Актуально на 13 окт 2023

Информационная безопасность: какую работу провести с учениками и родителями

Светлана Михайлова, замдиректора по воспитанию и социализации ГБОУ «Школа № 814» г. Москвы, почетный работник общего образования РФ, член Союза писателей России

Татьяна Лопатина, эксперт Системы Завуч, педагогический стаж – более 20 лет, куратор педагогов в дистанционном курсе «Проектная деятельность в технике стартапов»

Приняли новую концепцию информационной безопасности детей.

Возьмите план мероприятий на 2023/24 год и подборку сценариев по информационной безопасности. В документах эксперты учли новую концепцию информационной безопасности и возрастные особенности детей. Также есть раздаточные материалы по информационной безопасности для учеников и их родителей и готовый школьный стенд.

План мероприятий по информационной безопасности на 2023/24 годПамятки по информационной безопасности для детей и родителейСтенд по информационной безопасностиМероприятия для учеников на уровне НООМероприятия для учеников на уровнях ООО и СООРодительское собрание для обсуждения инфобезопасности детейСправка по реализации концепции информационной безопасности

В 2023/24 учебном году мероприятия по информационной безопасности надо пересмотреть из-за новой Концепции информационной безопасности детей в РФ (распоряжение Правительства от 28.04.2023 № 1105-р). Так как дети являются наиболее уязвимой категорией в рамках цифровой безопасности, школам важно уберечь их от негативной и вредной информации. Федеральный закон от 29.12.2010 № 436-ФЗ делит такую информацию на запрещенную среди детей и ограниченную в зависимости от возраста. Смотрите подробнее в памятке.

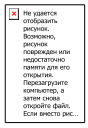
Чаще всего за информационную безопасность детей в школе отвечает замдиректора. Он организует, контролирует и координирует работу всего педагогического коллектива школы в этом направлении.

Минкомсвязи также рекомендует создать в школе совет по обеспечению информационной безопасности учеников (Методические рекомендации Минкомсвязи от 16.05.2019). В него можно включить педагогов, родителей и представителей органов власти. Пригласите членов общественных организаций – РДДМ «Движение первых», Общероссийского детского общественного движения «Страна молодых», кибердружин и др. Совет может проводить регулярный мониторинг качества системы контентной фильтрации и принимать участие в мероприятиях по информационной безопасности.

Подготовьте документацию

Проверьте наличие школьных документов, которые регулируют вопросы информационной безопасности в школе. При необходимости – разработайте их. Так рекомендует Минкомсвязи (Методические рекомендации от 16.05.2019). При этом приказы и положения обычно составляет директор школы, а инструкции для детей по информационной безопасности при использовании интернета – технический специалист. В итоге главный документ, за который отвечает заместитель директора, – план мероприятий по обеспечению информационной безопасности.

Разработайте план, чтобы обеспечить информационную безопасность детей. Включите в план мероприятия по установке системы контентной фильтрации, проверке библиотечного фонда. Отметьте просветительские мероприятия для детей и родителей. Запланируйте обучение педагогов на курсах повышения квалификации. Предусмотрите мероприятия внутреннего мониторинга информационной безопасности. Воспользуйтесь образцом плана, в котором эксперты учли новую Концепцию информационной безопасности.



План мероприятий по информационной безопасности на 2023/24 учебный год

Проверьте образовательные программы

Проанализируйте рабочие программы педагогов по учебным предметам и курсам внеурочной деятельности. А также рабочие программы факультативов, курсов, дисциплин из формируемой части учебного плана и программы допобразования. Убедитесь, что педагоги включили в содержание программ материал, чтобы обучить детей навыкам ответственного поведения в цифровой среде.

Пример

Темы по информационной безопасности, которые можно включить в содержание рабочей программы по информатике

№ п/п	Тема	Основное содержание
Безопасность общения		
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент
2	С кем безопасно общаться в интернете	Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети

3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн-генераторы паролей. Использование функции браузера по запоминанию паролей. Правила хранения паролей
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта
5	Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах
6	Публикация информации в социальных сетях	Персональные данные. Публикация личной информации
7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц
9	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах
Безопасность устройств		
10	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов
11	Распространение вредоносного кода	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах
12	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов
13	Распространение вредоносного кода для мобильных устройств	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке

		приложений на мобильные устройства
Безопасность информации		
14	Социальная инженерия: распознать и избежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах
15	Ложная информация в интернете	Фейковые новости. Поддельные страницы
16	Безопасность при использовании платежных карт в интернете	Транзакции и связанные с ними риски. Правила совершения онлайн-покупок. Безопасность банковских сервисов
17	Беспроводная технология связи	Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях
18	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах

Разработайте и интегрируйте в образовательный процесс уроки информационной безопасности и цифровой грамотности. Также предусмотрите мероприятия по изучению уровня информационной безопасности в школе, изучению рисков.

Зафиксируйте уроки информационной и цифровой грамотности и иные мероприятия в рабочей программе воспитания и календарном плане воспитательной работы. Например, в рамках модулей «Урочная деятельность», «Внеурочная деятельность», «Профилактика и безопасность». Или опишите в самостоятельном вариативном модуле.

Пример

Информационная безопасность в модуле «Профилактика и безопасность» рабочей программы воспитания и календарного плана воспитательной работы уровня ООО

Рабочая программа воспитания ООО. Модуль «Профилактика и безопасность»

Реализация воспитательного потенциала профилактической деятельности в целях формирования и поддержки безопасной и комфортной среды в образовательной организации предусматривает:

- <...>
- проведение исследований, мониторинга рисков безопасности и ресурсов повышения безопасности, в том числе – информационной; выделение и психолого-педагогическое сопровождение групп риска обучающихся по разным направлениям (агрессивное поведение, зависимости и др.);
- вовлечение обучающихся в воспитательную деятельность, проекты, программы профилактической направленности социальных и природных рисков в образовательной организации и в социокультурном окружении с педагогами,

родителями, социальными партнерами (антинаркотические, антиалкогольные, против курения; против вовлечения в деструктивные детские и молодежные объединения, культы, субкультуры, группы в социальных сетях; по информационной безопасности и безопасности в цифровой среде; на транспорте, на воде, безопасности дорожного движения, противопожарной безопасности, антитеррористической и антиэкстремистской безопасности, гражданской обороне и др.);

- организацию превентивной работы с обучающимися со сценариями социально одобряемого поведения, по развитию навыков саморефлексии, самоконтроля, устойчивости к негативным воздействиям, групповому давлению, в том числе – в цифровой среде;
- <...>

Календарный план воспитательной работы ООО. Модуль «Профилактика и безопасность»

Дела	Классы	Ориентировочное время проведения	Ответственные
<...>	<...>	<...>	<...>
Изучение уровня информационной и цифровой грамотности школьников	5–9-е	Сентябрь Январь Апрель	Замдиректора по ВР Советник по воспитанию
Психолого-педагогическое тестирование на выявление интернет-зависимости и игровой зависимости обучающихся	5–9-е	Октябрь	Замдиректора по ВР Советник по воспитанию Соцпедагог Психолог Классные руководители
Мониторинг рисков информационной безопасности	5–9-е	В течение года	Замдиректора по ВР Замдиректора по безопасности Советник по воспитанию Соцпедагог Психолог
Урок-дискуссия «Мир виртуальный или мир реальный»	8–9-е	Ноябрь	Советник по воспитанию

			Соцпедагог Психолог
Урок «Интернет и я: безопасное соединение»	5–7-е	Декабрь	Советник по воспитанию Соцпедагог Психолог
<...>	<...>	<...>	<...>

Раздайте памятки и оформите стенд

Минпросвещения направило в школы памятки по информационной безопасности детей и подростков (письмо от 24.05.2023 № 07-2755). Памятки для детей и родителей разработала Ассоциация организаций и граждан по оказанию помощи пропавшим и пострадавшим детям.

Для школьников предлагают четыре памятки. Они содержат рекомендации о том, сколько времени можно проводить в сети, как соблюсти анонимность и защитить свои персональные данные, а также как избежать интернет-зависимости.

Для родителей подготовили 21 памятку. В них постарались охватить все аспекты информационной безопасности детей и подростков. Памятки содержат пояснения, каким рискам и опасностям может подвергаться ребенок в соцсетях, видеохостингах, при участии в прямых трансляциях, в онлайн-общении с незнакомцами и т. п. Кроме того, дают практические советы родителям о том, как оградить детей от нежелательного контента, обеспечить родительский контроль и заключить с ребенком соглашение об использовании гаджетов. А также как помочь ребенку, если он оказался в опасной ситуации, например подвергся кибербуллингу.

Минпросвещения рекомендует школам использовать памятки в деятельности по профилактике рисков в цифровой среде. Со школьниками – в рамках учебных и внеклассных занятий. С родителями или законными представителями – при проведении родительских собраний, лекций и иных мероприятий. Можно разместить памятки на информационных стендах в фойе школы и в учебных кабинетах (письмо Минобрнауки от 14.05.2018 № 08-1184 «О направлении информации»). Скачайте ниже памятки в формате pdf, чтобы распечатать и раздать классным руководителям.

Памятки по информационной безопасности для детей и подростков

Памятка «Персональные данные»

Памятка «Время в сети»

Памятка «Анонимность в сети»

Памятка «10 советов»

Памятки по информационной безопасности для родителей или законных представителей


Памятка «Цифровая зависимость»


Памятка «Родительский контроль»


Памятка «Персональные данные»


Памятка «Опасные сообщества»


Памятка «Общение с незнакомцами»


Памятка «Обмен фото»


Памятка «Клиповое мышление»


Памятка «Вербовка»


Памятка «10 советов»


Памятка «Фейки»


Памятка «Семейное соглашение»


Памятка «Реальные последствия»


Памятка «Прямые трансляции»


Памятка «Поисковые системы»


Памятка «Опасные публикации»


Памятка «Онлайн-игры»


Памятка «Киберугрозы»


Памятка «Кибербезопасность»


Памятка «Иллюзии соцсетей»


Памятка «Видеохостинги»


Памятка «Мошенничество»

Ниже смотрите схему стенда по информационной безопасности, на котором вы сможете разместить все важные материалы. Такой же пакет документов можно дать и на школьном сайте.

Стенд по информационной безопасности

Разместите Концепцию информационной безопасности детей в РФ. Или QR-код со ссылкой на раздел школьного сайта, где размещен документ

Разместите план мероприятий по информационной безопасности на учебный год

Разместите памятки по информационной безопасности для детей и подростков

Разместите памятки по информационной безопасности детей для родителей

Проводите работу с учениками

Чтобы повысить информационную грамотность школьников и сформировать у них правильный безопасный алгоритм поведения в сети Интернет, можно использовать любые

форматы образовательной деятельности. Обучать детей цифровой и информационной безопасности можно в рамках внеурочной деятельности и дополнительного образования. Через классные часы, беседы, игры формируйте навыки законопослушного и ответственного поведения в цифровой среде, самостоятельного и ответственного потребления информационной продукции. Инициируйте участие школьников в проектах, которые продвигают традиционные ценности в информационной среде.

Учитывайте возрастно-психологические особенности школьников уровней НОО, ООО и СОО. От этого зависит, какие именно знания, умения и навыки в сфере информационной и цифровой безопасности педагоги будут формировать у учеников. А также – подбор материалов для занятий, форм деятельности, методов и средств обучения и воспитания.

На уровне НОО

На уровне НОО у школьников педагоги формируют базовые умения работы с информацией. Важно приучать детей мыслить критически при работе с информацией. То есть учить их анализировать новую информацию, сопоставлять ее с уже известной, сравнивать и делать выводы. Учить выделять источник информации в конкретных ситуациях.

Также важно формировать представление детей о том, что информация бывает разной. Это поможет им отличить достоверную информацию от недостоверной, этичную – от неэтичной и т. п. Выделять информационную угрозу и понимать, какой вред она несет для жизни, здоровья, учебы, межличностного общения.

Еще педагогам в начальной школе нужно развивать у детей навык принятия единственно правильного решения в конкретной ситуации. Дети должны усвоить алгоритм действий – когда и о чем необходимо сказать родителям или другим взрослым, которые рядом, когда убегать и т. п.

В работе с младшими школьниками целесообразно использовать игровые методы. Игра в непринужденной и доступной форме имитирует жизненные ситуации и позволяет усвоить навыки поведения в них. Смотрите ниже сценарий мероприятия и пример игры, в ходе которой у младших школьников можно сформировать правила безопасного поведения в интернете.

Сценарий интерактивного представления «Безопасность в интернете» для НОО

Пример

Игра «Сказочные ассоциации» для младших школьников

Педагог описывает сюжет сказки, или зачитывает из нее отрывок, или показывает отрывок фильма-сказки или мультфильма. Но не называет ее. Ученикам необходимо отгадать

название сказки, а также вспомнить или самостоятельно сформулировать правило безопасного поведения в интернете.

Отрывок № 1

Старик посадил старухину дочь в сани, повез ее в лес на то же место, вывалил в сугроб под высокой елью и уехал. Сидит старухина дочь, зубами от холода стучит. А Мороз по лесу потрескивает, с елки на елку поскакивает, пощелкивает, на старухину дочь поглядывает:

– Тепло ли тебе, девица? Тепло ль тебе, красная?

<...> А она ему:

– Ой, совсем застудил! Сгинь, пропади, проклятый!..

Ответ: сказка «Морозко». Правило безопасного поведения в интернете: «Будь вежлив при общении в сети. Не груби, не оскорбляй, не обижай других пользователей».

Отрывок № 2

– Здравствуй, добренький Буратино! Куда так спешишь?

– Домой, к папе Карло.

Лиса вздохнула еще умильнее:

– Уж не знаю, застанешь ли ты в живых бедного Карло, он совсем плох от голода и холода...

– А ты это видела? – Буратино разжал кулак и показал пять золотых. <...>

– Умненький, благоразумненький Буратино, хотел бы ты, чтобы у тебя денег стало в десять раз больше?

– Конечно, хочу! А как это делается?

– Проще простого. Пойдем с нами.

– Куда?

– В Страну Дураков.<...> В Стране Дураков есть волшебное поле, – называется Поле Чудес... На этом поле выкопай ямку, скажи три раза: «Крекс, фекс, пекс!», положи в ямку золотой, засыпь землей, сверху посыпь солью, полей хорошенько и иди спать. Наутро из ямки вырастет небольшое деревце, на нем вместо листьев будут висеть золотые монеты. Понятно?

Буратино даже подпрыгнул:

– Врешь!

– Идем, Базилио, – обиженно свернув нос, сказала лиса, – нам не верят – и не надо...

– Нет, нет, – закричал Буратино, – верю, верю!.. Идемте скорее в Страну Дураков!..

Ответ: сказка «Золотой ключик, или Приключения Буратино». Правило безопасного поведения в интернете: «Опасайся мошенников в сети».

Отрывок № 3

Пошел волк в кузницу и велел себе горло перековать, чтоб петь тоненьким голосом. Кузнец ему горло перековал. Волк опять побежал к избушке и спрятался за куст.<...>

Коза накормила, напоила козлят и строго-настрого наказала:

– Кто придет к избушечке, станет проситься толстым голосом да не переберет всего, что я вам причитываю, – дверь не отворяйте, никого не впускайте.

Только ушла коза, волк опять шасть к избушке, постучался и начал причитывать тонюсеньким голосом:

– Козлятушки, ребятушки!
Отопритеся, отворитеся!
Ваша мать пришла – молока принесла;
Бежит молоко по вымечку,
Из вымечка – по копытечку,
Из копытечка – во сыру землю!

Козлята отворили дверь, волк кинулся в избу и всех козлят съел. Только один козленочек схоронился в печке.

Ответ: сказка «Волк и семеро козлят». Правило безопасного поведения в интернете: «Под маской доброго человека может скрываться злой и опасный человек».

На уровне ООО и СОО

В основной школе подростки уже достаточно активно используют интернет. Как для развлечений, так и для выполнения школьных заданий, например для поиска информации для проектов. В приоритете у детей этого возраста – общение, и распространенным стало общение в соцсетях и мессенджерах. Кроме этого, подростки стараются казаться взрослыми и постоянно проверяют границы дозволенного – что они могут сделать без разрешения взрослых. Они могут совершать покупки через маркетплейсы, играть в онлайн-игры, общаться с незнакомцами, вступать в неформальные онлайн-сообщества.

Важно, как педагог преподносит информацию. Необходимо соблюдать баланс между негативом и позитивом в разговоре об информационной безопасности. Строгий запрет,

менторский категоричный тон учителя может вызвать нежелательную реакцию у подростков. Поэтому запреты нужно обосновывать, почему так делать не стоит, и приводить примеры, но не запугивать. А тон разговора следует выбрать доброжелательный и располагающий к конструктивному диалогу. Также обязательно приводить позитивные примеры последствий правильных действий.

Чтобы обеспечить интернет-безопасность учеников, педагогам следует обратить внимание подростков на несколько аспектов. Например, на то, как они ведут себя в сети. Пусть педагоги доносят до школьников, что в интернете, так же как и в реальной жизни, нужно вести себя вежливо и корректно. Знакомят с правилами поведения на форумах и чатах. Напоминают, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Еще нужно сформировать представление об основных опасностях интернета. Важно убедить не выдавать личную информацию в соцсетях, в сообщениях в чатах или электронной почте, при регистрации на сомнительных ресурсах. К личной информации относятся фамилия, имя, домашний адрес, номера телефонов, адрес электронной почты, возраст или дата рождения, название школы, фамилии друзей или родственников и т. п.

Педагогам необходимо объяснять подросткам опасность личных встреч с людьми, с которыми завели знакомство через интернет. Формировать осторожность и бдительность у школьников к таким встречам. Убеждать в том, что ни в коем случае нельзя встречаться с человеком, который упорно настаивает на встрече и на том, что о ней не нужно говорить родителям, учителям. Поддерживать у школьников потребность в случае опасности обращаться к взрослым. Например, сообщать родителям и педагогам, если что-либо или кто-либо в сети тревожит или угрожает ребенку. Ниже смотрите готовые сценарии.

Сценарий мероприятия «Мир реальный и виртуальный» для 5–7-х классов

Сценарий беседы «Что нужно знать о кибербуллинге» для 5–11-х классов

Сценарий классного часа «Интернет и я: безопасное соединение» для 7–10-х классов

В 8–9-х классах можно организовать кейс-поединки на тему информационной безопасности. Предложите школьникам изучить готовые учебные кейсы – проблемные ситуации, для которых нет очевидного и единственно верного решения. Задача учеников – найти выход из проблемной ситуации. Скачайте ниже готовые кейсы.

Кейс № 1 **Кейс № 2**


Кейс № 1 «Как Дмитрий карьеру начинал, или Игрушки как ловушки»

Введение

Драфт кейса

[Скачать]


Кейс № 2 «Новенькая в классе, или Пособие по выживанию»

Введение

Драфт кейса

[Скачать]

Кейс № 3


Кейс № 3 «Денежка рубль сбережет, а рубль голову стережет»

Введение

Драфт кейса

[Скачать]

Проводите работу с родителями

Для профилактики интернет-зависимости у школьников, националистических проявлений, устранения риска вовлечения школьников в противоправную деятельность проводите разъяснительную и консультационную работу с родителями. Это повысит их осведомленность о правилах и рисках предоставления детям средств связи с выходом в интернет. Разместите на сайте школы и ее страничках в соцсетях рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в интернете.

Проводите регулярные родительские собрания и индивидуальные встречи с родителями по вопросам информационной безопасности школьников. Основную часть времени в интернете дети проводят либо с домашних компьютеров, либо смартфонов и планшетов из дома. Поэтому именно на родителях лежит задача быть в курсе того, чем занимается ребенок, когда сидит за гаджетом, с кем общается и как проводит время в сети.

Перед собранием проведите анкетирование родителей. Это поможет собрать сведения и подготовиться к встрече с родителями на тему информационной безопасности. Заранее раздайте анкеты родителям, например за неделю до встречи. Так вы сможете своевременно обработать результаты и подобрать соответствующие материалы к собранию.

Анкета для родителей по информационной безопасности

Доносите до родителей, что самый действенный способ защиты детей – это профилактические беседы. Разговор родителя с ребенком на самые разные темы поможет оградить его от негативного влияния нежелательной или вредной информации. Многие ошибки как в реальной жизни, так и в интернете дети совершают по незнанию или из любопытства. Если ребенок получит нужную информацию от родителей, то ему не понадобится искать ее в интернете.

Однако родителям нужно учить детей правильно искать информацию в интернете или других источниках. И формировать умение отказаться от просмотра информации «не по возрасту», то есть формировать самоконтроль. Еще необходимо договориться с ребенком о ведении страницы в социальных сетях. Желательно, чтобы у ребенка и родителей такая страница была общая. Либо чтобы родители имели доступ к личной странице ребенка и могли в любой момент зайти на нее и проконтролировать содержание.

Рекомендуйте родителям использовать специальные средства обеспечения детской безопасности в сети. Например, дополнительные модули к антивирусным пакетам «Родительский контроль», детские браузеры и программы-фильтры. Такие средства не позволят загружать нежелательные сайты, ограничат время нахождения ребенка в интернете. Также они могут фиксировать сайты, которые посетил ребенок, и сообщать родителям о попытках взлома.

Доносите до родителей, что важно давать детям больше возможностей для живого общения со сверстниками. Поощрять участие в коллективных и групповых играх, творческой и проектной деятельности. Такое общение формирует коммуникативные навыки и способствует социализации детей.

Родителям и на собственном примере необходимо показывать важность живого общения для людей. Этому способствуют любые виды совместного времяпрепровождения родителей и детей: и ежедневное общение в кругу семьи, походы выходного дня, совместные посещения кино, театры и выставки и т. п.

Чтобы сократить время пребывания школьников в интернете, посоветуйте родителям увлекать детей заданиями, которые нужно выполнить с помощью компьютера, планшета или смартфона. Для младших школьников – игры по возрасту. Для детей постарше – освоение простых программ обработки фотографий, создания музыки, рисования и т. п. Для старшеклассников – программирование, написание приложений, игр и т. п. Это способствует развитию креативности, формирует новые полезные навыки.

Сценарий родительского собрания «Информационная безопасность школьника»

Возьмите на контроль

Проконтролируйте, как педагоги выполняют положения Концепции информационной безопасности детей. Посетите уроки. Это поможет понять, как учителя подбирают содержание уроков с учетом требований концепции информационной безопасности. Проведите также собеседования с педагогами – так вы выявите затруднения в реализации концепции.

Проконтролируйте, что ученики принимают участие в проектах по продвижению традиционных ценностей в информационной среде. Установите количество просветительских мероприятий по вопросам защиты персональных данных, инфобезопасности и цифровой грамотности, которое провели за отчетный период.

Проверьте, что все педагоги прошли курсы повышения квалификации вобласти цифровой грамотности школьников. Результаты проверки зафиксируйте в справке. По итогам сформулируйте вывод и рекомендации для педагогов и руководителей ШМО, чтобы своевременно скоординировать работу по обеспечению информационной безопасности. Скачайте готовую справку.

Справка по итогам контроля реализации концепции информационной безопасности