

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ХАКАСИЯ
Государственное автономное образовательное учреждение Республики Хакасия
дополнительного профессионального образования
«Хакасский институт развития образования и повышения квалификации»

«Согласовано»

на заседании Педагогического совета

«28» мая 2020 г.

Протокол № 2

«Утверждаю»

Ректор  С.Т. Дмитриева

«28» мая 2020 г.



ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Информационная безопасная среда»

Очно-заочная форма обучения, 16 час.

Составитель:

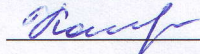
Комиссарова Г.И.,

и.о. зав. центром цифрового образования

Рассмотрено: на заседании центра
цифрового образования

ГАОУ РХ ДПО «ХакИРОиПК»

«28» мая 2020 г., протокол №5

 / Комиссарова Г.И.

АБАКАН
2020 г.

Пояснительная записка

Реализация целей и задач федерального проекта «Цифровая образовательная среда» требует совершенствования профессиональных компетенций педагогов в области информационной безопасности, на формирование информационной.

Программа «Информационная безопасная среда» раскрывает нормативные требования к организации образовательного процесса с учетом требований ФГОС, рассматривает вопросы информационной безопасности не только в образовательной среде, но и вне образовательного учреждения. Особое внимание уделяется защите персональных данных, работе в глобальной сети и информированию обучающихся и их родителей (лиц их замещающих) об основных видах информационных угроз и защите от них.

Программа разработана на основе профессионального стандарта «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель) (утвержден Приказом Министерства труда и социальной защиты РФ от 18.10.2013 №544н). Связь программы с профессиональным стандартом представлена обобщенными трудовыми функциями, трудовыми действиями, уровнем квалификации, которые служат ориентиром для характеристики профессиональных компетенций, подлежащих совершенствованию.

Обобщенные трудовые функции (ОТФ)	Трудовая(ые) функция(и) (ТФ)	Трудовое(ые) действие(я) (ТД)	Уровень квалификации (УК)
ОТФ1 Педагогическая деятельность по проектированию и реализации образовательного процесса с использованием ИКТ	ТФ1 Общепедагогическая функция. Обучение	ТД1 Осуществление профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов	6
	ТФ2 Развивающая деятельность	ТД2 Формирование навыков, связанных с информационно-коммуникационными технологиями	

Цель

Совершенствование профессиональной компетенции (далее – ПК) работников образования, а именно: методической (ПК), необходимой для профессиональной деятельности в рамках имеющейся квалификации.

Планируемые результаты обучения

В качестве планируемых результатов обучения по указанным трудовым действиям выступает профессиональная компетенция, которая характеризует приобретённые слушателями знания, умения и опыт деятельности:

ТД	ПК	Слушатель должен знать (З)	Слушатель должен уметь (У)	Слушатель должен владеть (приобрести опыт деятельности)(О)
ТД1	ПК1	З1.1 Знать требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете	У1.1 Уметь соблюдать нормы информационной этики и права У1.2 Использовать средства ИКТ в решении когнитивных, коммуникативных и организационных задач с соблюдением норм информационной безопасности	О1.1 Владеть правовыми аспектами использования компьютерных программ и работы в Интернете

Учебный план

№ п/п	Наименование модуля*	Всего часов	в том числе:			Форма контроля*
			лекции	практические занятия	самостоятельная работа	
1	Информационная безопасная среда *	16		4	12	
2.	Итоговая аттестация					зачет*
3.	Итого	16		4	12	

* символ обозначает тему модуля, форму контроля, которые полностью или частично реализуются в дистанционном режиме

Календарный учебный график

Дополнительная профессиональная программа повышения квалификации «Информационная безопасная среда» реализуется в соответствии с ежегодным планом-графиком повышения квалификации ГАОУ РХ ДПО «ХакИРОиПК».

Рабочая программа модуля «Информационная безопасная среда»

Освоение модуля направлено изучение нормативно-правовых вопросов информационной безопасности образовательной среды, приобретению опыта в вопросах защиты информации, использованию антивирусных программ и родительского контроля на гаджетах и персональных компьютерах.

1. Учебно-тематический план модуля

№ п/п	Наименование тем модуля*	Всего часов	в том числе:			Форма контроля*
			лекции	практические занятия	самостоятельная работа	
1.	Основные понятия информационной безопасной среды*			2	6	
2.	Информационные угрозы и методы защиты*			2	6	
3.	Промежуточная аттестация**					
3.	Итого	16		4	12	

* символ обозначает тему модуля, форму контроля, которые полностью или частично реализуются в дистанционном режиме

** промежуточная аттестация не предусмотрена программой

2. Содержание модуля

Тема 1. Основные понятия информационной безопасной среды

Нормативно-правовая база ИБС. Информационная безопасность ребенка: СанПин, сетевой этикет. Родительский контроль. Программы для родительского контроля, установка и использование.

2. Информационные угрозы и методы защиты

Вирусы. Социальная инженерия. Телефонные мошенники. Финансовые киберугрозы. Кэш-бек сервисы. Антивирусы (программы, установка и использование). Защита почтовых сервисов и аккаунтов социальных сетей (пароли, белые и черные списки).

3. *Оценочные материалы для проведения промежуточной аттестации по модулю*

Промежуточная аттестация не предусмотрена программой.

Организационно-педагогические условия

Требования к квалификации педагогических кадров, обеспечивающих реализацию образовательного процесса: занятия проводят старшие преподаватели, методисты, специализирующиеся в области преподавания интернет-технологий.

Требования к квалификации обучающегося. Квалификация обучающихся определяется в соответствии с перечнем направлений и квалификаций (ПС): учитель.

Требования к материально-техническим условиям. Занятия проводятся: а) в учебной аудитории (компьютерном классе), рассчитанной на нормативное количество слушателей, оснащенной компьютерами с лицензионным программным обеспечением, доступом в Интернет; б) с применением дистанционных образовательных технологий на платформе e-learning.

Требования к информационному и учебно-методическому обеспечению. В ходе освоения программы слушатели имеют доступ к информационным ресурсам библиотеки института и обеспечиваются следующими дидактическими материалами: список литературы, рекомендуемой для самостоятельной работы.

Список литературы, рекомендуемой для самостоятельной работы

1. Федеральный закон Российской Федерации «О персональных данных (с изменениями на 24 апреля 2020 года)»: [сайт]. URL: <http://docs.cntd.ru/document/901990046>
2. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации (с изменениями на 3 апреля 2020 года)»: [сайт]. URL: <http://docs.cntd.ru/document/901990051>
3. Федеральный закон Российской Федерации «О защите детей от информации, причиняющей вред их здоровью и развитию (с изменениями на 31 июля 2020 года)»: [сайт]. URL: <http://docs.cntd.ru/document/902254151>
4. Актуальные киберугрозы: I квартал 2020 года.: [сайт]. URL:
5. <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/>
6. (Вебинар) Интернет-мошенничество: Виды, тренды, способы защиты.: [сайт]. URL: <https://youtu.be/-QXLaaPCMuI>
7. (Вебинар) Формирование информационной безопасности обучающихся в образовательной организации.: [сайт]. URL: <https://youtu.be/O2CfQ43osC4>
8. Где мои дети.: [сайт]. URL: <https://pcappcatalog.com/994098803/gps>
9. Интернет-мошенничество: Виды, тренды, способы защиты.: [сайт]. URL: <https://youtu.be/-QXLaaPCMuI>
10. Информационная-образовательная среда ДОУ.: [сайт]. URL: <https://www.maam.ru/detskijasad/informaciono-obrazovatel'naja-sreda-v-dou.html>
11. Информационная безопасность детей.: [сайт]. URL: <https://whatisgood.ru/theory/soviet/posobie-informacionnaya-bezopasnost-detej/>
12. Кибербезопасность. Чему учить ребенка в интернете: рекомендации педагогам.: [сайт]. URL: <https://diso.ru/blog/34>
13. Компьютерные вирусы. Типы, виды, пути заражения.: [сайт]. URL: <https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html>
14. Надежный пароль. Каким он должен быть?: [сайт]. URL: https://chaynikam.net/view_articles.php?id=19
15. Об учителе в цифровом образовательном пространстве.: сайт]. URL: <http://detionline.com/assets/files/journal/32/dio32temakushnir.pdf>
16. Овчинский, В.В. Основы борьбы с киберпреступностью и кибертерроризмом. Хрестоматия. – М.: Норма, 2017. – 528с.
17. Основные понятия информационной безопасности.: [сайт]. URL: <https://www.intuit.ru/studies/courses/697/553/lecture/12442>
18. Солдатова, Г.У., Рассказова, Е.И., Нестик, Т.А. Цифровое поколение России: компетентность и безопасность. – Смысл М.: 2017. – 375 с.

19. Социальная инженерия.: [сайт]. URL: <https://www.stekspb.ru/blog/it/socialnaya-inzheneriya/>
20. Формирование информационной безопасности обучающихся в образовательной организации.: [сайт]. URL: <https://youtu.be/O2CfQ43osC4>
21. Цифровая компетентность подростков и родителей.: [сайт]. URL: <http://detionline.com/assets/files/research/DigitalLiteracy.pdf>

Формы аттестации

Промежуточная аттестация программой не предусмотрена.

Итоговая аттестация по программе проводится в форме зачета.

Оценочные материалы

Оценка планируемых результатов освоения программы осуществляется на основе оценочных материалов для проведения итоговой аттестации: требования к аттестационному испытанию, примерные задания аттестационного испытания, критерии оценки аттестационного испытания, принципы выставления оценки за аттестационное испытание.

Требования к аттестационному испытанию

Аттестационное испытание по итогам освоения программы:

- устанавливает соответствие результатов освоения дополнительной общеразвивающей программы заявленной цели и планируемым результатам обучения;
- осуществляется в форме выполнения теста.

Тест выполняется после освоения программы с применением дистанционных образовательных технологий на платформе e-learning. Количество заданий – 10.

Примерное время выполнения теста и количество попыток не ограничено.

Примерные задания аттестационного испытания

№ п/п	Задание	Источник
1	Какие вирусы активизируются после включения ОС? А. Снифферы Б. Загрузочные В. Трояны Г. Черви	https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html
2	Очень сложные пароли гарантируют 100% защиту? А. Нет Б. Да, если после работы полностью очищать куки и не хранить пароль на компьютере В. Да, если пароль не сохранен на компьютере	https://chaynikam.net/view_articles.php?id=19
3	Представляют ли угрозу вирусы для крупных компаний? А. Нет Б. Да, представляют В. Скорее нет. В крупных компаниях развита система безопасности	https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html
4	Фильтрация контента, для чего она служит? А. Защищает от скрытой загрузки вредоносного программного обеспечения Б. Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени В. Отключает назойливую рекламу Г. Отсеивает поисковый спам	https://www.saferunet.ru/expert/article/743/
5	Что может привести к заражению компьютера? А. Получение сообщения по электронной почте Б. Загрузка пиратского ПО В. Создание нового файла Г. Отправка сообщения по электронной почте	https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
6	Антивирус полностью защищает компьютер от	https://www.kaspersky.ru/resource-

	<p>вирусов и атак при работе в сети. Вы согласны с этим?</p> <p>А. Нет</p> <p>Б. Да, если это лицензионный антивирус известного производителя</p> <p>В. Защищает совместно с включенным бродмауэром</p> <p>Г. Да</p>	<p>center/threats/computer-viruses-and-malware-facts-and-faqs</p> <p>https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html</p>
7	<p>Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?</p> <p>А. Да</p> <p>Б. Да, если это антивирусы от известных производителей</p> <p>В. Да, если это антивирусы одного производителя</p> <p>Г. Нет</p>	<p>https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs</p>
8	<p>Сетевой этикет это:</p> <p>А. Понятие, возникшее с появлением электронной почты</p> <p>Б. Программа для изучения правил этикета</p> <p>В. Совокупность данных на компьютере</p>	<p>https://psihomed.com/setevoy-etiket/</p>
9	<p>Что такое троллинг?</p> <p>А. Вид виртуального общения в котором нагнетается конфликт.</p> <p>Б. Возможность авторизоваться на сайте.</p> <p>В. Разновидность веб-страниц в которых встроено видео.</p>	<p>https://7ya-ru.turbopages.org/s/7ya.ru/article/Agressiya-podrostkov-v-Internetе-trolling-i-kiberbullying/</p>
10	<p>Что такое плагиат?</p> <p>А. Неуникальный текст</p> <p>Б. Возможность определить автора текста</p> <p>В. Скопированный текст</p> <p>Г. Умышленное присвоение авторства</p>	<p>https://compress.ru/article.aspx?id=12181</p>

Критерии оценки аттестационного испытания

Результаты по тесту формируются путем суммирования набранных баллов – по 1 баллу за каждое правильно выполненное задание. Максимальный балл – 10 (100%).

Принципы выставления оценки за аттестационное испытание

Оценка «зачтено» выставляется, если слушатель ответил правильно не менее чем на 70% вопросов теста, в противном случае выставляется оценка «не зачтено».