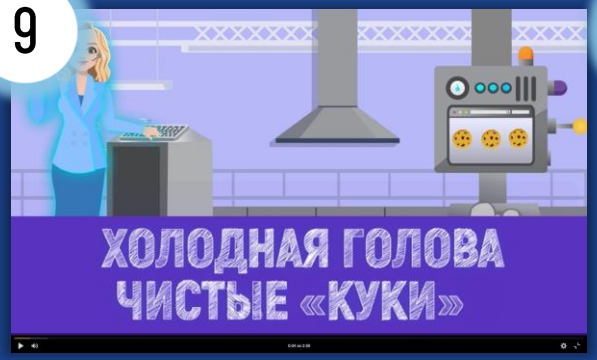
4


5


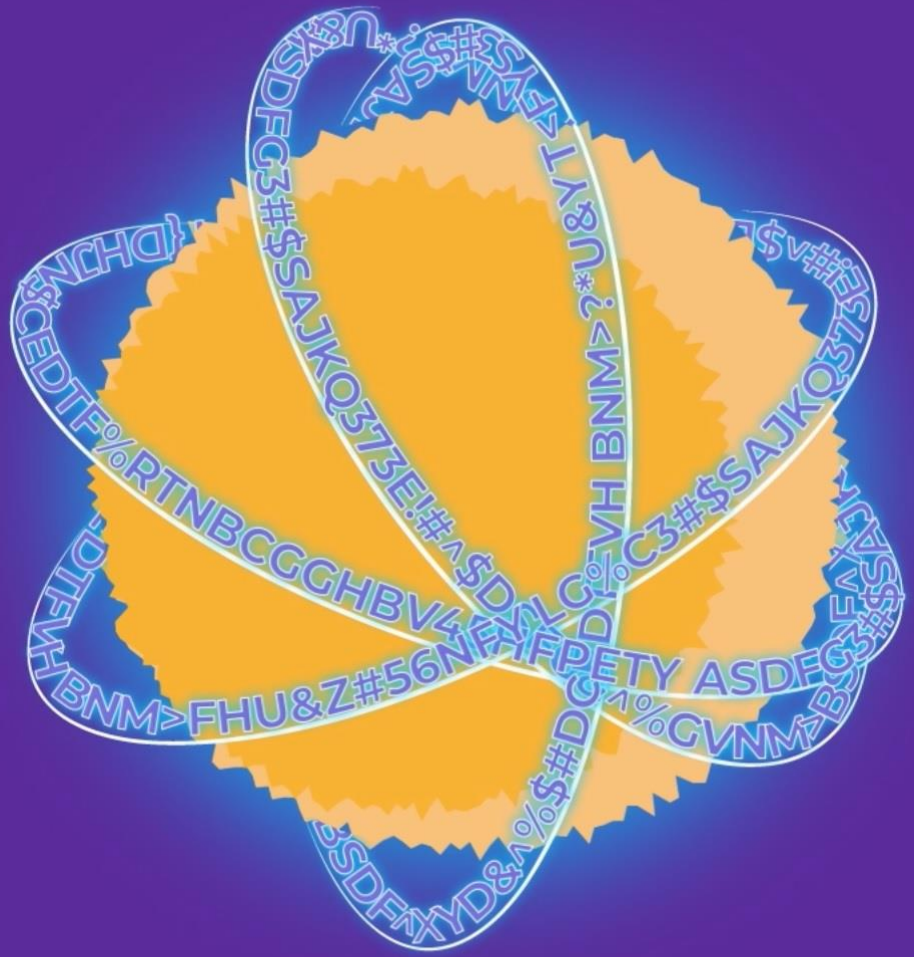
6


7


8


9


10

ТРИ ПРАВИЛА WI-FI

4 Практикоориентированные кейсы и сценарии для организации обучения в игровой форме

Практикоориентированные кейсы - это реальные ситуации столкновения детей и подростков с современными информационными угрозами, происходившими в образовательных организациях. **Для реализации игровых сценариев используются:**

- Любые четыре комплекта практикоориентированных кейсов **«Угрозы»** (всего 48 карточек)
- Любые четыре комплекта практикоориентированных кейсов **«Контрмеры»** (всего 48 карточек)
- **Новые кейсы** для существующих наборов, а также **новые тематические наборы** кейсов, распространяются через сайт проекта и скачиваются пользователями

3. Дидактическая игра

Методическая поддержка педагогов после обучения (образовательный контент)

ГОРОДСКОЙ ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ ЦЕНТР

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ

ПРАКТИКООРИЕНТИРОВАННЫЕ КЕЙСЫ И СЦЕНАРИИ ДЛЯ ОРГАНИЗАЦИИ ОБУЧЕНИЯ В ИГРОВОЙ ФОРМЕ

КЕЙСЫ И СЦЕНАРИИ ДЛЯ ОРГАНИЗАЦИИ ОБУЧЕНИЯ В ИГРОВОЙ ФОРМЕ

ЭТО НЕ ИГРА

СОВЕРШЕНСТВОВАНИЕ КОМПЕТЕНЦИЙ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ И УПРАВЛЕНЧЕСКИХ КАДРОВ В ОБЛАСТИ ЦИФРОВОЙ ГРАМОТНОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

- 2 – 16 УЧАСТНИКОВ
- 10 – 90 МИНУТ
- БОЛЕЕ 140 ЭЛЕМЕНТОВ
- 18+ ВОЗРАСТ УЧАСТНИКОВ

Дидактическая интерактивная педагогическая игра

Дидактическая

обучение распознаванию и предупреждению угроз

Интерактивная

совместная работа, принятие командных решений, игра против игры

Педагогическая

знакомство с арсеналом педагогических средств противодействия, смодели-рованные ситуационные задачи с выбором вариантов решения (кейсы)

Игра

для обучения используются игровые механики, динамики и компоненты

Реиграбельность

контрольные сценарии можно переигрывать несколько раз, и каждый раз сюжетная линия будет складываться по-новому, требуя от команды новых тактик решения ранжированных задач

высокая реиграбельность делает возможным проведение соревнований по этой игре: выучить содержание карточек и за счёт этого выиграть не получится!

Компоненты игры

- сценарии – 4 шт.
- поле-трекер – 1 шт.
- карточки классов – 16 шт.
- кейсы «Угрозы» – 48 шт.
- кейсы «Контрмеры» – 48 шт.
- блоки для контрмер – 4 шт.
- категории угроз – 4 шт.
- фишки участников – 5 шт. + 3 шт.

игровое поле формируется из игровых объектов

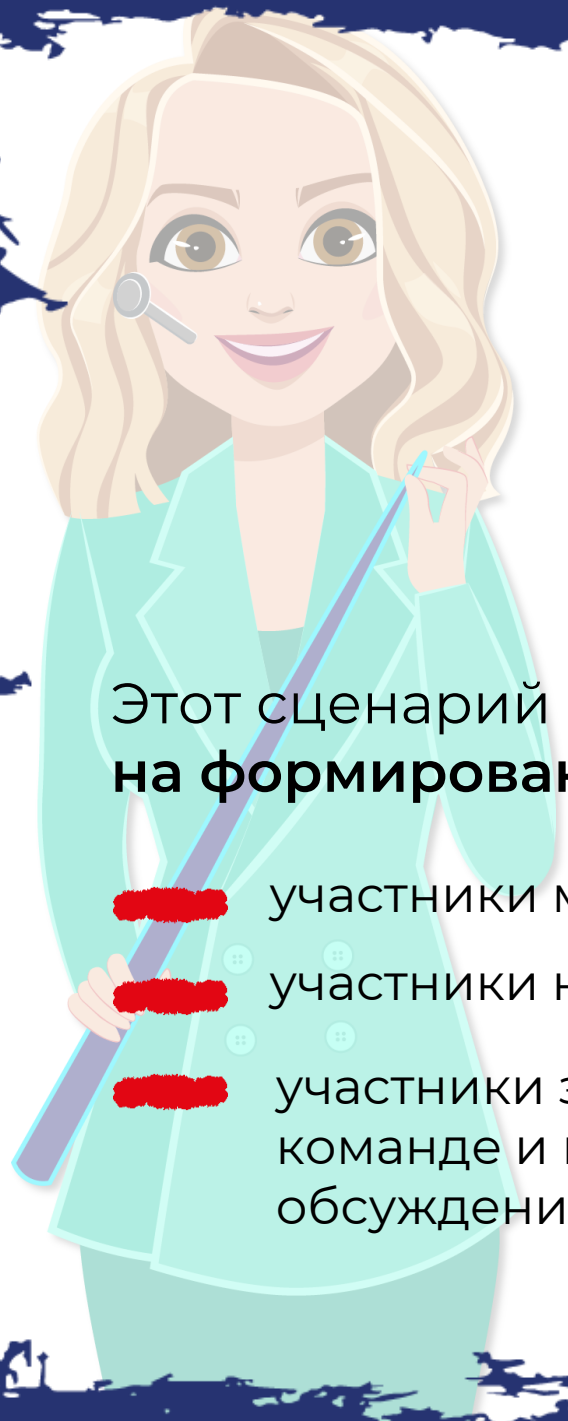
Гибкость

4 сценария: 3 – обучающих,
1 – контрольный

по нарастанию сложности

Дополнительные кейсы и новые тематические наборы кейсов на сайте проекта: «Суицидальные группы», «Опасный досуг», «Овершеринг», «Кибербуллинг, «Груминг» и пр.

Сценарий 1. Первое знакомство. (обучающий)



Цель сценария

познакомить с тематикой игры, показать существующие угрозы и научить распознавать признаки конкретных угроз

Этот сценарий **нацелен также на формирование команды** в случае, если:

- участники мало знакомы
- участники незнакомы
- участники знакомы, но не работали в одной команде и не имеют опыта совместного обсуждения и принятия решения

Сценарий 2. Биржа (обучающий)

Цель сценария

обучение участников распознаванию категорий угроз, верной оценке социальной опасности возможной угрозы и соревнование с коллегами в точности оценки

Каждый участник имеет специализацию, выраженную как **«категория угрозы»**; в ходе сценария участники по специальным правилам обмениваются кейсами угроз и стараются распознать **«свою»** угрозу. Игра окончена, когда один или несколько участников успешно распознали некоторое количество угроз по своей категории и набрали необходимое количество очков

Важно

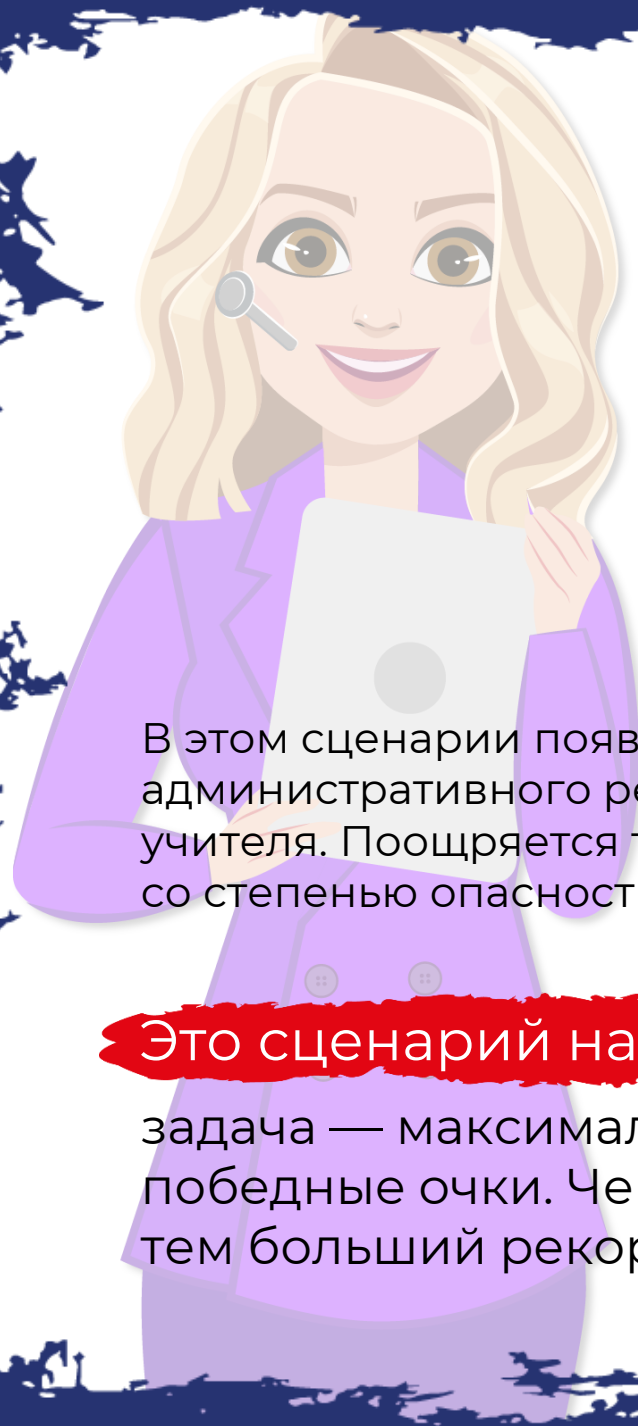
чем серьёзнее угроза, которую удалось распознать, тем больше очков получает участник. **Серьёзные ситуации легче обнаружить, но и последствия в случае беспечности также очень серьёзны**

I Интерес

II Активность

III Подготовка

IV Преступление



Сценарий 3. Профилактика (обучающий)

Цель сценария

совместными командными усилиями участники учатся выявлять и подбирать **меры профилактики угрозам**, чтобы максимально **эффективно и соразмерно** их предотвратить

В этом сценарии появляются **«карточки контрмер»** — инструментов административного реагирования, имеющихся в арсенале школьного учителя. Поощряется точное соотнесение эффективности контрмеры со степенью опасности возможной угрозы

Это сценарий на выбывание:

задача — максимально долго сопротивляться угрозам и зарабатывать победные очки. Чем дольше команда противодействует угрозам, тем больший рекорд очков она сможет установить

Сценарий 4. Школьные классы (контрольный)

Цель сценария

комплексная проверка знаний **команды участников** в области распознавания угроз и способов реагирования на них

Командный мозговой штурм. Участники могут выступить в роли специалистов по 4-м категориям угроз. Эффективность действий специалиста по своему «профилю» возрастает: в ситуации, когда угроза требует педсовета, помощи психолога, социального педагога или разработки программы поэтапного выхода из кризиса, «профильному» специалисту будет достаточно просто «поговорить с учеником», так как баллы эффективности его действий удваиваются

Игра против игры

Действие этого сценария происходит **в условной школе, состоящей из 16 «классов».** Участники совместно принимают стратегические и тактические решения с целью избавить смоделированную школу от непрерывного потока возникающих угроз. **Только командная работа, умелое планирование и владение материалом поможет участникам завершить сценарий победой!!!**

Методическая ценность

Ценность приобретенных знаний

о системе и закономерностях возникновения угроз разного вида, разной сложности и правил адекватного реагирования на них

Мозговой штурм

как метод развития коммуникативной компетенции участников и форма взаимо-действия способствует активному использованию речевых навыков, повышению культуры речи, мотивации и познавательной активности не только во время игры, но и по её окончании

Стратегия и тактика

поведения педагога, педколлектива, администрации ОУ осваиваются в процессе игры при возникновении той или иной угрозы

Лидерские качества участников

игра развивает их, так как способствует возникновению и признанию лидером того, кто глубоко владеет материалом или обладает организационными навыками по итогам прежнего игрового опыта

Главная методическая особенность дидактической интерактивной педагогической игры

взаимодействие и сотрудничество

необходимость в рамках дидактической модели прийти к совместному командному решению на основе анализа ситуационных задач, аргументированных рассуждений о возможных решениях и выводов

Курс ПК «Информационная безопасность детей: социальные и технологические аспекты»

48 часов

Старт курса

Старт обучения:
20 февраля 2023 года

Запись: по заявкам от региональных координаторов

Участники обеспечиваются учебными и контрольными материалами в Экосистеме ДПО

Работа региона

Регион может использовать полученные материалы в своей работе

Регион может организовывать мероприятия и вебинары для педагогических и управленческих команд

Регион может устроить чемпионат с использованием дидактической интерактивной игры «Это не игра»!

Результаты работы по направлениям:

- ✓ формирование системного видения угроз сети Интернет
- ✓ умение распознавать речевые и невербальные индикаторы, а также особенности сетевого поведения для выявления опасностей на ранних стадиях
- ✓ понимание особенностей профилактики сетевых угроз
- ✓ способность в случае ЧП действовать осмысленно и эффективно

Контакты для ваших вопросов:

ccto@apkpro.ru

+7 (495) 696-26-17 (доб. 7300)