Академия Минпросвещения России

# Инструктивные материалы для представителей организаций ДППО, ЦНППМ и региональных методистов по применению образовательного контента для организации работы, направленной на повышение уровня профессионального мастерства педагогических работников и управленческих кадров образовательной организации по вопросам совершенствования профессиональных компетенций в области цифровой грамотности, в том числе информационной безопасности

# Оглавление

Введение ..... 4
1. Презентации по различным видам информационных угроз ..... 8
1.1. Кибербуллинг ..... 8
1.2. Школьная стрельба ..... 9
1.3. Суицидальные сообщества ..... 10
1.4. Интернет-истерия, рискованное поведение ..... 11
1.5. Фишинг ..... 13
1.6. Овершеринг ..... 14
1.7. АУЕ (запрещено на территории России) ..... 15
1.8. Груминг ..... 16
1.9. Вредоносное ПО ..... 18
1.10. Экстремизм и секты ..... 20
1.11. Наркоторговля в сети Даркнет ..... 22
2. Раздаточные обучающие материалы ..... 23
2.1. Плакат «Кибербуллинг» ..... 23
2.2. Настольный календарь «Технологические угрозы сети Интернет» ..... 23
2.3. Плакат «Полезные номера» ..... 23
2.4. Карточки для мессенджера Телеграм «Обязанности работников в отношении персональных данных» ..... 23
2.5. Карточки для мессенджера Телеграм «Виды вредоносного ПО» ..... 24
2.6. Справочник «Внешние признаки наркотического отравления» ..... 24
2.7. Брошюра «Пояснения к практикоориентированным кейсам» ..... 24
2.8. Брошюра «Словарь сленговых и жаргонных слов и выражений» ..... 25
2.9. Чек-лист «Признаки депрессии» ..... 25
2.10. Плакаты «Напомните родителям» ..... 25
3.1. «Пароль-трансформер» ..... 26
3.2. «На крючке» ..... 26
3.3. «Роли паролей» ..... 27
3.4. «Факторы надежности» ..... 27
3.5. «Запаска для смартфона» ..... 28
3.6. «3 правила wi-fi» ..... 28

3.7. «Мишень с инициативой» ..... 29
3.8. «Гигиена почты» ..... 29
3.9. «Школа бэкапа» ..... 30
3.10. «Холодная голова, чистые куки» ..... 30
4. Раздел практикоориентированные кейсы и сценарии для организации обучения в игровой форме ..... 31

# Введение

Президент Российской Федерации в своих выступлениях неоднократно подчеркивал, что государство и общество должны объединить усилия по созданию безопасного онлайн-пространства для детей.

В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Также указанным Федеральным законом установлено, что к запрещенной для распространения среди детей относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

4) содержащая изображение или описание сексуального насилия;

5) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

6) оправдывающая противоправное поведение;

7) содержащая нецензурную брань;

8) содержащая информацию порнографического характера;

9) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Вместе с тем, по данным проекта «Дети. Mail.ru», проведенном в 2020 году среди более чем 15 тыс. пользователей, 51% детей старше 6 лет сталкивался с киберугрозами: оскорблениями и преследованиями со стороны других пользователей (12%), с материалами, демонстрирующими сцены насилия (25%), со взломом аккаунта или кражей денег с банковской карты (9%), или общением с незнакомцами, преследующими корыстные цели (5%).

Учитывая важнейшее значение информационной безопасности в воспитании детей и в целях их защиты от негативного влияния информации, распространяемой в сети «Интернет» ФГАОУ ДПО «Академия Минпросвещения России» (далее - Академия) реализует дополнительную профессиональную программу (повышение квалификации) «Информационная безопасность детей: социальные и технологические аспекты».

Целью реализации указанной Программы является совершенствование профессиональных компетенций слушателей в области информационной безопасности детей.

Для более глубокого изучения вопросов, связанных с информационной безопасностью детей в сети «Интернет», и постоянного развития педагогов по данной теме в рамках государственной работы по информационно-технологическому обеспечению управления системой образования Академия (в целях реализации мероприятий по формированию и обеспечению функционирования единой федеральной системы научно-методического сопровождения педагогических работников и управленческих кадров) на 2022 год Академия выполняет мероприятие по информационно-методическому

сопровождению деятельности педагогических работников и управленческих кадров образовательной организации по вопросам совершенствования профессиональных компетенций в области цифровой грамотности, в том числе информационной безопасности (далее – мероприятие госзадания).

В соответствии с мероприятиями госзадания Академией разработан образовательный контент, включающий:

- презентации по различным видам информационных угроз – 11 ед. (общее количество слайдов – 217 ед.);

- обучающий раздаточный материал по распознаванию и профилактике информационных угроз – 10 ед. (общий объем – 1 п.л.);

- информационно-обучающие видеоролики в технологии видеоскрайбинга – 10 ед., продолжительность каждого превышает 60 секунд;

- практикоориентированные кейсы для организации обучения в игровой форме – не менее 102 ед. (общий объем – 3,7 п.л.);

- сценарии (обучающие и контрольные) для проведения обучения в игровой форме – 4 ед.

Настоящие инструктивные материалы разработаны для представителей организаций ДППО, ЦНППМ и региональных методистов в целях применения указанного выше образовательного контента для организации работы, направленной на повышение уровня профессионального мастерства педагогических работников и управленческих кадров образовательной организации по вопросам совершенствования профессиональных компетенций в области цифровой грамотности, в том числе информационной безопасности.

Некоторые материалы образовательного контента не предназначены для детей и подростков. При изучении образовательного контента пользователям необходимо обращать внимание на возрастную маркировку и обеспечить хранение прилагаемых документов вне доступа несовершеннолетних, а также воздержаться от их распространения в общем (свободном) доступе в сети

Интернет и иных способов обнародования, предполагающих неавторизованный доступ.

Образовательный контент включает теоретические блоки и практические задания, понятное объяснение предмета изучения, историю возникновения, законодательное регулирование, маркеры, по которым можно судить о наличии угрозы, признаки вовлеченности ребенка в опасную информационную среду и степень этой вовлеченности, а также основные способы противодействия и профилактики, основанные на опыте школ, которые уже столкнулись с исследуемой угрозой.

Все примеры и практические задания взяты из актуальной педагогической практики. Профайлы в соцсетях собраны из реальных аккаунтов школьников, столкнувшихся с описываемой.

Самостоятельное изучение образовательного контента, разработанного в рамках мероприятия госзадания, призвано сформировать актуальную, подробную и детальную карту угроз, которым могут подвергнуться школьники и студенты СПО в информационно-телекоммуникационной сети «Интернет».

## 1. Презентации по различным видам информационных угроз

Каждая презентация содержит теоретический блок, в котором даны понятное объяснение предмета изучения, история возникновения, законодательное регулирование конкретного вида угрозы, маркеры, по которым можно судить о её наличии, признаки вовлеченности ребенка в опасную информационную среду и степень этой вовлеченности, а также рассматриваются некоторые способы противодействия и профилактики такой угрозы.

Также в презентации содержатся практические советы и задания, позволяющие закрепить полученные теоретические знания. Все материалы основаны на реальном опыте российских школ, которые уже столкнулись с исследуемой угрозой (получены в ходе интервью и собеседований с учителями при подготовке материалов).

Примеры и практические задания взяты из актуальной педагогической практики. Профайлы в соцсетях собраны из реальных аккаунтов школьников, столкнувшихся с описываемой в презентации угрозой.

Прилагаемые материалы предназначены для учителей-предметников, классных руководителей, школьных психологов и социальных педагогов, а также управленческих команд образовательных организаций.

### 1.1. Кибербуллинг

Проблеме школьной травли очень много лет. Школьные учителя, как правило, знают, как эффективно бороться с ней, если она уже возникла, и владеют основными инструментами и методами профилактики.

Новое время бросает новые вызовы: кибербуллинг - та же самая проблема, но не в стенах школы, а в сети Интернет, и она практически имунна к привычным способам профилактики. Методы эффективного противодействия кибербуллингу отличаются от традиционных и привычных

инструментов борьбы со школьной травлей. Они требуют владения определенными навыками из области информационных технологий. Эти навыки не требуют специального образования — они есть в арсенале любого уверенного пользователя ПК. Важно понять, общий вектор противодействия кибербуллингу, чтобы обладать достаточным уровнем ИТ-компетентности, чтобы обеспечить посильную защиту ребенка от преследования в сети Интернет со своей стороны.

Презентация «Информационные угрозы: кибербуллинг» повысит уровень информированности педагога о кибербуллинге как одной из самых распространенных и быстрорастущих угроз сети Интернет, а также познакомит с инструментами и методами противодействия кибербуллингу.

### 1.2. Школьная стрельба

Школьная стрельба, колумбайн или «скулшутинг» происходит только в реальном мире, но, безусловно относится к информационным угрозам сети Интернет. Этот факт зафиксирован на уровне государственной политики и правоприменительной практики: существующее исключительно в сети Интернет. Движение «Колумбайн», героизирующее юных террористов, и провоцирующее школьников на совершение этого преступления, в январе 2022 года было признано экстремистским и запрещено на территории Российской Федерации.

Результаты исследований психологов и криминалистов, изучающих причины и последствия школьной стрельбы, свидетельствуют о том, что в большинстве случаев трагедию можно было предотвратить — «колумбайнеры», совершившие преступление в разные годы, демонстрировали примерно одинаковый набор признаков, свидетельствующих об их криминальном намерении. Если бы уровень информированности взрослых об этом явлении был достаточно высок, преступления с некоторой долей вероятности удалось бы не допустить.

Администрации социальных сетей и популярных стриминговых платформ предпринимают определенные усилия для того, чтобы выполнять требования законодательства — они находят и удаляют сообщества, посвященные теме школьной стрельбы. Но ни они, ни правоохранительные органы, ни специальные мониторинговые организации не могут вычистить всю всемирную сеть.

Изучение презентации «Информационные угрозы: скулшутинг» позволит педагогам определить первые признаки угрозы по индикаторам и маркерам, совокупность которых может свидетельствовать о готовящейся школьной стрельбе.

### 1.3. Суицидальные сообщества

Социальные сети встроили в свои алгоритмы поиск маркеров суицидальных групп после того, как был найден и осужден создатель и куратор группы «Синий Кит». У суицидальных групп возникло большое количество последователей, в течение года после ликвидации служба поддержки сети «Вконтакте» заблокировала около 2,5 тысяч групп, имевших сходные с ним признаки. «Оранжевые совы», «Красные Лисы» и прочие клоны «Синего Кита» возникали и очень быстро блокировались службами поддержки соцсетей. Казалось, проблема решена.

Усилия администрации социальных сетей дали результат — сейчас с помощью поискового запроса не удастся найти открытые суицидальные группы. Но оказалось, что проблему это не решает.

Со стороны детей сформировался массовый запрос: в 2019 году хэштеги #хочувигру и #ищукуратора вошли в топ-100 запросов наиболее популярных соцсетей.

Потенциальные жертвы суицидальных интернет-сообществ — это как правило дети, чувствующие себя ненужными, у которых зачастую не сложились доверительные отношения в семье. Учитель, классный

руководитель способен увидеть у ученика поведенческие признаки депрессии или опознать суицидальные намерения в том числе по страничке в соцсети. Изучение презентации «Информационные угрозы: суицидальные группы» помогает разобраться в проблеме.

### 1.4. Интернет-истерия, рискованное поведение

Эксперты заявляют, что многие дети, родившиеся в эпоху интернета, воспринимают мир и своё в нем место совсем не так, как мы, и в этом есть как положительные стороны, так и отрицательные. У детей и подростков формируется острая психологическая зависимость от виртуальной поддержки - жажда лайков, которая, в свою очередь, формирует «подиумное мышление», суть которого звучит так: «событие имело место в моей жизни только в том случае, если про него написано в соцсети».

Абсолютная информационная доступность, размытие географических и культурных границ, мгновенный доступ к почти любой информации – отводит на второй план умение её искать и анализировать. По любому запросу информации будет слишком много, поэтому ключевым умением человека нового времени становится способность максимально быстро отфильтровать ненужную информацию.

Психика ребенка цифровой эпохи также становится более поверхностной и подвижной. Именно с этим фактом связан комплекс информационно-психологических угроз под общим названием «Интернет-истерия». Это явление спонтанно возникает, а потом так же необъяснимо сходит на нет.

Например, с лета 2021 года по апрель 2022 по России прокатился смертельный челлендж: дети выбрасывались из окна под песню группы ЛСП «Камнем вниз», причем происходило это всегда в совершенно конкретный момент песни. Музыканты заявили о своей непричастности, убрали песню со всех платформ и попросили радиостанции исключить её из ротации. В этом челлендже не было ни смысла, ни идеи. Это не было ни протестом, ни шагом

отчаяния — это был просто тренд в соцсетях, и единственное объяснение причины было желание популярности аккаунта — пусть посмертной, но детей это не останавливало. В общей сложности в челлендже «Камнем вниз» за год приняли участие около 50 детей из разных регионов России. К лету 2022 года сообщения о нем появляться перестали.

Но если «Камнем вниз» можно считать сравнительно новой угрозой, то игра «Беги или умри» существовала задолго до появления интернета; с его появлением, а точнее, с развитием соцсетей и трансформацией мышления и поведения подростков, бессмысленно-опасное соревнование (перебежать через дорогу как можно ближе к проезжающему автомобилю) получило вторую жизнь.

Надо признать, что пубертат всегда считался самым сложным и опасным периодом в жизни человека. Гормональный шторм, перестройка психики, стремительное физиологические взросление, от которого как правило сильно отстает взросление психологическое превращают детей в одну большую группу риска. Но если раньше рискованное поведение имело смысл только при определенном стечении обстоятельств (много зрителей, присутствие объекта влюбленности и т.п.), то сегодня интернет и видеокамеры в смартфонах могут создать это стечение в любую секунду.

Из презентации «Информационные угрозы: интернет-истерия и рискованное поведение» педагог сможет узнать о том, что представляют собой современные челленджи и треды, и как определить, опасна ли очередная идея очередного видеоблогера, ставшая трендом или превратившаяся в челлендж. Кроме того, в материале дается общая картина наиболее распространенных в России моделей рискованного досуга, которые представляют потенциальную опасность для детей: зацепинг, руфинг, диггерство, бэйс-джампинг и т.п.

## 1.5. Фишинг

Эта презентация содержит информацию об интернет-угрозах, с которыми часто сталкиваются и дети, и взрослые. Формально фишинг входит в большую группу технологических угроз «Вредоносное программное обучение», но именно у этого вида киберпреступлений есть несколько очень характерных особенностей, которые ставят его на особое положение среди себе подобных.

Все разновидности компьютерных вирусов представляют собой более или менее сложную программу, которая умеет прятаться от эвристических анализаторов и копировать саму себя. Роль человеческого фактора в распространении таких программ минимальна или вообще нулевая.

Фишинг - это, в первую очередь, социальная инженерия и тонкое знание психологии, а уже потом - более или менее качественная работа криминальных программистов и дизайнеров. Проводя аналогии с криминальным миром офлайна, работа вирусных программ - это кража со взломом, а фишинг - мошенничество. Причём, как показывает практика, именно этот инструмент самый эффективный и наиболее часто используемый. Примерно половина всех зафиксированных в минувшем году онлайн-преступлений были совершены посредством фишинговых технологий.

Изучение презентации «Информационные угрозы: фишинг» даст педагогу представление о том, как работает социальная инженерия в руках мошенников, каким бывает фишинг и где с ним можно столкнуться, обучит основным правилам безопасности и даст представление о том, как научить детей базовым правилам защиты от атак с использованием указанного инструмента киберпреступности.

Узнать про фишинг можно также ознакомившись с анимированным роликом «На крючке» в цикле мультфильмов про киберучительницу Веру Ивановну.

## 1.6. Овершеринг

Несмотря на малоизвестное название, этот учебный материал имеет первостепенное значение для классного руководителя, который хочет уберечь детей от инцидентов в сети Интернет. Более того, для многих российских учителей и представителей управленческих команд образовательных организаций эта презентация может стать настоящим открытием.

Дело в том, что большинство из нас не понимает, насколько много информации мы совершенно добровольно выставляем на всеобщее обозрение. В первую очередь, конечно, этим неосознанно злоупотребляют ученики начальной и средней школы. Их гиперобщительность, желание всем понравиться, обрести много друзей, заполняя страницу своего профиля в соцсети, заставляют писать про себя всё, что они знают и что могут узнать - точный адрес, телефоны, персональные данные всех своих родственников, подробнейше рассказывают обо всех своих увлечениях, интересах, местах и способах досуга.

Новое мышление детей, родившихся в цифровую эпоху, формирует у них то, что называется «подиумное мышление». Ребенок считает состоявшимся только то событие в своей жизни, о котором он написал отчет в соцсети. Но и дети, в силу возрастной наивности, и взрослые, в силу недостаточной ИТ-компетентности, склонны недооценивать потенциальный вред, который они наносят себе такой откровенностью.

Всё, что выложено в сети Интернет —выложено навсегда и для всех. Все, что человек пишет даже в виде «подзамочного» поста или личного сообщения можно найти в сети даже годы спустя. Поэтому следует предельно внимательно относиться к тому, что ребенок сообщает о себе, и что сообщают о нём его сверстники в интернете.

Сегодня одна из самых дорогих и востребованных услуг на интернет-рынке - очистка интернет-репутации; это - те самые случаи, когда детские

глупости или юношеские ошибки догоняют уже взрослого человека в самый неожиданный и совершенно неподходящий момент.

В необходимости быть осмотрительным при публикации личных данных может также убедить и тот факт, что на криминальном рынке уже несколько лет существует специальность «профайлера» - человека, который мониторит социальные сети в поисках слишком откровенных и беспечных пользователей, и составляют на них подробнейшие досье, вплоть до плана квартиры и детализации материального благосостояния потенциальной жертвы.

Результаты работы таких «специалистов» пользуются спросом - потому что никто не сможет рассказать о вас больше достоверной информации, чем вы сами.

Изучение презентации «Информационные угрозы: овершаринг» даст педагогу представление о том, как сократить свой «информационный след» и сохранить личную информацию от кражи и публикации, обучит основным правилам безопасности и даст представление о том, как научить детей базовым правилам защиты персданных.

### 1.7. АУЕ (запрещено на территории России)

17 августа 2020 г. Верховный суд России признал международное общественное движение АУЕ экстремистской организацией. После решения участие в деятельности этого неформального движения может подпадать под уголовную ответственность, предусмотренную ст. 282.2 УК РФ за организацию или участие в деятельности организации, в отношении которой действует вступившее в силу решение суда о запрете ее деятельности в связи с осуществлением экстремистской деятельности, а также за склонение, вербовку или иное вовлечение в деятельность такой организации.

Экстремистским движениям в образовательном контенте посвящена отдельная презентация, но АУЕ необходимо уделить особое

внимание. Экстремистские движения и тоталитарно-деструктивные секты являются угрозой для детей.

АУЕ в своем изначальном виде задумывался и реализовывался как некая «криминальная пионерия» —кадровый резерв для бандитов и воров, создавших в начале 90-х годов на Дальнем Востоке что-то вроде криминального государства. «Государство», впрочем, довольно быстро прекратило своё существование, а вот АУЕ, как социально-культурное искажение, оказалось очень живучим.

Важнейшей особенностью этого явления в его сегодняшнем виде является абсолютная спонтанность: считать АУЕ «движением» или «организацией» не вполне корректно, так как отсутствуют основные признаки, квалифицирующие эти термины: выраженная вертикальная иерархия и структура, предполагающая управление в соответствии с заявленными задачами и целями.

Обычно, ученики, объявляющие себя «смотрящими по школе» и вымогающие у малышей деньги «на общак», занимаются обычным личным обогащением посредством мошенничества.

В тех случаях, когда школьники объединяются в группировки АУЕ для совершения противоправных действий, они не являются элементом некоей структуры и могут рассматриваться скорее как фанатское явление.

Презентация «Информационные угрозы: АУЕ (квазикриминальная субкультура)» дает знания об истории происхождения АУЕ, выгодоприобретателей от этого движения, а также признаки вовлеченности ученика в данную субкультуры и методы противодействия ей.

## 1.8. Груминг

Сообщения о нападениях педофилов на детей появляются с пугающей частотой. Последние дни лета 2022 года ознаменовались двумя шокирующими историями - 26 августа в городе Курильск на Итурупе 28-летняя женщина

обманом заманила 7-летнюю девочку в квартиру к своему сожителю, тот изнасиловал ребенка и выбросил ее из окна. На следующий день в Омской области педофил выбил зубы несовершеннолетней девочке во время изнасилования. Всё могло закончиться хуже, но прохожий услышал крики девочки и спугнул нападавшего.

Эти эпизоды - проявления так называемой «уличной» педофилии, и это - верхушка айсберга. Латентность преступлений против половой неприкосновенности детей по данным МВД России составляет 90% - то есть, 9 из 10 преступлений остаются безнаказанными, потому что о них просто никто не узнает.

Слово «груминг» имеет несколько значений. Наиболее известное из них - стрижка домашних питомцев. Но ещё, например, этим словом называется процедура ухаживания обезьян друг за другом - поиск насекомых у партнера, другие тактильные проявления с сексуальным подтекстом. Из этого значения выросло ещё одно: словом «груминг» называется демонстративный «ухаживающий» интерес взрослого человека к несовершеннолетнему ребенку в сети Интернет.

С точки зрения закона сам по себе груминг не является преступлением - существует много причин, по которым взрослый может быть заинтересован в ребенке. Но в тех случаях, когда этот интерес не мотивирован, а взрослый заведомо незнаком с объектом своего интереса, с большой вероятностью можно говорить о груминге как о признаке активности сетевого педофила.

Сексуальный интерес к детям в абсолютном большинстве культур считается совершенно неприемлемым, но педофилы, как и любые девианты, отверженные обществом, стремятся объединяться в группы, чтобы не ощущать своё одиночество как уродство. Поэтому они в числе первых освоили даркнет — территорию полной анонимности — и получили возможность общаться и обмениваться опытом совращения детей.

На форумах «тёмного интернета», посвященных этому извращению, они делятся методиками и инструментами, с помощью которых можно завоевать доверие ребенка, просто общаясь с ним в соцсети, и, как показывает статистика, эти методики и инструменты вполне эффективны: они находят ребенка, страдающего от одиночества, убеждают его в том, что он - особенный и уникальный, но его просто никто не понимает. В ход идут манипуляции, прикладные психологические инструменты и даже специальная литература - есть даже «специальные» сказки, которые работают на эту же задачу.

Презентация «Информационные угрозы: груминг» даст педагогу возможность ориентироваться в ситуации, и при появлении тревожных признаков в сетевой активности ребенка, помогут правильно идентифицировать ситуацию и принять соответствующие меры.

### 1.9. Вредоносное ПО

Угрозы, исходящие от распространения опасного программного обеспечения, можно назвать «фоновыми» - они существуют начиная с того момента, как устройство впервые подключается к сети Интернет. Стопроцентная защита от этой опасности существует, но она в абсолютном большинстве случаев неприменима. Единственный способ полностью уберечь себя от вредоносных программ - никогда не подключаться ни к сети Интернет, ни к альтернативным носителям информации - флешкам, жестким дискам и т.п. В любом другом случае риск заражения присутствует всегда, Но мы можем минимизировать его вероятность, предприняв необходимые меры безопасности и тщательно их соблюдая.

В первую очередь, речь идет об установке современных программных систем защиты устройства. Раньше их называли «антивирусами», но сегодня их функционал находится далеко за пределами поиска вредоносного кода в установленных на устройство программах и файлах. Представленные на рынке продукты - это мощные, интегрированные, многоуровневые комплексы,

которые занимаются непрерывным мониторингом всех систем и областей работы устройства - начиная от оперативной памяти и жестких дисков, заканчивая всем входящим и исходящим интернет-трафиком.

Как правило эти системы регулярно и достаточно часто обновляются и в большинстве случаев они имеют платный и бесплатный функционал.

Установка таких программных продуктов сегодня — безусловная необходимость.

В тех случаях, когда речь идет о подростках, соблюдение базовых мер безопасности несколько осложняется. Дети, в большинстве своем, уверены в том, что понимают «в компах» намного больше, чем взрослые, и зачастую это соответствует действительности. Но вопросы соблюдения ключевых правил информационной гигиены не имеют практически никакого отношения к ИТ-компетентности.

Как правило, дети отлично осведомлены о системах защиты и комплексных программах мониторинга. Непрерывная защита устройства потребляет достаточно много ресурсов системы - процессорной мощности, оперативной памяти, замедляет интернет-трафик и в целом делает устройство менее производительным. Причем, чем более серьёзный уровень защиты включен, тем больше ресурсов системы уходит на обеспечение безопасности.

Школьников, которые отлично об этом осведомлены, может категорически не устраивать то, что потенциально мощная машина работает медленнее, чем могла бы и дети просто отключают системы защиты - для того, чтобы устройство начало «летать», а игры не зависали. Быстродействие действительно увеличивается, но ровно до того момента, пока устройство не будет заблокировано вымогателем, подсадившим в него «шифровальщик» или «руткит».

Представленные в презентации «Информационные угрозы: вредоносное ПО» материалы дадут педагогу представление обо всем спектре

существующего вредоносного ПО и основных способах защиты от связанных информационно-технологических угроз.

### 1.10. Экстремизм и секты

Сегодня аккаунт в соцсетях стал источником большинства информации о человеке. Если речь идет о школьниках, то для них соцсеть — возможность самовыражения, которой они могут быть лишены офлайн. Поэтому учителям (как минимум – классным руководителям) имеет смысл следить за активностью школьников на социальных платформах. Как правило, первые признаки опасных ситуаций, с которыми сталкиваются дети, проявляются именно там.

Правонарушения экстремистского толка и раньше не были для подростков чем-то из ряда вон выходящим - нонконформизм и склонность к радикальным решениям, присущие пубертатному периоду, толкают детей на совершение необдуманных поступков, попадающих под действие статей Уголовного Кодекса Российской Федерации.

Наиболее яркими и часто встречающимися представителями молодежных экстремистских организаций до недавнего времени были два противоборствующих лагеря - ультраправые националисты (к которым, в том числе, относятся и “скинхеды”) и ультралевые активисты из анархистских организаций.

После нескольких крупных массовых акций в 2010 году, вызвавших широкий общественный резонанс (беспорядки, устроенные националистами на Манежной площади в 2010, и нападение анархистов на администрацию г. Химки) правоохранительные органы практически полностью ликвидировали организационные и координирующие структуры этих организаций, по сути прекратив их активность офлайн. И радикальные организации переместились в сеть Интернет, став еще одной информационной угрозой для российских школьников.

Ещё одним широким пластом экстремистских организаций, вовлекающих в свои ряды несовершеннолетних, можно считать ячейки исламских фундаменталистов. Есть несколько громких судебных прецедентов, когда молодых людей и девушек привлекали к уголовной ответственности при попытке отправиться на Ближний Восток. Был период, когда оперативники ФСБ России вели круглосуточный видеомониторинг транспортных узлов, выявляя и задерживая завербованных в стране «добровольцев» на полпути в Сирию. Известны случаи, когда исламские радикалы осуществляли вербовку «исламских жён», похищая девушек и переправляя их на Ближний Восток. Самый яркий такой прецедент - дело Варвары Карауловой, которая дважды пыталась бежать из России в запрещенную организацию ИГИЛ в Сирии. В декабре 2016 года она была приговорена к 4,5 годам заключения в колонии общего режима по обвинению в приготовлении к участию в деятельности террористической организации «Исламское государство».

Стоит особо отметить, что исламские экстремистские организации базируются на религиозных канонах, то есть разновидностью экстремистских организаций можно считать тоталитарно-деструктивные секты. Сегодня их активность в России сравнительно невысокая. Но на практике, действующие в стране опасные секты пока заняты набором неофитов, и учителям не стоит терять бдительность в этом направлении —особенно с учетом того, что вербовка в тоталитарно-деструктивные секты сегодня в абсолютном большинстве случаев начинается в соцсетях.

Ортодоксальные и радикальные религиозные организации присутствуют не только в исламе и восточных религиях. Христианство в целом и православие в частности также содержат огромное количество религиозных течений, которые могут быть отнесены к тоталитарно-деструктивным и даже экстремистским сектам.

Презентация «Информационные угрозы: секты, экстремизм» даст педагогу возможность ориентироваться в ситуации и при появлении тревожных

признаков в сетевой активности ребенка, помогут правильно идентифицировать ситуацию и принять соответствующие меры.

### 1.11. Наркоторговля в сети Даркнет

Наркопотребление —самая распространенная из информационных угроз, имеющая крайне неприятные последствия. Но есть еще одна опасность - вовлечение ребенка в наркоторговлю. По данным МВД России каждый седьмой наркокурьер на момент задержания учился в школе. Наркоторговцы очень заинтересованы в том, чтобы вовлекать в свой бизнес несовершеннолетних: дети не осознают уровень риска и готовы работать за сравнительно небольшие деньги, которые им кажутся огромными.

Примерно с середины нулевых годов вся индустрия мировой наркоторговли ушла в Даркнет. Как и везде в мире, российский сегмент «темного интернета» – среда обитания всех разновидностей и типов современной преступности.

Наркомания формирует собственную культуру и криптоязык: педагога должно насторожить появление в речи ребенка ранее незнакомых слов, но особенность наркоманского арго заключается в том, что оно использует обычные слова в другом значении, поэтому сторонний слушатель может ничего не заподозрить, услышав, как дети обсуждают купленные «в ЦУМе» «розовые кеды».

Изучив презентацию «Информационные угрозы: Даркнет» педагог будет знать, как опознать, что ребенок употребляет наркотики или вовлечен в наркоторговлю. Кроме того, в материалах содержится информация о действиях, которые может предпринять учитель, при выявлении ученика-наркомана.

## 2. Раздаточные обучающие материалы

### 2.1. Плакат «Кибербуллинг»

Плакат содержит информацию об основных признаках кибербуллинга и ключевые методики противодействия этой информационной угрозе.

Плакат можно распечатать и повесить в школе или другом среднеспециальном образовательном учреждении для изучения детьми и взрослыми.

### 2.2. Настольный календарь «Технологические угрозы сети Интернет»

Календарь на 2023 год, который поможет распознать различные угрозы, исходящие от вредоносного ПО в сети Интернет.

Календарь можно распечатать и использовать в школе или другом среднеспециальном образовательном учреждении, в том числе для изучения детьми и взрослыми.

### 2.3. Плакат «Полезные номера»

Номера экстренных служб, служб психологической и иной помощи, которые помогут ребенку и взрослым при столкновении с информационными угрозами.

Плакат можно распечатать и повесить в школе или другом среднеспециальном образовательном учреждении для изучения детьми и взрослыми.

### 2.4. Карточки для мессенджера Телеграм «Обязанности работников в отношении персональных данных»

В компактной и доступной форме корточки помогают учителям запомнить обязательные нормы и правила обращения с персональными данными, определенные действующим законодательством и ведомственными нормативными актами.

Карточки необходимо использовать в закрытых учительских чатах и каналах.

2.5. Карточки для мессенджера Телеграм «Виды вредоносного ПО»

Карточки содержат информацию о вредоностном ПО, которое распространяется в сети Интернет, и методах борьбы с ним.

Эти карточки учителя и представители управленческих команд могут использовать в школьных и классных телеграм-чатах, а также любых других мессенджерах и соцсетях, которыми обеспечивается присутствие образовательной организации в сети Интернет.

2.6. Справочник «Внешние признаки наркотического отравления»

Составленный совместно с наркологами и психиатрами справочник с описанием того, как меняются глаза человека и его поведение, употребившего наркотики.

НЕ ЯВЛЯЕТСЯ ДИАГНОСТИЧЕСКИМ СРЕДСТВОМ.

Материал не предназначен для детей и подростков. Убедительно просим обеспечить их хранение вне доступа несовершеннолетних, а также воздержаться от их публикации в общем доступе в сети Интернет и иных способов обнародования, предполагающих свободный неавторизованный доступ.

2.7. Брошюра «Пояснения к практикоориентированным кейсам»

Все, что могло быть непонятно или неочевидно во время изучения карточек кейсов и контрмер, подробно изложено в этой брошюре. Мы рекомендуем её изучение для получение более глубоких и детальных знаний об информационных угрозах

2.8. Брошюра «Словарь сленговых и жаргонных слов и выражений»

В словарь включены наиболее распространенные жаргонные и сленговые слова, которые используют подростки, вовлеченные в онлайн-игры, потребителей наркотических веществ и квазикриминальную субкультуру.

Материал не предназначен для детей и подростков. Убедительно просим обеспечить их хранение вне доступа несовершеннолетних, а также воздержаться от их публикации в общем доступе в сети Интернет и иных способов обнародования, предполагающих свободный неавторизованный доступ.

2.9. Чек-лист «Признаки депрессии»

Чек-лист поможет учителю выявить у ребенка признаки депрессии. Разработан совместно с психологами и психиатрами Федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный медицинский университет им. Н.Н. Бурденко» Министерства здравоохранения Российской Федерации.

Материал не предназначен для детей и подростков. Убедительно просим обеспечить их хранение вне доступа несовершеннолетних, а также воздержаться от их публикации в общем доступе в сети Интернет и иных способов обнародования, предполагающих свободный неавторизованный доступ.

2.10. Плакаты «Напомните родителям»

Плакат напомнит учителям и родителям основные правила общения с детьми, оказавшимися в трудной жизненной ситуации.

3. Информационно-обучающие видеоролики

Информационно-обучающие видеоролики призваны в доступной и понятной игровой форме обобщить базовые знания и умения современного интернет-пользователя.

Посмотрев эти ролики, вы научитесь создавать надежные пароли, удалять свои цифровые следы, пользоваться двухфакторной аутентификацией и будете знать, что нужно делать, чтобы ваши смартфон и компьютер были максимально защищены от большинства интернет-угроз. Важная информация, которую следует запомнить, выделяется при помощи технологии видеоскрайбинга, что способствует легкому запоминанию.

3.1. «Пароль-трансформер»

Видеоролик рассказывает о простых и удобных способах придумать и запомнить сложный пароль.


3.2. «На крючке»

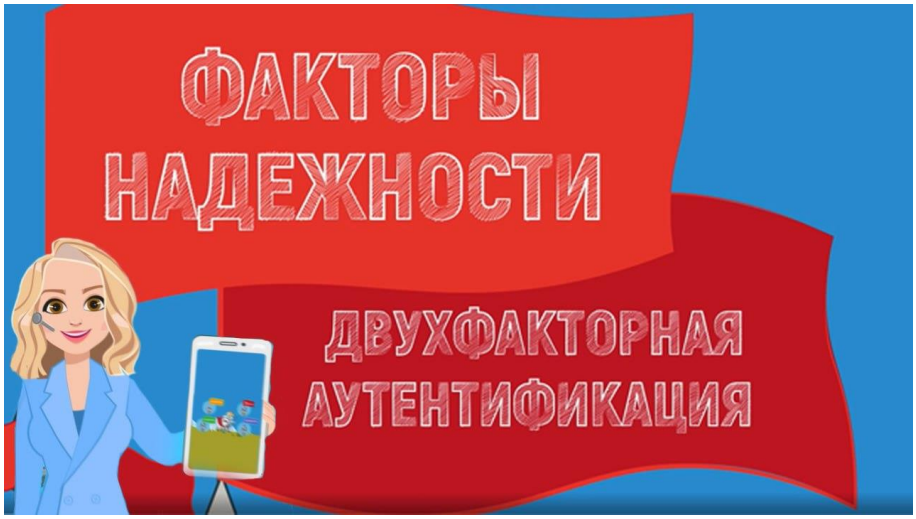
Видеоролик рассказывает о том, что такое фишинг и как с ним бороться.


3.3. «Роли паролей»

В видеоролике рассказывается о том, что такое двухфакторная аутентификация и зачем она нужна.

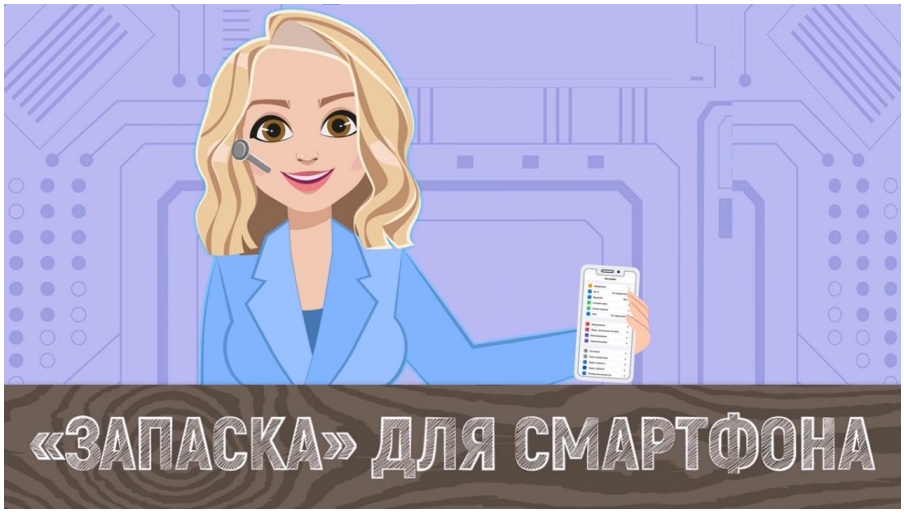

3.4. «Факторы надежности»

Видеоролик о том, какая бывает 2FA и как ею правильно пользоваться.



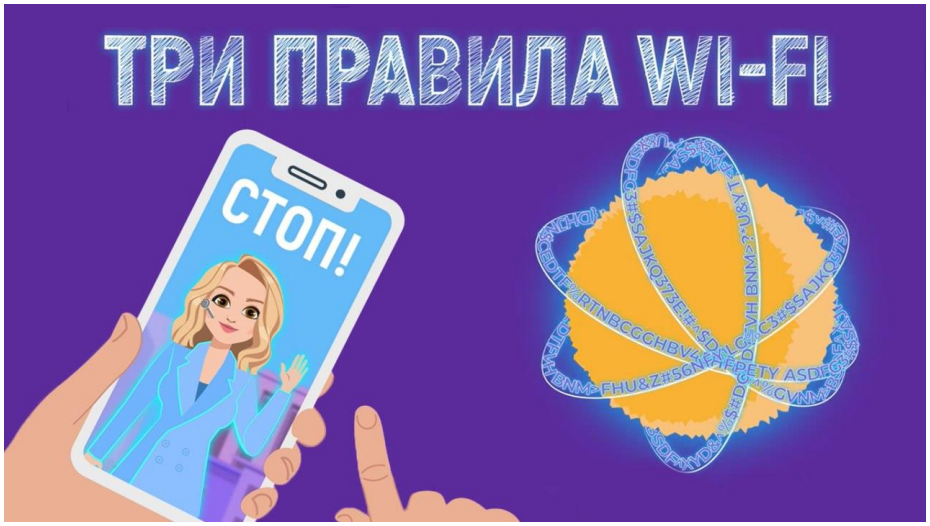

3.5. «Запаска для смартфона»

Видеоролик содержит информацию о том, как обеспечить безопасность своего мобильника




3.6. «3 правила wi-fi»

В видеоролике рассказывается о минусах использования публичного wi-fi и способах безопасности при его использовании

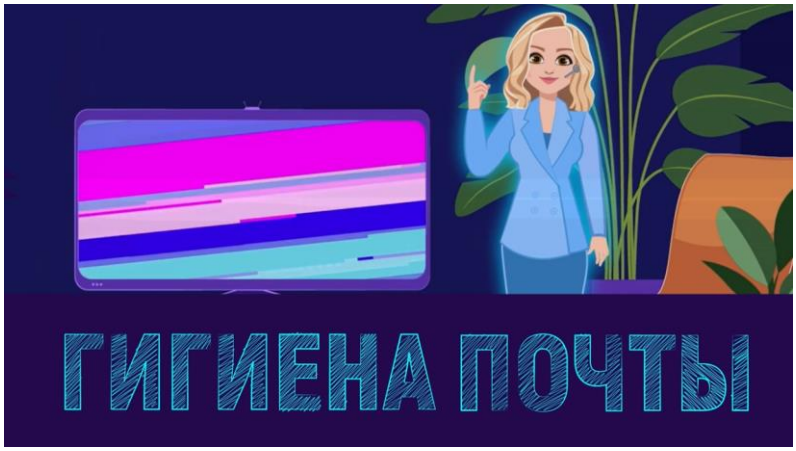



3.7. «Мишень с инициативой»

Видеоролик содержит информацию о том, что такое овершеринг и почему он не нужен.

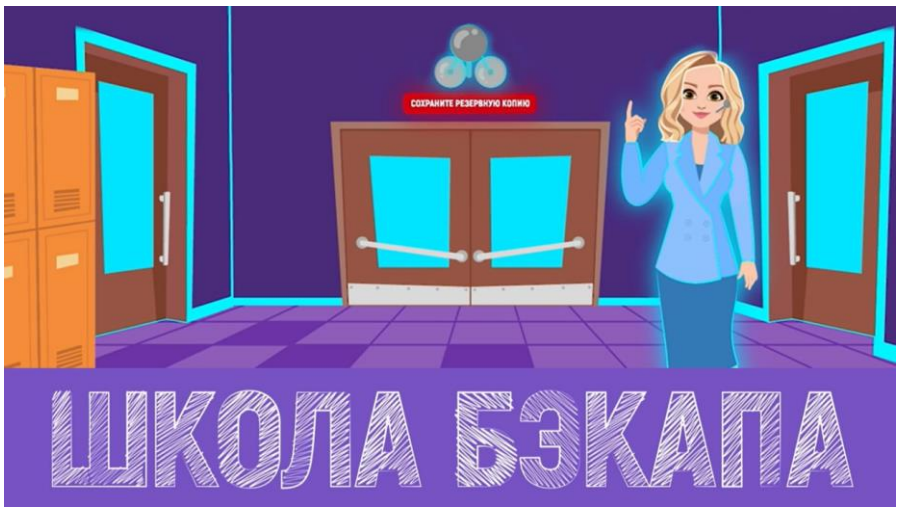

3.8. «Гигиена почты»

Видеородик рассказывает о простых правилах, которые помогут не получить по e-mail ничего лишнего



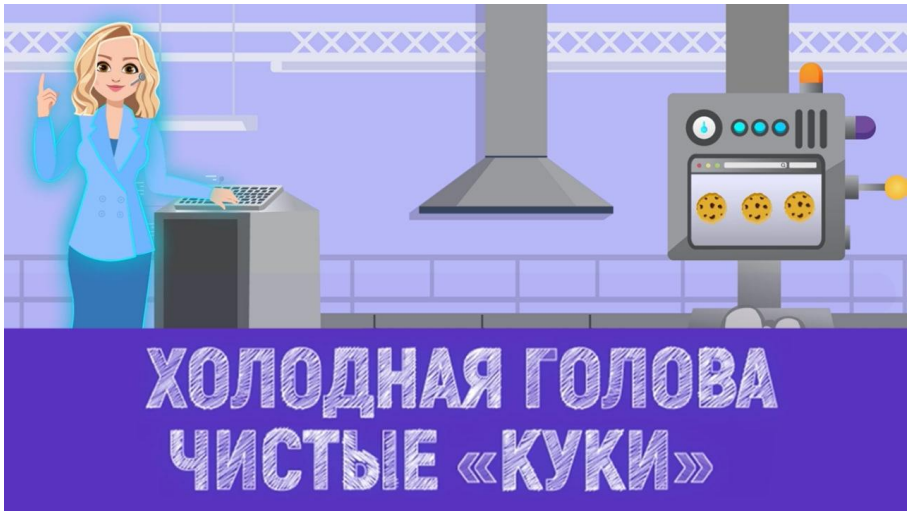

3.9. «Школа бэкапа»

В видеородике содержится информация о том, кто и зачем придумал резервные копии и надо ли их создавать.




3.10. «Холодная голова, чистые куки»

Видеоролик рассказывает о «цифровом следе» и как его чистить.




4. Раздел практикоориентированные кейсы и сценарии
для организации обучения в игровой форме

В этом разделе можно ознакомиться с уникальной разработкой ФГАОУ ДПО «Академия Минпросвещения России» - практикоориентированными кейсами для организации обучения в игровой форме и обучающими и контрольными сценариями.

С помощью данного набора возможно научиться распознавать ключевые информационные угрозы, с которыми могут столкнуться ученики в сети Интернет, именно с запрещенными в России АУЕ и Колумбайн, наркоторговлей в сети Даркнет и различными проявлениями экстремизма.

Практикоориентированные кейсы - это реальные ситуации столкновения детей с современными информационными угрозами, происходившие в российских школах.

Контрмеры - это инструменты профилактики и реагирования на информационные угрозы.

Оба набора карточек можно изучать сами по себе, а можно использовать в обучающих и контрольных сценариях.

Сценарии (обучающие и контрольные) для проведения обучения в игровой форме

В брошюрах содержатся правила четырех сценариев проведения обучения в игровой форме для противодействия информационным угрозам.

Сценарии преподнесены в порядке возрастания сложности: начиная от самого простого сценария «Давайте знакомиться» и заканчивая сложной поливариантной игровой механикой «Здравствуй, школа».

Сценарий 1 «Давайте знакомиться», сценарий 2 «Биржа», сценарий 3 «Профилактика» направлены на обучение, а сценарий 4 «Здравствуй, школа» является контрольным сценарием, направленным на закрепление полученных знаний.

Каждое применение сценария 4 создает новый случайный сюжет, с непредсказуемым сочетанием, сложностью и последовательностью возникновения угроз, и каждый раз предполагающий новую тактику реагирования.

Материалы не предназначен для детей и подростков. Убедительно просим обеспечить их хранение вне доступа несовершеннолетних, а также воздержаться от их публикации в общем доступе в сети Интернет и иных способов обнародования, предполагающих свободный неавторизованный доступ.