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
«23» мая 2019 г.
Протокол № 2

«Утверждаю»
Ректор С.Т. Дмитриева
«23» мая 2019 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
«Кибербезопасность детей в современном мире»

Заочная с ДОТ форма обучения, 16 час.

Составитель:
Комиссарова Галина Ивановна,
методист учебно-методического центра
дистанционного образования

«Рассмотрено»
на заседании учебно-методического центра
дистанционного образования
ГАОУ РХ ДПО «ХакИРОиПК»
«19» апреля 2019 г., протокол №3
_____ / Булгакова О. В.

АБАКАН
2019 г.

Пояснительная записка

Дополнительная профессиональная программа «Кибербезопасность детей в современном мире» рассчитана на знание педагогами и обучающимися основ безопасного поведения в киберпространстве. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, преподаватель любой дисциплины может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте урока различные аспекты организации информационной безопасности. Преподаватель должен иметь представление о современном уровне развития вычислительной техники, информационный сетей, технологий коммуникации и навигации.

Программа разработана на основе профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», утвержденного Приказом Министерства труда и социальной защиты РФ от 18 октября 2013 г. № 544н. Связь Программы с профессиональным стандартом представлена обобщенными трудовыми функциями, трудовыми функциями, трудовыми действиями, уровнем квалификации, которые служат ориентиром для характеристики профессиональных компетенций, подлежащих совершенствованию.

Обобщенная(ые) трудовая(ые) функция(и) (ОТФ)	Трудовая(ые) функция(и) (ТФ)	Трудовое(ые) действие(я) (ТД)	Уровень квалификации (УК)
ОТФ1Педагогическая деятельность по проектированию и реализации образовательного процесса с использованием ИКТ	ТФ1 Общепедагогическая функция	ТД1 Осуществление профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов ТД2 Формирование навыков, связанных информационно-коммуникационными технологиями, в частности, со знанием киберугроз и защиты от них	6

Особенность программы заключается в том, что она:

– основана на применении практико-ориентированного, компетентностного подхода и модульного принципа представления содержания;

– способствует осмыслению накопленного слушателями собственного опыта с позиции правовых аспектов использования компьютерных программ и работы в Интернете.

Цель

Совершенствование профессиональной компетенции (далее – ПК) работников образования, а именно: правовой (ПК1), необходимой для профессиональной деятельности в рамках имеющейся квалификации.

Планируемые результаты обучения

В качестве планируемых результатов обучения по указанным трудовым действиям выступают профессиональные компетенции, которые характеризуют приобретенные слушателями знания, умения и опыт деятельности:

ТД	ПК	Слушатель должен знать (З)	Слушатель должен уметь (У)	Слушатель должен владеть (приобрести опыт деятельности)(О)

ТД1 ТД2	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 модулей*	Всего часов	в том числе			Форма контроля*
			лекции	практические занятия	самостоятельная работа	
1.	Методы обеспечения безопасности персонального компьютера и Интернета*	16			16	
2.	Итоговая аттестация					зачет*
3.	Итого	16			16	

* символ обозначает модуль/форму контроля, которые полностью или частично реализуются в дистанционном режиме

Календарный учебный график

Дополнительная профессиональная программа повышения квалификации «Кибербезопасность детей в современном мире» реализуется по индивидуальным запросам работников образования.

Рабочие программы

Рабочая программа модуля 1.«Методы обеспечения безопасности персонального компьютера и Интернета»

Программа модуля позволяет познакомиться с основными видами киберугроз и методами защиты киберпространства, персональных данных.

Учебно-тематический план

№ п/п	Наименование тем модуля*	Всего часов	в том числе:			Форма контроля**
			лекции	практические занятия	самостоятельная работа	
1.	Понятие кибербезопасности, виды защиты киберпространства*	4			4	
2.	Кто обеспечивает защиту киберпространства*	4			4	
3.	Защита персональных данных, почему она нужна*	4			4	
4.	Сетевой этикет: правила и нормы в электронной почте, социальных сетях*	4			4	
5.	Текущая аттестация**					
6.	Итого	16			16	

* символ обозначает тему модуля, которая полностью или частично реализуется в дистанционном режиме

** текущая аттестация не предусмотрена учебным планом программы

2. Содержание модуля

Тема 1. Понятие кибербезопасности, виды защиты киберпространства.

Понятие кибербезопасности, виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации). Подбор и настройка брендмауэра и антивирусного софта.

Тема 2. Кто обеспечивает защиту киберпространства

Правовые основы кибербезопасности: международное и Российское законодательства в сфере компьютерной информации. Уголовная ответственность.

Тема 3. Защита персональных данных, почему она нужна

Насколько интернет много знает о нас. Иллюзия о конфиденциальности. Что можно и нельзя размещать в открытом доступе. Опасности открытой информации и риски, связанные с открытым доступом. Ответственность за нарушение требований по обеспечению безопасности персональных данных.

Тема 4. Сетевой этикет: правила и нормы в электронной почте, социальных сетях.

Понятие и правила сетевого этикета. Правила общения в сети. Анонимность и троллинг. Интернет-травля: как не ввязаться и не стать жертвой. Как выходить из травматичного интернет-общения, способы защиты и правовое регулирование.

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): работники образования.

Требования к материально-техническим условиям. Занятия проводятся 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, вопросы к зачетам.

Список литературы, рекомендуемой для самостоятельной работы

1. Безопасный Интернет детям. Министерство внутренних дел Российской Федерации: [сайт]. — URL: http://mvd.ru.
2. Згадзай, О. Э. Киберпреступность: факторы и проблемы борьбы / О. Э. Згадзай, С.Я. Казанцев // Вестник НЦ БЖД. – 2013 — № 4 (18). — С. 80–86.
3. Информационная безопасность. Итоги года глазами Positive Technologies: [сайт]. — URL: https://www.securitylab.ru/news/490260.php.
4. Овчинский, В.В. Основы борьбы с киберпреступностью и кибертерроризмом. Хрестоматия. – М.: Норма, 2017. – 528 с.
5. Психология и гигиена соцсетей: [сайт]. — URL: https://batenka.ru/resource/med/psycho-sn/.
6. Рассолов, И.М., Чубукова, С.Г., Суворов, А.А. Информационное право. Учебник / И.М. Рассолов, С.Г. Чубукова, А.А. Суворов. – М.: Проспект, 2016. – 352с.

Формы аттестации

Текущая аттестация по модулю программы – не предусмотрена учебным планом.

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 профессиональной программы заявленной цели и планируемым результатам обучения;
- осуществляется в форме теста.

Тест выполняется после освоения программы с применением дистанционных образовательных технологий на платформе e-learning. Количество заданий – 15. Время выполнения теста и количество попыток не ограничено.

Примерные задания аттестационного испытания

1. Какие вирусы активизируются после включения ОС?
А.Снифферы
Б.Загрузочные
В.Трояны
Г.Черви
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
3. Представляют ли угрозу вирусы для крупных компаний?
А.Нет
Б.Да, представляют
В.Скорее нет. В крупных компаниях развита система безопасности
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
5. Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?
А.15
Б.8
В.10
Г.6
6. Какую угрозу можно назвать преднамеренной? Сотрудник:
А.Открыл письмо содержащее вредоносное ПО
Б.Ввел неправильные данные
В.Совершил не авторизованный доступ
Г.Включил компьютер без разрешения
7. Безопасно ли вводить пароли простым копированием?
А.Безопасно, если это мой компьютер
Б.Да
В.Безопасно, если после работы очистить куки
Г.Нет
8. 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 почт
9. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?
А.Нет
Б.Да, если это лицензионный антивирус известного производителя
В.Защищает совместно с включенным бродмауэром
Г.Да
10. Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?

А.Да
Б.Да, если это антивирусы от известных производителей
В.Да, если это антивирусы одного производителя
Г.Нет
11. Что чаше всего используют злоумышленники при атаке на компьютеры должностных лиц и руководителей крупных компаний?
А.Фишинг
Б.Спам
В.Загрузка скрытого вредоносного ПО
12. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?
А.Да, если это мой личный компьютер
Б.Да
В.Нет
Г.Да, если компьютер не подключен к интернету
13. Сетевой этикет это:
А.Понятие, возникшее с появлением электронной почты+
Б.Программа для изучения правил этикета
В.Совокупность данных на компьютере
14. Что такое троллинг?
А.Представитель царства животных.
Б.Вид виртуального общения в котором нагнетается конфликт.
В.Возможность авторизоватся на сайте.
Г.Разновидность веб-страниц в которых встроено видео.
15. Что такое плагиат?
А.Неуникальный текст
Б.Возможность определить автора текста
В.Скопированный текст
Г.Умышленное присвоение авторства

Критерии оценки аттестационного испытания

Результаты по тесту формируются путем суммирования набранных баллов – по 1 баллу за каждое правильно выполненное задание. Максимальное количество баллов – 15 (100%).

Принцип выставления оценки за аттестационное испытание

Оценка «зачтено» выставляется, если верные ответы слушателя на вопросы теста составляют не менее 70%, в противном случае выставляется оценка «не зачтено».