УТВЕРЖДАЮ

Директор ОАУ «ИРКП»

_____ И.Н. Ускова

«05» июня 2024 г.

ПРОГРАММА
дополнительного профессионального образования
повышения квалификации

Информационная безопасность
(72 академических часа)

Белгород, 2024

Областное автономное учреждение
«Институт региональной кадровой политики»

УТВЕРЖДАЮ
Директор ОАУ «ИРКП»
_____ И.Н. Ускова
«05» июля 2024 г.

ПРОГРАММА
дополнительного профессионального образования
повышения квалификации

«Информационная безопасность»

Разработчики программы:
Киселев Андрей Леонидович, старший преподаватель кафедры ПОВТиАС БГТУ им. В. Г. Шухова;
Гаврющенко Александр Павлович, кандидат технических наук кафедры ПОВТиАС, доцент БГТУ им. В. Г. Шухова;
Зуев Сергей Валентинович, кандидат физико-математических наук, доцент кафедры ПОВТиАС БГТУ им. В. Г. Шухова.

Составители учебно-тематического плана программы:
Киселев Андрей Леонидович, старший преподаватель кафедры ПОВТиАС БГТУ им. В. Г. Шухова;
Гаврющенко Александр Павлович, кандидат технических наук кафедры ПОВТиАС, доцент БГТУ им. В. Г. Шухова;
Зуев Сергей Валентинович, кандидат физико-математических наук, доцент кафедры ПОВТиАС БГТУ им. В. Г. Шухова.

Рассмотрена на заседании экспертной группы

Протокол № 30 от «05» июля 2024 г.

Белгород, 2024

УЧЕБНЫЙ ПЛАН

Цель: совершенствование и получение новых компетенций, необходимых для осуществления профессиональной деятельности, повышение профессионального уровня в рамках имеющейся квалификации государственных гражданских служащих, работающих в области по обеспечению безопасности данных при их обработке в информационных системах.

Задачи: изучить определение угроз безопасности данных, формирование требований к обеспечению безопасности данных при их обработке в ИС (формирование требований к системе защиты данных), внедрение организационных и технических мер, а также реализуемых ими мероприятий по обеспечению безопасности данных при их обработке в ИС (внедрение системы защиты данных).

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Категории слушателей, на обучение которых рассчитана программа дополнительного профессионального образования (далее – программа): дипломированные специалисты (бакалавры, магистры) в сфере управления, государственные служащие, лица, включенные в резерв управленческих кадров.

1.2. Сфера применения слушателями полученных профессиональных компетенций, умений и знаний.
Полученные в ходе повышения квалификации профессиональные компетенции, умения и знания предназначены для их применения в своей деятельности, направленную на обеспечение исполнения основных функций.

2. ХАРАКТЕРИСТИКА ПОДГОТОВКИ ПО ПРОГРАММЕ

2.1. Нормативный срок освоения программы: 72 академических часа.
2.2. Режим обучения: не менее 4 часов в день.
2.3. Форма обучения: очная с применением сетевой формы реализации и дистанционных образовательных технологий и электронного обучения.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ

Слушатель, освоивший программу, должен:
3.1. обладать: способность использовать нормативные правовые акты, методические документы в области обеспечения безопасности данных при их обработке и национальные стандарты в области защиты информации в своей профессиональной деятельности (ПК-1);
- способность использовать достижения науки и техники, пользоваться реферативными и справочно-информационными изданиями в области защиты информации (ПК-2);
- способность формировать требования к обеспечению безопасности данных при их обработке в ИС (формировать требования к системе защиты данных) (ПК-3);
3.2. владеть: навыками работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности данных, планирования мероприятий по обеспечению безопасности данных, внедрения организационных и технических мер по обеспечению безопасности данных, работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения.
3.3.уметь: устанавливать требования по обеспечению безопасности данных при их обработке, разрабатывать модели угроз безопасности данных по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей ИС, возможных способов реализации угроз безопасности и последствий от их реализации,

анализа банка данных угроз безопасности информации, определять параметры настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности данных, разрабатывать документы для проведения работ по аттестации на соответствие требованиям о защите информации.

3.4. знать: нормативные правовые акты, методические документы в области обеспечения безопасности данных при их обработке и национальные стандарты в области защиты информации, основные понятия в области обеспечения безопасности данных при их обработке, основы построения систем защиты данных, требования к созданию систем защиты данных и обеспечению их функционирования.

4. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

График обучения / Форма обучения	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность обучения (дней)**
Очная с применением сетевой формы реализации и дистанционных образовательных технологий и электронного обучения.	4-7	6	14

5. ТРЕБОВАНИЯ К СТРУКТУРЕ ПРОГРАММЫ

Таблица 1

Учебный план
дополнительной профессиональной программы повышения квалификации
«Информационная безопасность»

№ п/п	Наименование модулей, дисциплин, разделов	Всего, час.	В том числе:			Форма контроля
			Лекции	Практические занятия (семинары), тренинги	Самостоятельная работа	
1.	2.	3.	4.	5.	6.	7.
1.	**Модуль 1. «Основы обеспечения безопасности объектов»**	**20**	**8**	**4**	**8**	
2.	**Модуль 2. «Организация работ по обеспечению безопасности объекта»**	**40**	**20**	**6**	**14**	
3.	**Модуль 3. «Контроль за обеспечением безопасности объекта»**	**10**	**6**	**2**	**2**	
	Итоговая аттестация	**2**		**2**		**Тестирование**
	ИТОГО	**72**	**34**	**14**	**24**	

Таблица 2

Учебно-тематический план
дополнительной профессиональной программы повышения квалификации
«Информационная безопасность»

№ п/п	Наименование модулей, дисциплин, разделов, тем	Всего, час.	В том числе:			
			Лекции	Практические занятия (семинары), тренинги	Самостоятельная работа	Форма контроля
1.	2.	3.	4.	5.		6.
1.	**Модуль 1. «Основы обеспечения безопасности объектов»**	**20**	**8**	**4**	**8**	
1.1	Правовые основы обеспечения безопасности	8	2	2	4	
1.2	Угрозы безопасности информации, обрабатываемой на объектах	12	6	2	4	
2.	**Модуль 2. «Организация работ по обеспечению безопасности объекта»**	**40**	**20**	**6**	**14**	
2.1	Категорирование объектов по ИБ	10	4	2	4	
2.2	Требования по обеспечению безопасности объектов	14	8	2	4	
2.3	Система безопасности объекта	10	4	2	4	
2.4	Стадии (этапы) работ по созданию систем безопасности	6	4		2	
3.	**Модуль 3. «Контроль за обеспечением безопасности объекта»**	**10**	**6**	**2**	**2**	
3.1	Контроль за обеспечением безопасности объекта	10	6	2	2	
	Итоговая аттестация	**2**		**2**		**Тестирование**
	ИТОГО	**72**	**34**	**14**	**24**	

6. ТРЕБОВАНИЯ К МИНИМУМУ СОДЕРЖАНИЯ ПРОГРАММЫ

Таблица 3

6.1. Учебная программа

№ п/п	Наименование темы	Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы
1.	Модуль 1. «Основы обеспечения безопасности объектов»	Правовые основы обеспечения безопасности. Угрозы безопасности информации, обрабатываемой на объектах
2.	Модуль 2. «Организация работ по обеспечению безопасности объекта»	Категорирование объектов по ИБ. Требования по обеспечению безопасности объектов. Система безопасности объекта. Стадии (этапы) работ по созданию систем безопасности
3.	Модуль 3. «Контроль за обеспечением безопасности объекта»	Контроль за обеспечением безопасности объекта
4.	Практические занятия (семинары)	Правовые основы обеспечения безопасности. Угрозы безопасности информации, обрабатываемой на объектах. Категорирование объектов по ИБ. Требования по обеспечению безопасности объектов. Система безопасности объекта. Стадии (этапы) работ по созданию систем безопасности. Контроль за обеспечением безопасности объекта
5.	Самостоятельная работа	Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием учебных вопросов, а также методических пособий и литературы, необходимых для усвоения учебного материала. В ходе самостоятельной работы обучающиеся получают консультации у преподавателей.
6.	Используемые образовательные технологии	Лекции, практические занятия, самостоятельная работа с применением сетевой формы реализации и дистанционных образовательных технологий и электронного обучения
7.	Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы	Язов Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа. Монография / Ю.К. Язов, С.В. Соловьев – Воронеж: Кварта, 2018. – 588 с. б) дополнительная литература : Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.). Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О данных». Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом

		регулировании». Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Перечень сведений конфиденциального характера. Утвержден Указом Президента Российской Федерации от 6 марта 1997 г. № 188. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами. Утвержден постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211. Требования к защите данных при их обработке в информационных системах данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. Положение о банке данных угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. Состав и содержание организационных и технических мер по обеспечению безопасности данных при их обработке в информационных системах данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

		Базовая модель угроз безопасности данных при их обработке в информационных системах данных. Утверждена ФСТЭК России 15 февраля 2008 г. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. Методический документ. Методика тестирования обновлений безопасности программных, программно-аппаратных средств. Утвержден ФСТЭК России 28 октября 2022 г. Методический документ. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. Утвержден ФСТЭК России 28 октября 2022 г. Об утверждении методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 31 мая 2013 г № 127. Об утверждении образца формы уведомления об обработке данных. Приказ Федеральной службы по надзору в сфере связи и массовых коммуникаций от 17 июля 2008 г. № 08. ГОСТ Р 2.610-2019 ЕСКД. Правила выполнения эксплуатационных документов. Ростехрегулирование, 2019. ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. Росстандарт,2021. ГОСТ 34.602-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Росстандарт, 2021. ГОСТ Р 59792-2021 Информационные технологии. Виды испытаний автоматизированных систем. Росстандарт, 2021. ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Росстандарт, 2021. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения. Росстандарт, 2019. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021. ГОСТ Р ИСО/МЭК 27001-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Росстандарт, 2021; программное обеспечение: БДУ – программа ScanOVAL [Электронный ресурс]. Режим доступа – https://bdu.fstec.ru/site/scanoval свободный. Загл. с экрана. – Яз.рус.;

		базы данных, информационно-справочные и поисковые системы: www.pravo.gov.ru, www.fstec.ru, www.gost.ru/wps/portal/tk362/, www.bdu.fstec.ru; правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

Тематика практических работ и перечень вопросов для самостоятельного обучения уточняются при составлении рабочих программ преподавателями.

7. ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММ

Формой и методом контроля и оценки результатов освоения тем является успешное прохождение (более 70% правильных ответов) итогового тестирования. Срок выполнения итоговой аттестации – 2 академических часа.

По результатам освоения программы дополнительного профессионального обучения выдается удостоверение о повышении квалификации.