Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет» (КемГУ)

Беловский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования
«Кемеровский государственный университет» (БИФ КемГУ)
Управление развития дополнительного образования (УРДО)

УТВЕРЖДАЮ:
Первый проректор
_____Ю.Н.Журавлев
«25» декабря 2023 г.

ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

(повышение квалификации)

«Кибергигиена: Личная информационная безопасность»

Начальник УРДО О.М. Левкина

Директор БИФ Кем ГУ В.А.Саркисян

Белово 2023

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

В настоящее время выросла потребность общества в технически грамотных учителях, преподавателях, воспитателях, полностью отвечающих социальному заказу государства в области кибергигиены. Повсеместная цифровизация образования, жизнь и трудовая деятельность в цифровом мире дает педагогическим работникам новые широкие возможности, но и таит серьезные опасности, знать о которых необходимо каждому специалисту.

Предлагаемая дополнительная профессиональная образовательная программа повышения квалификации «Кибергигиена: Личная информационная безопасность» способствует привлечению внимания к вопросам кибербезопасности и формированию у граждан навыков безопасного поведения в интернете. Регулярное обучение по вопросам кибербезопасности не только предотвращают негативные инциденты, но и могут помочь повысить осознание угроз и укрепить культуру безопасности в организации.

1.1 Цель и задачи реализации программы

Цель программы: формирование и (или) развитие у слушателей профессиональных компетенций, способствующих разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства.

Задачи:

1. Приобретение знаний, умений и навыков, соответствующих современным запросам общества;
2. Актуализация знаний в сфере кибергигиены и кибербезопасности;
3. Приобретение навыков безопасного поведения в информационном пространстве.

Данная программа разработана в соответствии со следующими нормативными документами:

- Федеральный закон "Об образовании в Российской Федерации"от 29 декабря 2012 г. N 273-ФЗ;
- Приказ Минобрнауки России от 01.07.2013 N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" (Зарегистрировано в Минюсте России 20.08.2013 N 29444);
- ФГОС ВО по направлению подготовки 44.03.01 Педагогическое образование (уровень бакалавриата), утвержденный Приказом Минобрнауки России от 22 февраля 2018 г. № 121.
- Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании), (воспитатель, учитель)» (Приказ Министерства труда и социальной защиты РФ от 18 октября 2013г. № 544н, с изменениями, внесенными приказом Министерства труда и соцзащиты РФ от 25 декабря 2014г. № 1115н и от 5 августа 2016г. № 422н)

1.2. Связь программы дополнительного профессионального образования (ДПО) с ФГОС ВО

Программа ДПО разработана на основании ФГОС ВО.

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное совершенствование которых осуществляется в результате реализации программы ДПО.

ФГОС ВО 44.03.01 Педагогическое образование	Программа повышения квалификации «Кибергигиена: Личная информационная безопасность»
Выпускник должен обладать следующими	Содержание программы ДПО направлена на совершенствование следующих компетенций:

общепрофессиональными компетенциями:	
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ПК-1. Способен решать задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1.3. Планируемые результаты обучения

В результате освоения программы предполагается совершенствование следующих профессиональных компетенций:

Профессиональная компетенция	Планируемые результаты обучения
ПК-1. Способен решать задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** принципы применения методов обеспечения кибербезопасности; правила безопасной работы в сети интернет; **Уметь:** выявлять угрозы информационной безопасности; определять угрозы конфиденциальности, целостности, доступности информации; проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности. **Трудовые действия:** реализация педагогической деятельности с учетом правил кибербезопасности;

1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Лица, желающие освоить данную программу должны иметь/получать высшее или среднее профессиональное образование. Указанное образование должно подтверждаться документом государственного или установленного образца.

1.5. Режим занятий

Учебная нагрузка включает все виды учебной работы слушателя.

Для всех видов аудиторных занятий устанавливается академический час продолжительностью 45 минут.

2. Содержание программы

2.1. Учебный план

дополнительной профессиональной программы

«Кибергигиена: Личная информационная безопасность»

Категория слушателей: Лица, желающие освоить данную программу должны иметь/получать высшее или среднее профессиональное образование. Указанное образование должно подтверждаться документом государственного или установленного образца.

Объем программы –18 часов трудоемкости, в т.ч. 10 часов аудиторных занятий
Форма обучения – *очно-заочная с применением дистанционных технологий*

№ п/п	Наименование модулей/дисциплин	Общая трудоемкость, час.	Аудиторные занятия, час.		Самост. работа, час	Форма контроля
			лекции	практич. и лаборат. занятия		
1.	Утечки данных	2	1		1	Зачет
2.	Пароли	2		1	1	Зачет
3.	Фишинг	2	1		1	Зачет
4.	Безопасность в интернете	2		1	1	Зачет
5.	Обнаружение инцидента кибербезопасности	2	1		1	Зачет
6.	Безопасность технических устройств	2		1	1	Зачет
7.	Телефонное мошенничество	2	1		1	Зачет
8.	Психологические приемы и актуальные приемы атак	2	1		1	Зачет
9.	Итоговая аттестация: зачет	2		2		Зачет
	Всего	**18**	**5**	**5**	**8**	

2.2. Содержание

дополнительной профессиональной программы

«Кибергигиена: Личная информационная безопасность»

Наименование дисциплины (раздела, модуля) и тем	Всего, час.	Содержание темы	Компетенции
Утечки данных	2	Крупные утечки данных. Виды: умышленные, случайные.	ПК-1
Пароли	2	Правила составления паролей. Стойкий пароль. Парольные фразы. Принципы двухфакторной аутентификации для усиления безопасности учетных записей.	ПК-1
Фишинг	2	Макрасы. Правила определения фишингового письма. Порядок действий при потере устройства. Порядок действий при потере доступа к сайту. Порядок действий при обнаружении фишингового письма. Как действуют BEC-атаки.	ПК-1
Безопасность в интернете	2	Правила и требования для безопасной удаленной работы. Правила безопасного пребывания в интернете. Очистка метаданных.	ПК-1
Обнаружение инцидента кибербезопасности	2	Признаки попыток нарушения кибербезопасности. Действия при обнаружении нестандартного поведения устройства. Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность. Понятие организационной защиты информации. Источники и классификация угроз информационной безопасности.	ПК-1

Безопасность технических устройств	2	Правила безопасности для компьютера. Правила работы со съемными носителями. Правила безопасности для телефона.	ПК-1
Телефонное мошенничество	2	Виды звонков, СМС. Признаки телефонного мошенничества. Правила поведения при атаках мошенников.	ПК-1
Психологические приемы и актуальные приемы атак	2	Атаки типа социальная инженерия. Дифицит, недостаточность. Симпатия и доверие. Авторитет. Социальная поддержка.	ПК-1

2.3.Календарный учебный график

Дисциплины (модули)	**Трудо-емкость, час**	**Неделя 1**	**Неделя 2**
Утечки данных	2	УП,З	
Пароли	2	УП,З	
Фишинг	2	УП,З	
Безопасность в интернете	2	УП,З	
Обнаружение инцидента кибербезопасности	2		УП,З
Безопасность технических устройств	2		УП,З
Телефонное мошенничество	2		УП,З
Психологические приемы и актуальные приемы атак	2		УП,З
Итоговая аттестация: зачет	2		З

УП – учебный процесс;
З – зачет по дисциплине (модулю);

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1 Организационно-педагогические условия реализации программы

Преподаватели, участвующие в учебном процессе по ДПП, формируются из числа профессорско-преподавательского состава БИФ КемГУ, других высших образовательных организаций, также приглашенных специалистов из других организаций.

Обязательными требованиями к преподавателям, ведущим учебный процесс по ДПП, являются:

1. наличие высшего образования;
2. наличие документа, подтверждающего высшее образование по профилю преподаваемой дисциплины;
3. стаж преподавательской деятельности не менее 3 лет (или стаж в должности по профилю преподаваемой дисциплины не менее 3 лет);
4. отсутствие судимости (подтверждается наличием справки).

Преподаватели по ДПП назначаются по согласованию руководителя программы и директора БИФ КемГУ в соответствии с расчетом трудозатрат педагогической деятельности.

3.2. Материально-технические условия реализации программы

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечений
Аудитория	Аудиторные занятия	Компьютер, мультимедийный проектор, экран, доска

3.3. Учебно-методическое обеспечение программы
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Программа ДПО ставит своей целью обучение взрослых слушателей. Слушатели являются субъектами собственной профессиональной деятельности, самостоятельно определяя время, затрачиваемое на изучение основной и дополнительной учебной литературы.

Перечень рекомендуемой литературы не является исчерпывающим и использование дополнительной литературы из фондов ЭБС, дают преимущество самостоятельного освоения обширного информационного материала, в целях совершенствования навыков работы с нормативно-правовыми базами данных и работы с разноплановыми источниками профессиональной информации.

№ п/п	Наименование дисциплин	Литература
1.	Утечки данных	Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режимдоступа: http://www.iprbookshop.ru/52209.html
2.	Пароли	Мельников В.П. Информационная безопасность и защита информации: учеб.пособие / В.П. Мельников, 2007г
3.	Фишинг	Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационнойбезопасности / Д. Г. Ермаков, А. В. Присяжный. — Екатеринбург : Уральский федеральныйуниверситет, ЭБС АСВ, 2013. — 64 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/66577.html
4.	Безопасность в интернете	Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций/ А. В. Артемов. — Электрон. текстовые данные. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 c. — 2227-8397. —Режим доступа: http://www.iprbookshop.ru/33430.html
5.	Обнаружение инцидента кибербезопасности	Костин, В. Н. Методы и средства защиты компьютерной информации: информационнаябезопасность компьютерных сетей : учебное пособие / В. Н. Костин. —Москва : Издательский Дом МИСиС, 2018. — 31 c. — ISBN 978-5-906953-53-7. —Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —URL: http://www.iprbookshop.ru/98200.html
6.	Безопасность технических устройств	Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами/ А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. —692c. —ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPRBOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98349.html
7.	Телефонное мошенничество	Основы национальной безопасности: учебно-методическое пособие / составителиС. Ю. Махов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2019. — 88 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная системаIPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/95409.html
8.	Психологические	Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. —

	приемы и актуальные приемы атак	3-е изд. —Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечнаясистема IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html
9.	Итоговая аттестация: зачет	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 04.12.2023).

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1 Текущий контроль и промежуточная аттестация

Оценка успеваемости слушателей по учебным дисциплинам осуществляется в ходе текущего и промежуточного контроля.

Текущий контроль – это непрерывно осуществляемое наблюдение за уровнем усвоения знаний и формированием умений, навыков и компетенций. Формами текущего контроля являются опросы, собеседования, решение практически ситуационных задач в рамках лекционных и практически занятий.

Промежуточный контроль – это вид контроля, предусмотренный учебным планом, который проводится в форме зачетов по учебным дисциплинам.

Компетенции по дисциплине формируются последовательно в ходе проведения теоретических и практических занятий. Для контроля знаний обучающихся разработаны вопросы, выносимые на зачет.

По учебным дисциплинам установлены следующие универсальные критерии оценки знаний (умений и владения) слушателей:

в форме зачета:

- отметка ***«зачтено»*** ставится слушателю, если он обнаруживает полное знание учебно-программного материала, успешно выполняет предусмотренные программой задания, усвоил основную литературу по курсу и знаком с дополнительной литературой, рекомендованной в программе, без затруднений излагает материал в устной речи, владеет специальной терминологией;

- отметка ***«не зачтено»*** ставится, если слушатель обнаружил пробелы в знаниях основного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, затрудняется в устном изложении материала, не владеет специальной (по данной учебной дисциплине) и плохо владеет общенаучной терминологией.

Условия, процедура подготовки и проведения зачета по отдельной дисциплине самостоятельно разрабатываются преподавателями.

4.2 Итоговая аттестация

Целью итоговой аттестации является оценка уровня сформированности профессиональных компетенций слушателей. Итоговая аттестация (далее – ИА) направлена на установление соответствия уровня профессиональной подготовки обучающихся требованиям стандарта. Итоговая аттестация слушателей состоит из междисциплинарного зачета по дисциплинам.

Целью ИА является установление уровня подготовки обучающихся и установление уровня их готовности к выполнению профессиональных задач.

Критерии оценки ответов слушателей:

1. Уровень усвоения материала, предусмотренного программой ДПО.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Ответы на вопросы: полнота, аргументированность, убежденность.
4. Качество ответа (его общая композиция, логичность, общая эрудиция).

5. Использование дополнительной литературы при подготовке ответов.

Примерные вопросы к зачету

1. Понятие "информационная безопасность" и ее задачи
2. Составляющие информационной безопасности
3. Понятие защиты информации и ее задачи
4. Методы защиты препятствие;
5. Методы защиты управление доступом;
6. Методы защиты механизмы шифрования;
7. Методы защиты противодействие атакам вредоносных программ;
8. Методы защиты регламентация;
9. Методы защиты принуждение;
10. Фишинг. Правила определения
11. Понятие кибербезопасности
12. Компьютерная безопасность
13. Понятие информационных угроз
14. Вредоносное программное обеспечение
15. Понятие киберпреступности
16. Спам
17. Кибератаки и их психологические приемы
18. Кибератаки их типы и приемы
19. Похищение паролей
20. Стадии Кибератаки
21. Защита документов MS Word
22. Защита документов MS Excel
23. Безопасность технических устройств
24. Телефонное мошенничество и методы борьбы с ним.
25. Антивирусные программы и пакеты.

Критерии оценки устного ответа слушателя

зачтено - демонстрирует знание основных положений соответствующего раздела программы; свободно излагает материал, владеет навыками публичного выступления.

не зачтено - демонстрирует недостаточный уровень знаний по соответствующему разделу дисциплины; излагает материал непоследовательно и допускает ошибки в языковом оформлении.

5. Составители программы

Е.В.Кузнецова, педагог дополнительного образования Беловского института (филиала) ФГБОУ ВО «Кемеровский государственный университет».