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

ПРИНЯТА
Научно-методическим Советом

(протокол от 27.08.2021 № 1)

УТВЕРЖДЕНА
Директор ГБУ ДПО «СПбЦОКОиИТ»

_____ А.Б. Федосов

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Информационная безопасность в образовательной организации

Авторы:
Дорофеева Т.В.,
Туманов И.А.

Санкт-Петербург
2021 год

Пояснительная записка

Дополнительная профессиональная программа повышения квалификации “Информационная безопасность в образовательной организации” (далее - программа) предназначена для использования в системе повышения квалификации педагогических работников образовательных организаций.

Программа предназначена для подготовки слушателей к выполнению трудовых функций, связанных с управлением информационной безопасностью образовательной организации и предусматривает изучение:

- основных направлений обеспечения информационной безопасности образовательной организации;
- основных направлений государственного регулирования в направлении обеспечения информационной безопасности;
- технических и программных средств обеспечения информационной безопасности образовательной организации;
- организационных требований к обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- организационных требований к обеспечению информационной безопасности персональных данных, обрабатываемых без использования ИСПДн.

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», «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования».

Программа ориентирована на руководителей, заместителей руководителей 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 компетенций 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	ПК2. Способность использовать возможности информационно-образовательной среды. ПК3. Способность работать с информацией в компьютерных

	образовательной деятельности. Организовывать разработку локальных нормативных актов образовательной организации.	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;
- компоненты компьютерных сетей;
- нормативные документы в области управления образованием;
- способы контроля и оценки качества образования;
- средства организации контроля и мониторинга с использованием ИКТ-инструментов;
- основы работы с персональными данными.

слушатель должен уметь:

- использовать нормативные документы в профессиональной деятельности;
- проектировать логическую и физическую схему сети;
- настраивать сетевое оборудование;
- анализировать нормативные документы, использовать их для формирования и реализации управленческих стратегий;
- использовать современные информационные технологии в управлении;
- осуществлять контроль эффективности использования современных технологий в управлении образованием;
- оценивать эффективность использования средств информатизации;
- проектировать электронное образовательное пространство ОО;
- проектировать локальные нормативные акты, регламентирующие процессы информатизации в ОО.

Учебный план

Тема	**Всего часов**	**В том числе**		**Форма аттестации**
		Лекции	**Практические занятия**	
Модуль 1. Информационная безопасность в образовательной организации				
Тема 1. Информационная безопасность. Государственное регулирование в сфере информационной безопасности.	3	3	-	
Тема 2. Угрозы информационной безопасности.	2	1	1	

Тема 3. Обеспечение информационной безопасности персональных данных, обрабатываемых в ИСПДн.	3	2	1	
Тема 4. Обеспечение информационной безопасности персональных данных, обрабатываемых без использования ИСПДн.	3	2	1	
Тема 5. Обеспечение безопасности при доступе к сетям общего пользования	3	3	-	
Тема 6. Организация работы по обеспечению информационной безопасности в образовательной организации	2	1	1	
Тема 7. Итоговая аттестация	2	-	2	
ИТОГО	**18**	**12**	**6**	**Устный зачет**

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, уровень компетентности которых соответствует требованиям к должности по единому квалификационному справочнику, имеющим 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: Google Chrome, Mozilla Firefox.
2. ПО для просмотра файлов в формате pdf (Adobe Acrobat Reader или аналог)
3. Мультимедийный проигрыватель: WindowsMediaPlayer, VLC или другой.

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. Постановление правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» № 211 от 21 марта 2012 г.
8. Приказ ФСТЭК России “Об утверждении состава и содержания организационных и техническим мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” №21 от 18.02.2013 г.
9. Приказ ФСТЭК России “Об утверждении Требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах” № 17 от 11.02.2013 г.
10. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России № 282 от 30.08.2002 г.
11. Письмо Министерства образования и науки Российской Федерации «Об обеспечении защиты персональных данных» № 17-110 от 29.07.2009.
12. Информационное сообщение ФСТЭК № 240/22/2637.
13. Методический документ. Меры защиты информации в государственных информационных системах" (утв. ФСТЭК России 11.02.2014).

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

Тематика практических работ:

Практическая работа 1 «Анализ мер защиты информации в ИСПДн»:

- задание на выбор мер защиты для 4 УЗ из приказа ФСТЭК №21;
- задание на расшифровку выбранных мер защиты по документу ФСТЭК «Меры защиты информации в ГИС»

Практическая работа 2 «Подготовка документов по использованию сети Интернет»:

- задание на создание комплекта нормативных документов уровня образовательной организации по использованию сети Интернет на основе предлагаемых шаблонов;

Практические работы считаются выполненными, если слушатель самостоятельно (или в основном самостоятельно) выполнил задания с незначительными замечаниями, при этом оценка не выставляется.

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. Алгоритм проектирования модели угроз образовательной организации.
3. Информационные системы обработки персональных данных. Обеспечение безопасности обработки персональных данных в ИСПДн.
4. Особенности обработки персональных данных без использования средств автоматизации.
5. Обеспечение информационной безопасности при доступе к сетям общего доступа.
6. Планирование работы по обеспечению информационной безопасности образовательной организации.
7. Подготовка организационно-распорядительной документации по обеспечению информационной безопасности.

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.