Комитет по делам образования города Челябинска

Муниципальное бюджетное учреждение дополнительного профессионального образования

«Центр развития образования города Челябинска»

РЕКОМЕНДОВАНО И ОДОБРЕНО
решением Методического совета
МБУ ДПО ЦРО
(протокол от 08.11.2019 №2)

УТВЕРЖДАЮ
Директор МБУ ДПО ЦРО
_____ С.В. Мачинская
«12» ноября 2019 г.

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность в современном обществе»

Челябинск
2019

1. ЦЕЛЬ ПРОГРАММЫ

Актуальность. Информационные технологии стали неотъемлемой частью деятельности человека в любой профессиональной сфере. Данные технологии необходимы современному человеку для активного использования во всех видах профессиональной деятельности.

На сегодняшний день современное информационное общество – наиболее развитая фаза современной цивилизации, наступающая в результате информационно-компьютерной революции, когда стали использоваться информационные технологии, «интеллектуальные» системы, автоматизация и роботизация всех сфер и отраслей экономики и управления, создания единой новейшей интегрированной системы связи, предоставляющей каждому человеку любую информацию и знания, обусловливает радикальные изменения во всей системе общественных отношений, благодаря чему обеспечиваются наибольший прогресс и свобода личности, возможность ее самореализации.

Умение эффективно работать с информацией в современном мире является одним из важнейших факторов успеха. Мы живем в век информационного общества и не может не замечать, что стираются границы между абстрактной категорией «информация» и носителем этой информации. Виртуальный мир в современных реалиях представляет угрозу личности, собственности, о которых мы ранее не задумывались. В связи с этим защита информации в сети Интернет стала особенно актуальна в последнее врем.

Программа дополнительного профессионального образования разработана в соответствии с:

– Федеральным Законом № 273-ФЗ «Об образовании в Российской Федерации»;

– Федеральным государственным образовательным стандартом общего образования;

– Федеральным государственным образовательным стандартом дошкольного образования;

– Профессиональным стандартом «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)».

Цель программы: повышение информационной компетентности педагогов путем определения рисков в сфере приватности и обеспечения безопасности использования персональных данных.

Задачами образовательной программы являются:

Основная цель курса – повышение уровня информационной компетентности педагогов по вопросу безопасного использования сети Интерне. Для решения поставленной цели необходимо решить следующие задачи:

1. Познакомить с понятийным аппаратом в рамках безопасного обращения с персональными данными в сети Интернет.
2. Расширить представления об основных способах защиты своих персональных данных.
3. Рекомендовать интернет-ресурсы, оказывающие поддержку в вопросах информационной безопасности и защите персональных данных.

Требования к квалификации слушателей. К освоению дополнительной профессиональной программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование, а также лица, получающие среднее профессиональное и (или) высшее образование в области образования и педагогики.

Слушатели курса должны иметь:

- практический опыт работы с прикладными офисными программами Office;
- практический опыт работы в сети Интернет и сервисах сети Интернет.

Категории педагогических работников, для которых предназначена программа. Настоящая программа предназначена для повышения квалификации педагогов муниципальной образовательной системы, а также всех заинтересованных лиц.

Профессиональные компетенции педагогов, качественное изменение которых осуществляется в процессе обучения (в рамках реализации программы). В результате обучения по программе должны быть сформированы следующие профессиональные компетенции, качественное изменение которых повлечет за собой повышение качества образования:

- общепользовательская ИКТ-компетентность;
- общепедагогическая ИКТ-компетентность;
- предметно-педагогическая ИКТ-компетентность (отражающая профессиональную ИКТ-компетентность, соответствующей области человеческой деятельности.

Структура программы повышения квалификации. Структурными компонентами настоящей программы являются следующие: титульный лист; пояснительная записка; планируемые результаты обучения; содержание программы; учебный план; календарный учебный график, рабочая программа; материально-технические условия реализации программы; требования к результатам обучения программы. Освоение программы рассчитано на 36 часов.

Настоящая программа включает в себя три раздела.

Первый раздел программы рассматривает нормативно-правовые документы, обеспечивающие защиту персональных данных.

Второй раздел программы знакомит слушателей с инструментами офисного пакета Microsoft Office, с возможностью их использования в проектировании мероприятия.

Третий раздел предлагает слушателям разработать проект мероприятия по кибребезопасности для участников образовательных отношений.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ:

В результате освоения дополнительной профессиональной программы «Информационная безопасность в современном обществе» слушатели должны:

Знать:

– механизмы защиты персональных данных в сети Интернет.

Уметь:

– управлять персональными данными при работе с различными онлайн-ресурсами, приложениями и устройствами;

– применять в своей практической деятельности способы, методы и приемы обеспечения информационной безопасности и защиты персональных данных.

Владеть:

– имеющимися навыками в повседневном и профессиональном контексте.

3. ХАРАКТЕРИСТИКА ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ ДОСТИЖЕНИЯ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ

Организационно-педагогические условия достижения планируемых результатов обеспечивают реализацию образовательной программы в полном объеме, соответствуют качеству подготовки слушателей установленным требованиям, соответствуют применяемым формам, средствам, методам обучения и воспитания, возрастным, психофизическим особенностям, склонностям, способностям, интересам и потребностям слушателей.

Теоретическое и практическое обучение проводится в оборудованных учебных кабинетах с использованием учебно-материальной базы, соответствующей установленным требованиям.

Наполняемость учебной группы составляет 12 человек.

Продолжительность учебного часа теоретических и практических занятий составляет 1 академический час (45 минут).

Кадровые условия обеспечивают преподаватели, реализующие данную программу. Требования, предъявляемы к преподавателю:

Преподаватель должен иметь высшее профессиональное образование или среднее профессиональное образование по направлению подготовки «Образование и педагогика» или в области, соответствующей преподаваемому предмету, а также высшее профессиональное образования или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности.

Преподаватель должен знать:

- приоритетные направления развития образовательной системы РФ;
- законы и иные нормативные правовые акты, регламентирующие образовательную деятельность;
- содержание учебных программ и принципы организации обучения по преподаваемому предмету;
- основные технологические процессы и приёмы работы на должностях в организациях по специальности в соответствии с профилем обучения в образовательной организации;
- основы экономики организации производства и управления;
- педагогику;
- физиологию, психологию и методику профессионального обучения;
- современные формы и методы обучения;
- основы трудового законодательства;
- теорию и методы управления образовательными системами;
- современные педагогические технологии продуктивного, дифференцированного обучения, реализации компетентностного подхода, развивающего обучения;
- методы убеждения, аргументации своей позиции, установления контактов с обучающимися, коллегами по работе;
- технологии диагностики причин конфликтных ситуаций, их профилактики и разрешения;
- основы экологии, экономики, социологии;

– основы работы с текстовым редактором, электронными таблицами, электронной почтой и браузерами, мультимедийным оборудованием;
– правила внутреннего трудового распорядка МБУ ДПО ЦРО;
– правила по охране труда и пожарной безопасности.

4. УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы повышения квалификации «Информационная безопасность в современном обществе»

Категория обучаемых: педагоги муниципальной образовательной системы, а также все заинтересованные лица.
Трудоемкость программы: 36 часов.
Форма обучения: очная.

№ п/п	Наименование разделов	Всего часов	В том числе				Формы контроля
			Лекции	Практические занятия	Дистант	Самостоятельная работа	
1.	Раздел № 1. Защита персональных данных в современном информационно обществе	6	2	4			Диагностика.
2.	Раздел № 2. Подготовка учебно-методических материалов инструментами офисного пакета	12	4	8			Промежуточная аттестация
3.	Раздел № 3. Проектная деятельность	16		16			Диагностика
4.	Итоговая аттестация	2		2			Защита итоговой выпускной работы
5.	**Итого:**	**36**	**6**	**30**			

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Трудоемкость программы: 36 часов.
Форма обучения: очная.
Режим занятий: по 6 часов в день, 6 дней.

№ п/п	Наименование тем	Всего часов	Дни занятий					
			1	**2**	**3**	**4**	**5**	**6**
1.	Тема 1.1. Нормативно-правовое обеспечение вопросов защиты персональных данных	2	ДИ Т2					
2.	Тема 1.2. Способы, методы и приемы обеспечения информационной безопасности	4	П4					
3.	Тема 2.1. Особенности работы с текстовым редактором Microsoft Word	6		Т2 П4 ПА				
4.	Тема 2.2. Визуализация данных в презентации Microsoft PowerPoint	6			Т2 П4 ПА			
5.	Тема 3.1. Проектирование мероприятия по кибербезопасности для участников образовательных отношений	12				П6	П6	
6.	Тема 3.2. Оформление проекта мероприятия инструментами офисного пакета	4						П4 ДИ
7.	Итоговая аттестация	2						ИА2
8.	**Итого часов**	**36**	**6**	**6**	**6**	**6**	**6**	**6**
9.	**Итого**	**36 часов**						

Обозначения:
ДИ – диагностика
Т – теоретическое занятие;
П – практическое занятие;
ПА – промежуточная аттестация;
ИА – итоговая аттестация.

6. РАБОЧАЯ ПРОГРАММА КУРСА
6.1. Учебно-тематический план
«Информационная безопасность в современном обществе»

Категория обучаемых: педагоги муниципальной образовательной системы, а также все заинтересованные лица.
Трудоемкость программы: 36 часов.
Форма обучения: очная.
Режим занятий: по 6 часов в день, 6 дней.

№ п/п	Наименование разделов и тем	Всего часов	В том числе				Формы контроля
			Лекции	Практические занятия	Дистант	Самостоятельная работа	
1.	Раздел 1. Защита персональных данных в современном информационном обществе	6	2	4			Диагностика
1.1.	Тема 1.1. Нормативно-правовое обеспечение вопросов защиты персональных данных	2	2				
1.2.	Тема 1.2. Способы, методы и приемы обеспечения информационной безопасности	4		4			
2.	Раздел 2. Подготовка учебно-методических материалов инструментами офисного пакета	12	4	8			
2.1.	Тема 2.1. Особенности работы с текстовым редактором Microsoft Word	6	2	4			Промежуточная аттестация (выполнение практического задания)
2.2.	Тема 2.2. Визуализация данных в презентации Microsoft PowerPoint	6	2	4			Промежуточная аттестация (выполнение практического задания)
3.	Раздел 3. Проектная деятельность	16		16			
3.1.	Тема 3.1. Проектирование мероприятия по кибербезопасности для участников образовательных отношений	12		12			
3.2.	Тема 3.2. Оформление проекта мероприятия инструментами офисного пакета	4		4			Диагностика

№ п/п	Наименование разделов и тем	Всего часов	В том числе				Формы контроля
			Лекции	Практические занятия	Дистант	Самостоятельная работа	
4	Итоговая аттестация	2		2			Защита итоговой выпускной работы
	Итого:	**36**	**6**	**30**			

ВСЕГО: количество часов по УТП – 36 часов
Аудиторные занятия (36 ч.)
Из них:

- теоретические – 6 ч.
- практические – 30 ч.

(в т.ч. итоговая аттестация – 2 ч.)

6.2. Содержание разделов «Информационная безопасность в современном обществе»

Рабочая программа

Раздел 1 «Защита персональных данных в современном информационном обществе» (6 ч.)

Тема 1.1. «Нормативно-правовое обеспечение вопросов защиты персональных данных» (2 ч.).

В данной теме рассматриваются следующие вопросы: государственная политика в сфере вопросов защиты информации, персональных данных; понятие «персональные данные»; понятийный аппарат в рамках безопасного обращения с персональными данными в сети Интернет; компетенции, права, обязанности и ответственность оператора персональных данных.

Виды занятий по теме: лекция (2 ч.).

Тема 1.2. «Способы, методы и приемы обеспечения информационной безопасности» (4 ч.).

В данной теме рассматриваются следующие вопросы: управление персональными данными в сети Интернет; интернет-ресурсы, оказывающие поддержку в вопросах информационной безопасности и защиты персональных данных.

Виды занятий по теме: практическое занятие (4 ч.).

Перечень практических занятий

Номер темы	Наименование практического занятия
Тема 1.2.	Современная жизнь в открытом информационном обществе (4 ч.)

Раздел 2 «Подготовка учебно-методических материалов инструментами офисного пакета» (12 ч.)

Тема 2.1. «Особенности работы с текстовым редактором Microsoft Word» (6 ч.).

В данной теме рассматриваются следующие вопросы: приемы редактирования и форматирования текстовой информации; приемы форматирования различных типов графических объектов.

Виды занятий по теме: лекция (2 ч.), практическое занятие (4 ч.)

Перечень практических занятий

Номер темы	Наименование практического занятия
Тема 2.1.	Форматирование документа текстового редактора Microsoft Word (4 ч.)

Тема 2.2. «Визуализация данных в презентации Microsoft Power Point» (6 ч.).

В данной теме рассматриваются следующие вопросы: приемы редактирования и форматирования слайдов; различные способы вставки графических объектов на слайд; дизайн презентации; анимационные эффекты; гиперссылки.

Виды занятий по теме: лекция (2 ч.), практическое занятие (4 ч.).

Перечень практических занятий

Номер темы	Наименование практического занятия
Тема 2.2.	Создание простой презентации (4 ч.)

Раздел 3. «Проектная деятельность» (16 ч.)

Тема 3.1. «Проектирование мероприятия по кибербезопасности для участников образовательных отношений» (12 ч.).

В данной теме рассматриваются следующие вопросы: изучение, анализ, подбор материалов для проектирования мероприятия по кибербезопасности.

Виды занятий по теме: практическое занятие (12 ч.).

Перечень практических занятий

Номер темы	Наименование практического занятия
Тема 3.1.	Обобщение и структурирование подобранных материалов для проектирования мероприятия по кибербезопасности (12 ч.)

Тема 3.2. «Оформление проекта мероприятия инструментами офисного пакета» (4 ч.).

В данной теме рассматриваются следующие вопросы: электронной оформление конспекта и презентации мероприятия (организационно-управленческого мероприятия/занятия/урока) по кибербезопасности.

Виды занятий по теме: практическое занятие (4 ч.).

Перечень практических занятий

Номер темы	Наименование практического занятия
Тема 3.2.	Печать конспекта и создание презентации (4 ч.)

Итоговая аттестация (2 ч). Итоговая работа по теме «Мероприятие по кибербезопасности для участников образовательных отношений».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ
«Информационная безопасность в современном обществе»

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятия	Наименование оборудования, программного обеспечения
Компьютерный класс, рабочие места – 12, преподаватель – 1	Лекция	Компьютер (13 шт.), мультимедийный проектор, экран. Программное обеспечение пакет Microsoft Office, браузер Google Chrome
	Практические занятия и практические работы	Компьютер (13 шт.), мультимедийный проектор, экран. Программное обеспечение пакет Microsoft Office, браузер Google Chrome

Список литературы и источников

Нормативно-правовые документы

1. Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948).

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) (рус., англ.) (от 28.01.1981 с изменениями, внесенными Международным договором от 15.06.1999). Ратифицирована Федеральным законом РФ от 19.12.2005 № 160-ФЗ.

4. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015).

5. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

6. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью и развитию».

7. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных».

8. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».

9. Федеральный закон от 24.07.1998 г. № 124-ФЗ (в ред. от 28.12.2016 г.) «Об основных гарантиях прав ребенка в Российской Федерации».

10. Федеральный закон от 21.07.2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием

Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»».

11. Распоряжение Правительства РФ от 02.12.2015 г. № 2471-р «Концепция детской информационной безопасности».

12. Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации (утв. Минобрнауки России 11.05.2011 г. № АФ-12/07вн).

13. Письмо Министерства образования и науки РФ от 28.04.2014 г. № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».

14. Письмо Министерства образования и науки Российской Федерации от 14.05.2018 г. № 08-1184 «О направлении информации» (вместе с методическими рекомендациями «О размещении на информационных стендах, официальных Интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет».

15. Письмо Министерства образования и науки РФ от 10.11.2006 г. № АС-1299/03 «О реализации контентной фильтрации доступа образовательных учреждений, подключаемых к сети Интернет в рамках приоритетного национального проекта «Образование»».

16. Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ (ред. от 02.082019) Глава 14 «Защита персональных данных работника».

17. Гражданский кодекс РФ от 30.11.1994 № 51-ФЗ (ред. от 18.07.2019) Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации».

18. Разъяснения Роскомнадзора от 30 августа 2013 г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки».

Литература

19. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Г.У. Солдатова, А.А. Приезжева, О.И. Олькина, В.Н. Шляпников. – изд. 2-е, испр. и доп. – М.: Генезис, 2017. – 224 с.

20. «Буллинг – причины, формы, профилактика» Методический материал (Для педагогов, воспитателей). Разработан: врачом-методистом Ларченко Н.А. Государственное казенное учреждение здравоохранения «Волгоградский областной центр медицинской профилактики». Волгоград, 2015.

21. Баева, И.А. Психологическая безопасность образовательной среды: учеб. пособие / под ред. И. А. Баевой. М., 2009.

22. Бочаров, М.И. Комплексное обеспечение информационной безопасности школьников. // Применение новых информационных технологий в образовании. 2009.

23. Как работать с комиксами проекта «Респект 2.0».
24. Левицкая, А. А. Региональные научно-образовательные центры европейской части России в области медиа-педагогики: сравнительный анализ / А. А. Левицкая // Дистанционное и виртуальное обучение. 2010. № 7. С.60-81.
25. Методические рекомендации по предотвращению буллинга (травли среди сверстников) в детских коллективах. Составители: А.Е. Довиденко, А.П. Третьякова, А.С. Мелях, Л.А. Губарева, М.В. Корба, Н.А. Алексеева, Н.В. Коровина, Т.П. Погадаева. - Екатеринбург, 2014.
26. Минин, А. Я. Информационные технологии в образовании: учеб. пособие. – М.: МПГУ, 2016. – 148 с.
27. Тоискин, В. С., Красильников В. В. Медиа-образование в информационно-образовательной среде: Учебное пособие. – Ставрополь: Изд-во СГПИ, 2009. -122с.
28. Федоров, А. В. Словарь терминов по медиа-образованию, медиа-педагогике, медиа-грамотности, медиа-компетентности. / Таганрог : Изд-во Таганрог. гос. пед. ин-та, 2010. – С. 25.
29. Челышева, И. В. Влияние современных масс-медиа на здоровье и развитие подрастающего поколения. / И. В. Челышева // Образование. Медиа. Общество. 2008. № 3. С.14-18.
30. Школа без насилия. Методическое пособие/Под ред. Н. Ю. Синягиной, Т.Ю. Райфшнайдер. — М.: АНО «ЦНПРО», 2015. — 150 с.

Интернет-ресурсы

31. Безопасный Интернет – детям! Полезные советы для тебя и твоих друзей. – Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd1/liflets_k_deti_06.pdf.
32. Безопасный интернет для детей: законодательство, советы, мнения, международный опыт [URL: http://i-deti.org/video/] (Дата обращения: 31.08.2018).
33. Веб-квест «Информационная безопасность» [URL: https://kopilkaurokov.ru/informatika/uroki/vieb-kviest-zashchita-informatsii-v-sieti-intierniet] (Дата обращения: 27.06.2018).
34. Вредоносные программы в Интернете. Правила поведения в Интернете. Безопасное использование электронной почты. Защита от вредоносных программ. –Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf.
35. Информационная безопасность образовательных учреждений [URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/] (Дата обращения: 28.06.2018).
36. Как защитить личные данные в Интернете [URL: https://lifehacker.ru/protecting-your-personal-data/] (Дата обращения: 03.09.2018)
37. Комикс «В темноте». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/246/.

38. Комикс «Всегда достается слабым?». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/207/.
39. Комикс «Мальчик из Швеции». Проект «RESPECT2.0» http://www.respect.com.mx/ru/comics/9/.
40. Комикс «Ощипанная птица». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/8/.
41. Комикс «Рыбный день». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/58/.
42. Комикс «Такой же, как и все». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/7/.
43. Комиксы из разных стран за респект и уважуху. Как работать с комиксами «РЕСПЕКТ». Методическое пособие для преподавателей и просветителей. – Воронеж, 2012 г. – 48 с. http://www.respect.com.mx/ru/technique/111/.
44. МВД РФ предупреждает! Пользователям интернета будьте осторожны! Мошенническое дублирование благотворительных сайтов. – Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf.
45. Методические рекомендации для образовательных учреждений по проведению родительского всеобуча на тему детской безопасности в Интернете. И.В. Вылегжанина – [Электронный ресурс] – Режим доступа: http://ozyorsk-shkola.ru/wp-content/uploads/2012/05/bezopasnost_rebjonka_v_informacionnom_obshhestve_copy.pdf.
46. Методическое пособие для преподавателей и просветителей http://www.respect.com.mx/ru/technique/191/.
47. Национальная стратегия действий в интересах детей на 2012 - 2017 годы [Электронный ресурс] URL:http://www.soprotivlenie.org.
48. Понятие и виды персональных данных [URL: https://otdelkadrov.online/5841-ponyatie-vidy-personalnyh-dannyh] (Дата обращения: 03.09.2018)
49. Сделайте Интернет безопасным для своих детей. – Google Центр безопасности. – [Электронный ресурс] – Режим доступа: http://www.google.ru/safetycenter/families/start/.
50. Уроки мобильной грамотности [URL:https://chelyabinsk.beeline.ru/customers/help/safe-beeline/ugrozy-mobilnykh-moshennikov/uroki-mobilnoi-gramotnosti/] (Дата обращения: 31.08.2018).
51. https://learningapps.org
52. https://www.youtube.com/watch?v=9OVdJydDMbg
53. https://rkn.gov.ru
54. https://pd.rkn.gov.ru/multimedia/video114.htm
55. http://персональныеданные.дети/
56. http://detionline.com/
57. http://сетевичок.рф/

8. ОПИСАНИЕ ФОРМЫ ПРОМЕЖУТОЧНОЙ И ИТОГОВОЙ АТТЕСТАЦИИ

В ходе реализации дополнительной профессиональной программы «Информационная безопасность в современном обществе» осуществляется диагностика, промежуточная аттестация и итоговая аттестация.

Диагностика, выявляющая уровень знаний и навыков владения содержанием программ, проводится в форме тестирования на начало и конец обучения (приложение). Диагностика рассчитана на определение субъективной позиции слушателей при освоении дополнительной профессиональной программы повышения квалификация, позволяет оценить возможные отдаленные результаты реализации этой программы. Содержание диагностики учитывает различия в подготовке слушателей, занимающихся педагогической и управленческой деятельностью. Результаты, полученные в ходе диагностики дают возможность принятия оперативных управленческих решений по обеспечению более высокого качества реализуемой образовательной программы. Данное тестирование проводится в онлайн-режиме.

Промежуточная аттестация проводится в форме выполнения практических заданий.

В случае полного и содержательного ответа на задание, слушатель получает отметку «зачтено» в случае, если вопрос не раскрыт, слушатель получает отметку «не зачтено».

Итоговая аттестация по дополнительной профессиональной программе «Информационная безопасность в современном обществе» проводится в форме представления итоговой выпускной работы по теме «Мероприятие по кибербезопасности для участников образовательных отношений». Слушатели делятся на 3-4 группы. Каждая группа разрабатывает проект мероприятия для выбранной путем жеребьевки категории участников образовательных отношений (обучающиеся, педагоги, родители (законные представители) обучающихся).

При подготовке проекта мероприятия в группе происходит обсуждение и выбор темы мероприятия, распределение ролей и зоны ответственности каждого члена команды.

Группы получают 16 часов (практические занятия) для разработки проекта мероприятия и его оформления в электронном формате.

Все мероприятия рекомендуется разрабатывать на основе правил работы в группе:

Правило добровольности. Каждый участник группы оставляет за собой право разглашения или неразглашения личной информации. Если участник мероприятия затрудняется сообщить о себе определенную личную информацию, он имеет право отказаться от выполнения задания. Тем не менее, это не означает полного отказа от участия в упражнении. Наравне со всеми он может выполнять упражнения, не предполагающие разглашения персональных данных, принимать участие в обсуждении результатов либо ограничиться частичным выполнением задания.

Правило конфиденциальности. Ничто из того, о чем говорится в группе относительно конкретных участников, не должно стать достоянием третьих лиц.

Это естественное этическое требование ответственного отношения к чужим персональным данным – базовое условие создания атмосферы доверия и безопасности в группе.

Принцип безоценочности. Задания, выполняемые в ходе мероприятия, не имеют правильных или неправильных ответов, поэтому педагог-модератор должен в первую очередь поощрять активность участников мероприятия, а не результаты выполнения задания. Все участники мероприятия должны, во-первых, избегать оценочных, в первую очередь негативных высказываний в отношении других детей, и, во-вторых, уважать точку зрения каждого участника.

Принцип бережного обращения с персональной информацией. Если выполнение задания предполагает сообщение участниками личной информации в письменном виде (заполнение различных бланков или опросников), ведущий после занятия должен удостовериться, что все материалы были либо уничтожены, либо попали обратно в руки к их владельцам, тем самым подчеркивая необходимость аккуратного обращения с персональными данными как в реальной жизни, так и в Интернете.

Представление проектов мероприятий для разных категорий участников образовательных отношений проходит на последнем занятии.

План защиты проекта мероприятия:

- Представление темы проекта мероприятия, категории участников.
- Обоснование формы проведения мероприятия.
- Освещение цели, задач и планируемых результатов мероприятия.
- Представление плана мероприятия.
- Презентация фрагмента мероприятия (проигрывание с аудиторией).
- Рефлексия.

Итоговая выпускная работа по теме «Мероприятие по кибербезопасности для участников образовательных отношений» включает в себя следующие компоненты:

– информационный (аннотация);

– методический (конспект занятия (урока)/организационно-управленческого мероприятия);

– технологический (презентация).

При условии соответствия всем требованиям, предъявляемым к итоговой выпускной работе предусмотрена пятибалльная система оценки.

Требования к итоговой работе.

Итоговая работа должна быть актуальной и востребованной, иметь возможность применения в практической деятельности, в том числе другими педагогами (возможность применения «как есть», т.е. без доработки, дополнительной консультации с автором).

В информационном компоненте (аннотации) указывается:

– Ф.И.О. слушателей;

– должность, преподаваемый предмет;

– вид итоговой выпускной работы;

– тема итоговой выпускной работы;

– категория участников мероприятия (родители (законные представители) обучающихся, педагоги, обучающиеся);

– компетенции, формируемые на мероприятии;

– форма проведения мероприятия.

Форму конспекта мероприятия слушатель выбирает самостоятельно с условием его дальнейшего использования в своей практической деятельности.

При подготовке текстового документа рекомендуется соблюдать следующие требования:

– *поля для всего документа*: верхнее и нижнее – по 2 см, левое – 3 см, правое – 1,5 см;

– *заголовки и титульная страница*: шрифт для заголовков – Times New Roman, 14-16 пт; стиль начертания – полужирный, без точки в конце заголовка (если он не состоит из двух предложений); выравнивание – по центру, без отступа в первой строке, интервал перед и после абзаца по 6 пт, междустрочный интервал – одинарный;

– *основной текст*: шрифт – Times New Roman, 12-14 пт.; выравнивание текста – по ширине; абзацный отступ в первой строке – 1,25 см; междустрочный интервал – одинарный или полуторный;

– в конспекте прослеживается связь с презентацией (указаны номера слайдов к каждому этапу/моменту мероприятия;

– текст конспекта выглядит аккуратно, пунктуационные отступы соблюдены, орфографических ошибок нет (отсутствует подчеркивание красной линией);

– в тексте присутствуют нумерованные/маркированные списки, таблицы и (или) изображения;

– выделение заголовков, применение в тексте полужирного, курсивного и подчеркнутого начертания обосновано;

– текстовый документ должен содержать информацию об авторах и тему итоговой работы.

Требования для качественной подготовки презентации:

– наличие титульного слайда в презентации (тема, информация об авторах);

– количество слайдов в презентации – не менее 10;

– в презентации присутствуют различные типы информации – графика, таблицы, изображения, текстовые блоки и т.д.;

– презентация выглядит аккуратно, дизайн выполнен в едином стиле, шрифты читабельны, изображения хорошего качества и т.д.;

– презентация является самодостаточным и/или дополняющим конспект материалом (отсутствует необоснованное дублирование текста конспекта);

При условии соответствия всем требованиям, предъявляемым к итоговой выпускной работе предусмотрена пятибалльная система оценки:

– отметка «2» – неудовлетворительно – выставляется если работа не сдана или имеет более 50% замечаний;

– отметка «3» – удовлетворительно – выставляется если работа частично соответствует требованиям (замечаний не более 50%);

– отметка «4» – хорошо – выставляется если работа соответствует

требованиям с некоторыми замечаниями (замечаний не более 75%);

– отметка «5» – отлично – выставляется если работа полностью соответствует требованиям.

По окончанию обучения по дополнительной профессиональной программе повышения квалификации «Информационная безопасность в современном обществе» слушатели получат удостоверение установленного образца.

СОСТАВИТЕЛИ ПРОГРАММЫ
«Новые возможности Microsoft Office 2016»

Ю.С. Бондарева, преподаватель МБУ ДПО «Центр развития образования города Челябинска.

Приложение

В ходе реализации дополнительной профессиональной программы «Информационная безопасность в современном обществе»» осуществляется диагностика по курсу

(полужирным шрифтом выделены правильные ответы)

1. Кто такой или что такое менеджер паролей?

a) Это сотрудник, который в крупных компаниях отвечает за надежность паролей.

b) Это программа, которая управляет данными доступа нескольких аккаунтов.

c) Это программа, которая позволяет преступникам распознавать чужие пароли.

2. Что такое фарминг (pharming)?

a) Способ обмана, с помощью которого пользователей перенаправляют на фиктивные сайты.

b) Процесс производства криптовалюты Биткоин низкооплачиваемыми работниками в больших производственных помещениях.

c) Массовая рассылка спама.

3. Кто такой или что такое Locky?

a) Известный в социальных сетях кот.

b) Программа, которая зашифровывает данные, за расшифровку которых вымогатели требуют выкуп.

c) Программа, с помощью которой можно индивидуально настроить блокировку экрана смартфона.

4. Каким из перечисленных путей вредоносные программы не могут сами установиться на компьютер?

a) Скачиванием и открытием файла.

b) Нажатием на ссылку.

c) Подключением классического блока питания.

5. Как я могу узнать, что соединение с веб-сайтов защищено?

a) Никак.

b) В строке ввода появляется символ навесного замка и приставка httpss://.

c) В окне браузера появляется звездочка.

6. Каким законом регулируются отношения, связанные с обработкой персональных данных?

a) «О защите информации».

b) «О персональных данных».

c) «О конфиденциальной информации».
d) «Об утверждении перечня сведений конфиденциального характера».

7. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т.д. это:

a) Исправление персональных данных.
b) Работа с персональными данными.
c) Обработка персональных данных.
d) Изменение персональных данных.

8. Персональные данные это:

a) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу.
b) Фамилия, имя, отчество, адрес проживания физического лица.
c) Год, месяц, дата и место рождения, адрес физического лица.
d) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна».

9. Каким должен быть пароль пользователя?

a) Содержать только цифры или только буквы.
b) Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.).
c) Быть простым и легко запоминаться, например, «123», «111», «qwerty» и т.д.
d) Содержать цифры и буквы, знаки препинания и быть сложным для угадывания.

10. Доступ к информации – это:

a) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
b) Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.
c) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.
d) Возможность получения информации и ее использования.