Приложение 9
к приказу ГБУ ДПО РЦОКИО
от 28.09.2022 № 513-ОД

Учебный план
дополнительной профессиональной программы
(программы повышения квалификации)

Обеспечение информационной безопасности организации

Цель: получение в области защиты информации и допуска к работе со средствами криптографической защиты информации, обновление и совершенствование имеющихся теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности организации.

Категория слушателей: педагогические работники образовательных организаций, специалисты по защите информации, должностные лица, ответственные за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, специалисты, ответственные за организацию обработки персональных данных, специалисты, ответственные за обеспечение безопасности персональных данных в информационных системах, пользователи средств криптографической защиты информации.

Трудоемкость программы: 40 часов.

Форма обучения: очная, очная с использованием электронного обучения, дистанционных образовательных технологий.

Календарный учебный график: количество дней определяется трудоемкостью из расчета 8 часов в день, стационарное и дистанционное обучение.

№ п/п	Наименование разделов	Трудоемкость программы, ч.	Форма контроля
		40	
1.	Основы информационной безопасности	6	Входная диагностика
2.	Обработка персональных данных	26	
3.	Защита информации ограниченного доступа с использованием средств криптографической защиты информации	6	Итоговая диагностика
4.	Итоговая аттестация	2	Тест
	ИТОГО	40	

Учебно-тематический план
дополнительной профессиональной программы
(программы повышения квалификации)

Обеспечение информационной безопасности организации

Цель: получение новой компетенции в области защиты информации и допуска к работе со средствами криптографической защиты информации, обновление и совершенствование имеющихся теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности организации.

Категория слушателей: педагогические работники образовательных организаций, специалисты по защите информации, должностные лица, ответственные за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, специалисты, ответственные за организацию обработки персональных данных, специалисты, ответственные за обеспечение безопасности персональных данных в информационных системах, пользователи средств криптографической защиты информации.

Трудоемкость программы: 40 часов.

Форма обучения: очная, очная с использованием электронного обучения, дистанционных образовательных технологий

Календарный учебный график: 5 дней, 8 часов в день, стационарное и дистанционное обучение.

№ п/п	Наименование разделов и тем	Всего часов	В том числе:					Формы контроля
			Лекции	Практические, лабораторные, семинарские занятия	Очно, в том числе стажировка	Дистант	Самостоятельная работа	
1.	**Основы информационной безопасности**	**6**	**5**	**1**	**6**	**6**		
1.1	Основные понятия	2	2		2	2		Входная диагностика
1.2	Нормативно-правовые основы обеспечения информационной безопасности в Российской	4	3	1	4	4		

№ п/п	Наименование разделов и тем	Всего часов	В том числе:					Формы контроля
			Лекции	Практические, лабораторные, семинарские занятия	Очно, в том числе стажировка	Дистант	Самостоятельная работа	
	Федерации							
2.	**Обработка персональных данных**	**26**	**17**	**9**	**26**	**26**		
2.1	Принципы и условия обработки персональных данных	3	2	1	3	3		
2.2	Права субъекта персональных данных	1	1		1	1		
2.3	Обязанности оператора	19	13	6	19	19		
2.4	Федеральный государственный контроль (надзор) за обработкой персональных данных	1	1		1	1		
2.5	Ответственность за нарушение законодательства Российской Федерации в области персональных данных	2		2	2	2		
3.	**Защита информации ограниченного доступа с использованием средств криптографической защиты информации**	**6**	**3**	**3**	**6**	**6**		
3.1.	Нормативные правовые акты Российской Федерации по эксплуатации средств криптографической защиты информации, об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с их использованием конфиденциальной информации	2		2	2	2		
3.2.	Электронная подпись	2	2		2	2		
4.6	Эксплуатация средств	2	1	1	2	2		Итоговая

№ п/п	Наименование разделов и тем	Всего часов	В том числе:					Формы контроля
			Лекции	Практические, лабораторные, семинарские занятия	Очно, в том числе стажировка	Дистант	Самостоятельная работа	
	криптографической защиты информации							диагностика
	Итоговая аттестация	**2**			**2**	**2**		**Тест**
Итого		**40**	**25**	**13**	**40**	**40**		

Всего: кол-во часов по учебному плану – 100 ч.

9) Аудиторные занятия, включая дистанционные образовательные технологии: ч.

из них:

– теоретические – 25 ч., в том числе с применением электронного обучения (дистанционных образовательных технологий) – 25 ч.;

– практические – 13 ч., в том числе с применением электронного обучения (дистанционных образовательных технологий) – 13 ч.

– итоговая аттестация – 2 ч., в том числе с применением электронного обучения (дистанционных образовательных технологий) – 2 ч.;

2) Внеаудиторные занятия: 60 ч.

из них:

– проведение входной и итоговой диагностики – 30 ч. (из расчета 1,0 час на 1 слушателя, при средней наполняемости 30 чел. в группе);

– проверка работ итоговой аттестации слушателей – 30 ч. (из расчета 1,0 час на 1 слушателя, при средней наполняемости 30 чел. в группе).

Планируемые результаты обучения слушателей дополнительной профессиональной программы (программы повышения квалификации)

Обеспечение информационной безопасности организации

Трудовая функция	Трудовые действия	Знания	Умения
применение	принятие правовых,	содержание	планировать

навыков использования определённых нормативных и правовых документов в ходе решения задач, связанных с обеспечением информационной безопасности и обработкой информации; разработка технических требований и технических заданий на защищаемые информационные системы; выявление возможных источников и каналов утечки информации.	организационных и технических мер по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных; разработка технических заданий на создание системы и (или) модели угроз безопасности информации, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;	основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных; процедуры задания и реализации требований по защите информации в информационных системах персональных данных; меры обеспечения безопасности персональных данных; требования по обеспечению безопасности персональных данных; порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их	мероприятия по обеспечению безопасности персональных данных; разрабатывать необходимые документы по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных;

	разработка предложений по совершенствованию и повышению эффективности принимаемых мер по защите персональных данных; защита информации ограниченного доступа с использованием средств криптографической защиты информации.	обработке в информационных системах персональных данных; нормативные правовые акты Российской Федерации по эксплуатации средств криптографической защиты информации, об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с их использованием конфиденциальной информации	определять уровень защищенности персональных данных; выявлять угрозы безопасности персональных данных при их обработке в информационных системах персональных данных; эксплуатировать средства криптографической защиты информации.