Государственное бюджетное учреждение
дополнительного профессионального образования
«Санкт-Петербургский центр оценки качества образования
и информационных технологий»

ПРИНЯТА
Научно-методическим Советом

(протокол от 15.12.2022 № 5)

УТВЕРЖДЕНА
Директор ГБУ ДПО «СПбЦОКОиИТ»

_____П.С. Розов

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Цифровая гигиена и кибербезопасность в ЭИОС

Автор:
Туманов И.А.

Санкт-Петербург
2022 год

Пояснительная записка

Дополнительная профессиональная программа повышения квалификации “Цифровая гигиена и кибербезопасность в ЭИОС” (далее - программа) предназначена для использования в системе повышения квалификации педагогических работников образовательных организаций.

Программа предназначена для повышения у педагогов образовательных учреждений цифровой компетентности в области цифровой гигиены и кибербезопасности, формирования профессиональных компетенций, необходимых для противодействия и профилактики деструктивного и аутодеструктивного поведения несовершеннолетних в сети Интернет, и повышения информационной безопасности в электронной информационной образовательной среде.

Содержание образовательной программы учитывает требования профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», «Педагог-психолог (психолог в сфере образования)», «Педагог дополнительного образования детей и взрослых».

Программа ориентирована на педагогов образовательных организаций.

Программа рекомендована для слушателей, прошедших подготовку в области ИКТ на уровне общепользовательской ИКТ-компетентности.

Программа реализуется с использованием электронного обучения.

Цель реализации программы - совершенствование компетенции в области планирования и обеспечения информационной безопасности образовательной организации.

Объем (срок освоения) программы - 18 часов.
Форма обучения: очная.

Планируемые результаты обучения:

Программа направлена на совершенствование следующих профессиональных компетенций:

Модули программы	Задачи профессиональной деятельности (ЗПД)	Профессиональные компетенции (ПК), подлежащие развитию
М1. Информационная безопасность в образовательной организации	Обеспечивать безопасность обработки персональных данных. Обеспечивать информационную безопасность организации образовательной деятельности.	ПК2. Способность использовать возможности информационно-образовательной среды. ПК3. Способность работать с информацией в компьютерных сетях. ПК5. Способность использовать современные информационные технологии в управлении образованием.

В соответствии с указанным выше профессиональным стандартом (- ами) в результате освоения программы слушатель должен приобрести следующие знания и умения:

слушатель должен знать:

- нормативные документы в области образования;
- нормативные документы по обеспечению информационной безопасности;
- нормативные документы в области управления образованием;
- основы работы с персональными данными.

слушатель должен уметь:

- использовать нормативные документы в профессиональной деятельности;

Учебный план

Тема	Всего часов	В том числе		Форма аттестации
		Лекции	Практические занятия	
Тема 1. Информационная безопасность. Государственное регулирование в сфере информационной безопасности	2	2	-	
Тема 2. Угрозы информационной безопасности	4	3	1	
Тема 3. Защита обучающихся от неправомерной информации	3	2	1	
Тема 4. Формирование и развитие навыков цифровой гигиены у обучающихся	4	2	2	
Тема 5. Обеспечение безопасности персональных данных	3	3	-	
Итоговая аттестация	2	-	2	Зачет
ИТОГО	**18**	**12**	**6**	

Календарный учебный график

Общая продолжительность обучения составляет одна – четыре недели в зависимости от расписания занятий.

Режим аудиторных занятий: 5-8 академических часов в день, 1-6 дней в неделю.

Дата начала обучения определяется по мере комплектования групп, и на каждую группу составляется календарный учебный график по форме приложения.

Организационно-педагогические условия

Квалификация педагогических кадров

Обучение по данной программе осуществляется старшими преподавателями, имеющим опыт методической или практической деятельности по тематике курса и опыт работы с техническими и программными средствами, использующимися при реализации программы.

Материально-технические условия реализации программы

Техническое обеспечение

- аудитория для проведения лекционных занятий, снабженная компьютером и мультимедийным оборудованием для презентаций;
- рабочие станции слушателей и преподавателя, объединенные в локальную компьютерную сеть, с возможностью работы с мультимедиа, доступом к учебному серверу и выходом в Интернет;

Программное обеспечение:

1. Интернет-браузеры.
2. ПО для просмотра файлов в формате pdf
3. Мультимедийный проигрыватель.

Учебно-методическое обеспечение программы

Основная литература:

1. Туманов И.А., Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет. [Текст] / Сост.: Туманов И.А., Дорофеева Т.В.- СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. – 39 с.

Рекомендованная литература:

1. Указ Президента Российской Федерации “Об утверждении Доктрины информационной безопасности Российской Федерации” №646 от 5 декабря 2016 года.
2. Указ Президента Российской Федерации “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” №203 от 9.05.2017 г.
3. Федеральный закон “Об информации, информационных технологиях и защите персональных информации” № 149-ФЗ от 27.07.2006 г.
4. Федеральный закон “О персональных данных” № 152-ФЗ от 27.07.2006 г.
5. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» № 687 от 15.09.2008 г.
6. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01.11.2012 г.
7. Солдатова Г. У., Чигарькова С. В., Дренёва А. А., Илюхина С. Н. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. – 176 с.
8. Солдатова Г. У., Рассказова Е. И., Нестик Т. А. Цифровое поколение России: компетентность и безопасность. — Смысл Москва, 2017. — 375 с.
9. Солдатова Г. У., Рассказова Е. И. Безопасность подростков в Интернете: риски, совладание и родительская медиация // Национальный психологический журнал. — 2014. — № 3 (15). — С. 39-51.

Общие требования к организации образовательного процесса

Процесс обучения осуществляется с позиций андрагогики, т.к. одной из важных особенностей обучения взрослых является получение дополнительных знаний и совершенствование профессиональных умений на основе осмысления ими собственной деятельности. Одним из важнейших условий реализации данной программы является активная позиция каждого слушателя, его инициатива, осмысление собственного опыта. При проведении занятий используются следующие педагогические технологии: технологии

развития критического мышления, технологии коллективного обучения, технологии реализации системно-деятельностного подхода.

Форма аттестации и контроля

Контроль достижения планируемых результатов обучающихся по программе осуществляется следующим образом:

- итоговая аттестация в форме устного зачёта.

Оценочные материалы

ПАСПОРТ ОЦЕНОЧНОГО СРЕДСТВА

1. Текущий контроль

Текущий контроль знаний слушателей проводится посредством выполнения практических работ. Практические работы считаются выполненными, если слушатель самостоятельно (или в основном самостоятельно) выполнил задания с незначительными замечаниями, при этом оценка не выставляется.

Тематика практических работ:

- *Практическая работа 1 «Создание глоссария киберугроз»*
- *Практическая работа 2 «Анализ ситуаций по работе с персональными данными в трудовой деятельности»*
- *Практическая работа 3 «Исследование цифрового имиджа образовательной организации»*

2. Промежуточная аттестация

Не предусмотрена.

3. Итоговая аттестация

Итоговая аттестация осуществляется в форме устного зачёта.

Основные вопросы устного зачета:

1. Требования федерального законодательства к обеспечению информационной безопасности в образовательной организации.
2. Угрозы информационной безопасности.
3. Виды цифровых компетенций.
4. Алгоритмы профилактики деструктивного поведения несовершеннолетних для педагогов и родителей.
5. Особенности обработки персональных данных без использования средств автоматизации.
6. Обеспечение безопасности обработки персональных данных в информационных системах персональных данных.
7. Обеспечение информационной безопасности при доступе к сетям общего доступа.
8. Особенности получения согласий на обработку персональных данных.

Критерии оценки устного ответа:

“Зачтено” выставляется слушателю в том случае, если:

- ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений;
- полно раскрываются причинно-следственные связи между требованиями федерального законодательства, регулирующего организацию информационной безопасности в образовательной организации и мерами, которые необходимо

принять в образовательной организации для приведения системы работы в соответствие установленным требованиям;
- делаются обоснованные выводы, демонстрируются глубокие знания базовых нормативно-правовых актов, особенностей организации работы по обеспечению информационной безопасности образовательной организации.

“Не зачтено” выставляется слушателю в том случае, если:
- ответы на поставленные вопросы излагаются с нарушением последовательности и логики изложения, требуют дополнительных пояснений;
- не раскрыты причинно-следственные связи между требованиями федерального законодательства, регулирующего организацию информационной безопасности в образовательной организации и мерами, которые необходимо принять в образовательной организации для приведения системы работы в соответствие установленным требованиям;
- не сделаны обоснованные выводы, слушатель демонстрирует поверхностные знания базовых нормативно-правовых актов, особенностей организации работы по обеспечению информационной безопасности образовательной организации.

По завершении курса слушателям предлагается заполнить рефлексивную анкету по итогам обучения по данной ДПП.