Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Среднерусский институт управления – филиал
Кафедра «Математика и информационные технологии»

Щеголев Александр Владимирович

Подписан: Щеголев Александр Владимирович
DN: C=RU, S=Орловская область, T=исполняющий обязанности директора, OU="СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", СНИЛС=13950729986, ИНН=575208091607, E=it@orel.ranepa.ru, G=Александр Владимирович, SN=Щеголев, CN=Щеголев Александр Владимирович
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: Среднерусский институт управления

УТВЕРЖДЕНА
ученым советом Среднерусского института управления – филиала РАНХиГС
Протокол от «24» февраля 2025 г. №1

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

«Информационная безопасность в деятельности органов государственной власти. Организация работы с персональными данными»

72 часа

Орел, 2025

Разработчики:

кандидат педагогических наук, доцент,
доцент кафедры «Математика
и информационные технологии» _____ А.Г. Савина

кандидат педагогических наук, доцент,
доцент кафедры «Математика
и информационные технологии» _____ А.А. Музалевская

Руководитель программы:
кандидат педагогических наук, доцент,
доцент кафедры «Математика
и информационные технологии» _____ А.А. Музалевская

Руководитель структурного подразделения
кандидат педагогических наук, доцент,
и.о. заведующего кафедрой «Математика
и информационные технологии» _____ А.Г. Савина

Дополнительная профессиональная программа рассмотрена и одобрена на заседании ученого совета Среднерусского института управления – филиала РАНХиГС «24» февраля 2025 г., протокол №1.

СОДЕРЖАНИЕ

1. Общая характеристика программы 4
1.1. Цель и задачи реализации программы 4
1.2. Нормативная правовая база 4
1.3. Планируемые результаты обучения 6
1.4. Категория слушателей 8
1.5. Формы обучения и сроки освоения 8
1.6. Период обучения и режим занятий 9
1.7. Документ о квалификации 9
2. Содержание программы 9
2.1. Календарный учебный график 9
2.2. Учебный план 9
2.3 Содержание программы по модулям/разделам/дисциплинам и (или) темам 12
3. Организационно-педагогические условия реализации программы 14
3.1 Кадровое обеспечение 14
3.2 Материально-техническое и программное обеспечение реализации программы 16
3.3 Учебно-методическое и информационное обеспечение программы 17
4. Оценка качества освоения программы 21
4.1. Формы и объем текущего контроля 21
4.2. Формы и объем итоговой аттестации 30
4.3. Критерии оценки итоговой аттестации 37

1. Общая характеристика программы

1.1. Цель реализации программы

Цель реализации программы «Информационная безопасность в деятельности органов государственной власти. Организация работы с персональными данными» состоит в обеспечении сформированности компетенций, позволяющих обучающимся эффективно решать профессиональные задачи в области обеспечения информационной безопасности общества, государственных и муниципальных органов власти, личности, задач по управлению рисками информационной безопасности в условиях институциональных изменений и цифровых трансформаций, с учетом динамики социально-экономических процессов и новых требований к качеству управления. В результате освоения программы обучающиеся приобретут новые компетенции по выполнению профессиональных трудовых функций по обеспечению информационной безопасности, в том числе защите персональных данных.

1.2. Нормативная правовая база

Программа повышения квалификации «Информационная безопасность в деятельности органов государственной власти. Организация работы с персональными данными» сформирована в соответствии с требованиями:

– Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

– Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

– Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указа Президента Российской Федерации от 22 мая 2015 г. №260 «О некоторых вопросах информационной безопасности Российской Федерации»;

– Указа Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Указа Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;

–Национального проекта «Экономика данных и цифровая трансформация государства» (утв. протоколом заочного голосования членов президиума

Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 г. №12пр.);

– постановления Правительства Российской Федерации от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения стандартов» (ред. от 23.09.2014 г.);

– справочника квалификационных требований к специальностям, направлениям подготовки (к укрупненным группам специальностей и направлений подготовки), к профессиональному уровню, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих (письмо Минтруда России от 26.04.2017 N 18-1/10/В-3260 «О разработке справочника квалификационных требований к специальностям, направлениям подготовки, знаниям и умениям, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих»);

– справочника типовых квалификационных требований для замещения должностей муниципальной службы (письмо Минтруда России от 15 июля 2016 г. N18-1/10/В-4800 «Высшие органы исполнительной власти субъектов Российской Федерации»);

– методических рекомендаций - разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки ВК-1032/06 от 22.04.2015);

– приказа РАНХиГС «Об утверждении Порядка разработки и утверждения в РАНХиГС дополнительных профессиональных программ – программ профессиональной переподготовки, программ повышения квалификации» №02-835 от 13.08.2021 г. (с измен. и доп. от 30.06.2023г. и 06.12.2023г.);

– приказа РАНХиГС «Об утверждении образовательного стандарта Академии по направлению подготовки 38.03.04 Государственное и муниципальное управление» № 01-3023 от 29 марта 2021 г.;

– приказа Министерства образования науки Российской Федерации от 1.07.2013г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» с внесенными изменениями от 14.01.2014 г. №31014;

– методических рекомендаций Министерства образования и науки Российской Федерации от 10.04.2014 года № 06-381. «Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ»;

– приказа РАНХиГС от 22.09 2017г. №01-6230 «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

– приказа РАНХиГС от 19.04.2019г. №02-461 «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию».

1.3. Планируемые результаты обучения

В результате освоения программы повышения квалификации обучающийся может осуществлять деятельность в области обеспечения информационной безопасности в деятельности государственных и муниципальных органов.

В результате освоения программы повышения квалификации обучающийся должен приобрести:

1) обозначенные в «Справочнике квалификационных требований к специальностям, направлениям подготовки (к укрупненным группам специальностей и направлений подготовки), к профессиональному уровню, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих»:

Вид профессиональной служебной деятельности «П. 16.2. Регулирование в сфере обеспечения информационной и сетевой безопасности»:

II. Требования к знаниям

2 Иные профессиональные знания:

2.1. основные мировые и отечественные тенденции развития и структуры направлений информационной и сетевой безопасности отрасли информационных технологий;

2.2. понятие базовых информационных ресурсов;

2.4. понятие система безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере связи;

2.6. знание нормативных правовых актов Российской Федерации и методических документов ФСТЭК России в области защиты информации, и обеспечения безопасности критической информационной инфраструктуры Российской Федерации»;

2.7. принципы работы программно-аппаратных средств защиты информации, понимание принципов алгоритмов защиты, основ защиты от разрушающих программных воздействий;

2.8. порядок организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;

2.11. знание национальных, межгосударственных и международных стандартов в области защиты информации, в том числе ГОСТ Р ИСО/МЭК 15408 (1-3), ГОСТ Р ИСО/МЭК 27001, 27002, 27004, 27005, 27033, 56545, 53109, 34.10, 34.13, 28147.

III. Требования к профессиональным умениям:

- анализ угроз безопасности информации, оценка рисков безопасности

информации;

- определение объектов защиты;
- моделирование угроз безопасности информации;
- разработка требований по защите информации;
- применение средств защиты информации;
- проведение категорирования объектов критической информационной инфраструктуры, функционирующих в сфере связи.

2) обозначенные в «Справочнике типовых квалификационных требований для замещения должностей муниципальной службы»:

Вид деятельности «Осуществление мероприятий по вопросам информационной безопасности»:

II. Требования к знаниям

1. Знания в области законодательства Российской Федерации, знание муниципальных правовых актов:

4.2. Федеральный закон от 27 июля 2006 г. N 149 «Об информации, информационных технологиях и защите информации»;

4.3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

4.4. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»;

4.5. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

4.6. Приказ Администрации Губернатора и Правительства Орловской области от 5 июня 2019 года № 225 «Об организации работы с персональными данными в Администрации Губернатора и Правительства Орловской области».

2. Иные профессиональные знания:

4.1. методы информационной безопасности;

4.2. методы и средства получения, обработки и передачи информации;

4.3. порядок работы со сведениями, составляющими государственную тайну;

4.4. процесс формирования и проверки электронной цифровой подписи.

К результатам освоения программы относится возможность осуществления деятельности, связанной с обеспечением информационной безопасности в деятельности государственных и муниципальных органов.

Перечень профессиональных компетенций конкретизирован в таблице 1.

Таблица 1

Планируемые результаты обучения

Вид деятельности	Профессиональные компетенции
Регулирование в сфере обеспечения информационной и сетевой безопасности [1]	ПКс-1 способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг с учетом требований информационной безопасности
	ПКс-2 способен применять национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области защиты информации
	ПКс-3 способен выполнять работы по обследованию объектов критической информационной инфраструктуры и разработке требований по защите информации
	ПКс- 4 способен участвовать в разработке документации по организации системы защиты информации на объектах критической информационной инфраструктуры
	ПКс- 5 способен применять в профессиональной деятельности средства защиты информации
Осуществление мероприятий по вопросам информационной безопасности [2]	ПКс-6 способен использовать в профессиональной деятельности законодательные и нормативные правовые акты субъекта РФ в области защиты информации и обеспечения безопасности персональных данных
	ПКс-7 способен организовывать мероприятия по воздействию на риски информационной безопасности

1.4. Категория слушателей

К слушателям программы ДПО следует отнести государственных гражданских служащих Орловской области, желающих приобрести профессиональные навыки в области обеспечения информационной безопасности, в том числе сотрудники и руководители всех уровней. К освоению дополнительной профессиональной программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование;

1.5. Формы обучения и сроки освоения

Форма обучения – очно-заочная с применением электронного обучения.
Срок получения образования составляет 2 недели.

1.6. Период обучения и режим занятий

Режим занятий устанавливается по согласованию со слушателями программы

[1] Входит в «Справочник квалификационных требований к специальностям, направлениям подготовки (к укрупненным группам специальностей и направлений подготовки), к профессиональному уровню, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих»

[2] Входит в «Справочник типовых квалификационных требований для замещения должностей муниципальной службы»

повышения квалификации.

1.7. Документ о квалификации

По окончании обучения слушателям выдается удостоверение о повышении квалификации по форме, самостоятельно устанавливаемой организацией, осуществляющей образовательную деятельность.

2. Содержание программы

2.1. Календарный учебный график

Календарный учебный график отражает реализацию учебного плана во времени, периоды проведения теоретических занятий, процедур промежуточной и итоговой аттестаций.

Таблица 2

Период	1 день	2 день	3 день	4 день	5 день
Неделя 1	УЗ/ТКУ	УЗ/ТКУ	УЗ/ТКУ	УЗ ЭО (КСР)/ТКУ ЭО	УЗ ЭО (КСР)/ТКУ ЭО
Неделя 2	УЗ/ТКУ	УЗ/ТКУ	УЗ ЭО (КСР)/ТКУ ЭО	УЗ ЭО (КСР)/ТКУ ЭО	УЗ/ТКУ/ИА

УЗ – учебные занятия;
ТКУ – текущий контроль успеваемости;
УЗ ЭОТ – учебные занятия с применением электронного обучения (КСР-контактная самостоятельная работа);
ТКУ ЭО – текущий контроль успеваемости с применением электронного обучения;
ИА – итоговая аттестация.

2.2. Учебный план

Учебный план программы повышения квалификации определяет перечень, трудоемкость, последовательность и распределение учебных дисциплин, а также формы аттестации.

Оценка качества освоения слушателями программы повышения квалификации осуществляется в ходе промежуточной и итоговой аттестации.

Трудоемкость программы повышения квалификации составляет 72 часа.

Таблица 3

№п/п	Наименование (модуля/раздела/дисциплины/темы), практики (стажировки)	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа, час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Лабораторные занятия (практикум) /в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час			Лекции/ в интерактивной форме	Лабораторные занятия (практикум) /в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час					
1.	2	3	4	5	6	7	8	9	10	11	12	13	14	16	17	18	19	20
1	**Раздел 1. Информационная безопасность в деятельности органов государственной власти**	**50**	**26**	**12**		**14**			**24**				**24**		**О**			
1.1	Тема 1. Порядок создания, развития, эксплуатации государственных информационных систем	6	2	2					4				4		О			ПКс-1
1.2.	Тема 2. Нормативное регулирование информационной безопасности. Методические документы и национальные стандарты	10	6	2		4			4				4		О			ПКс-6
1.3	Тема 3. Объекты защиты и угрозы безопасности информации	10	6	2		4			4				4		О			ПКс-3
1.4	Тема 4. Система защиты данных информационных систем	8	4	2		2			4				4		О			ПКс- 4 ПКс- 5

1.5	Тема 5. Обеспечение информационной безопасности при использовании государственными гражданскими служащими социальных сетей, почтовых и иных интернет-сервисов	10	6	2		4			4				4		О			ПКс- 4 ПКс- 5 ПКс-6
1.6	Тема 6. Сертификация средств защиты информации. Аттестация информационных систем по требованиям защиты информации	6	2	2					4				4		О			ПКс-2
2.	**Раздел 2. Организация работы с персональными данными**	**22**	**10**	**4**		**4**			**12**				**12**		**О**			
2.1	Тема 1. Организация обработки персональных данных	6	2	2					4				4		О			ПКс-3
2.2	Тема 2. Обеспечение безопасности персональных данных	8	4	2		2			4				4		О			ПКс-1 ПКс- 5 ПКс-6
2.3	Тема 3. Аттестация информационных систем по требованиям защиты персональных данных	6	2			2			4				4		О			ПКс-2
	Итого:	**70**	**34**	**16**		**18**			**36**				**36**					
	Итоговая аттестация	**2**															**2**	
	Всего:	**72**	**34**	**16**		**18**			**36**				**36**				**2**	

2.3 Содержание программы по модулям/разделам/дисциплинам и (или) темам

Таблица 4

Содержание программы по модулям /разделам/дисциплинам и (или) темам

Номер модуля/ раздела/ дисциплины и (или) темы	Содержание модуля /раздела/дисциплины и (или) темы
Раздел 1. Информационная безопасность в деятельности органов государственной власти	
Тема 1. Порядок создания, развития, эксплуатации государственных информационных систем	Государственные институты в информационном обществе. Основные положения государственной политики в сфере использования информационных технологий в деятельности органов государственной власти. Стратегические и нормативно-правовые документы, определяющие применение информационных технологий в системе государственного управления Российской Федерации. Национальные стандарты в сфере информационных технологий. Государственные информационные системы. Система открытого правительства в Российской Федерации, его основные функции. Формирование механизмов и технологий открытого государственного управления. Электронные сервисы взаимодействия с гражданами. Государственные услуги в электронном виде. Подходы к повышению качества предоставления государственных услуг. Принцип «одного окна». Многофункциональные центры в Российской Федерации. Порталы государственных и муниципальных услуг. Федеральный реестр и единый портал государственных услуг.
Тема 2. Нормативное регулирование информационной безопасности. Методические документы и национальные стандарты	Информация, информационные системы как объект правового регулирования информационной безопасности. Структура правовой защиты информации. Система документов в области защиты информации. Законодательная база обеспечения информационной безопасности. Федеральные законы в области защиты информации. Основные положения Доктрины информационной безопасности Российской Федерации. Стандарты в области информационной безопасности. Правонарушение в информационной сфере, состав правонарушения. Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере. Правовой режим защиты государственной тайны. Правовая регламентация лицензионной и сертификационной деятельности в области защиты информации, в том числе государственной тайны. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции
Тема 3. Объекты защиты и угрозы безопасности информации	Объекты и субъекты информационной защиты. Свойства информации как объекта защиты. Риски угроз информационным ресурсам. Определение состава защищаемой информации. Значение носителей защищаемой информации как объектов

	защиты. Особенности помещений как объектов защиты для работы по защите информации. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Угрозы безопасности. Классификация угроз безопасности. Способы реализации угроз безопасности. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия. Выявление каналов и определение возможных методов несанкционированного доступа к информации. Разрушающие программные воздействия. Структура разрушающего программного воздействия. Классификация разрушающих программных воздействий. Экономические последствия утечки информации.
Тема 4. Система защиты данных информационных систем	Организация защиты информации. Основные задачи в организации защиты информации. Уровни организации защиты информации: правовой, административный, технический. Технические средства защиты: средства предупреждения угроз, средства выявления факта реализации угроз, средства минимизации ущерба. Средства защиты системы контроля доступа пользователя. Выбор механизмов и средств защиты информации. Формальные модели безопасности. Распределение функций по защите информации.
Тема 5. Обеспечение информационной безопасности при использовании государственными гражданскими служащими социальных сетей, почтовых и иных интернет-сервисов	Системы защиты облачных сервисов и электронной почты. Системы контроля доступа устройств к сети. Репутационные сервисы и SIEM-системы. IT-активы, управление паролями. Рекомендации по личной безопасности в интернете.
Тема 6. Сертификация средств защиты информации. Аттестация информационных систем по требованиям защиты информации	Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России. Требования и рекомендации по защите информации. Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Аттестация объекта информатизации по требованиям безопасности информации. Порядок проведения аттестации. Схема аттестации объекта информатизации, Программы и методики аттестационных испытаний. Заключение по результатам аттестации объекта информатизации. Выдача аттестата соответствия объекта информатизации. Перечень и содержание документов разрабатываемые в организации до начала процесса аттестации. Технический контроль аттестованного объекта информатизации
Раздел 2. Организация работы с персональными данными	
Тема 1. Организация обработки персональных данных	Общий порядок организации обработки персональных данных. Неавтоматизированная и автоматизированная обработка персональных данных, особенности обработки. Структура информационной системы персональных данных (ИСПД). Требования и методы по обезличиванию персональных дан-

	ных, обрабатываемых в информационных системах персональных данных. Разработка уведомления об обработке (о намерении осуществлять обработку) персональных данных. Перечень правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона 152-ФЗ от 27 июля 2006 года № 152-ФЗ «О персональных данных», необходимых для принятия органами государственной власти. Принципы обработки персональных данных. Условия обработки персональных данных. Конфиденциальность персональных данных. Общедоступные источники персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Порядок обработки персональных данных, разрешенных субъектом персональных данных для распространения. Порядок обработки персональных данных при рассмотрении обращений граждан. Специальные категории персональных данных. Правовое регулирование отношений в области защиты персональных данных.
Тема 2. Обеспечение безопасности персональных данных	Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Риски и уязвимости обработки персональных данных в государственных учреждениях, модель угроз. Основные мероприятия по обеспечению защиты персональных данных. Организационно-административные меры защиты персональных данных. Политика конфиденциальности. Программно-технические средства защиты. Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации. Состав и содержание мер по обеспечению безопасности персональных данных. Особенности использования средств криптографической защиты информации в рамках построения системы защиты персональных данных в организации
Тема 3. Аттестация информационных систем по требованиям защиты персональных данных	Классификация ИСПД по классам защищенности. Определение уровня защищённости персональных данных. Профили защиты, порядок их регистрации и сертификации во ФТЭК РФ.

3. Организационно-педагогические условия реализации программы

3.1 Кадровое обеспечение

Реализация программы обеспечивается профессорско- преподавательским составом Среднерусского института управления – филиала РАНХиГС, имеющим базовое образование, соответствующее профилю преподаваемых дисциплин, и стаж научно-педагогической работы более 20 лет.

Таблица 5

Сведения о профессорско-преподавательском составе и ведущих специалистах

Ф.И.О. преподавателя/ведущего специалиста	Специальность, присвоенная квалификация по диплому	Дополнительные квалификации	Место работы, должность, основное/ дополнительное место работы	Ученая степень, ученое (почетное) звание	Стаж работы в области профессиональной деятельности/ по дополнительной квалификации	Стаж научно-педагогической работы		Наименование преподаваемой дисциплины/темы (модуля), практики/стажировки (при наличии) по данной программе
						Всего	В том числе по преподаваемой дисциплине (модулю)	
Музалевская Алла Анатольевна	Магистр» по направлению подготовки «Прикладная информатика»	1. «Организация электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ) в системе дистанционного обучения (СДО)», 40 часов, ФГБОУ ВО «РАНХиГС», 2021 г. 2. «Инновационные образовательные технологии преподавания математических и информационных дисциплин», 24 часа, АНО «Научно- исследовательский институт менеджмента, экономики, статистики, информатики», 2021 г. 3. «Электронная информационно- образовательная среда образовательной организации (ЭИОС)», 24 часа, ФГБОУ ВО «РАНХиГС», 2022 г. 4. «Организация обучения инвалидов и лиц с ограниченными возможностями здоровья в вузе», 72 часа, ФГБОУ ВО «Орловский государственный университет экономики и торговли», 2021 г.	Среднерусский институт управления – филиал РАНХиГС, доцент кафедры математики и информационных технологий, основное место работы – штатный	кандидат педагогических наук, доцент	35	35	30	Раздел 1. Информационная безопасность в деятельности органов государственной власти Раздел 2. Организация работы с персональными данными

3.2 Материально-техническое и программное обеспечение реализации программы

Используемые для реализации программы специальные помещения представляют собой учебные аудитории.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения (видео-, аудиотехника, компьютеры, мультимедийные средства), необходимыми для представления учебной информации большой аудитории.

Материально-техническая база

Таблица 6

Материально-техническая база для реализации программы

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения лекционных, практических и лабораторных занятий, индивидуальных и групповых консультаций, текущего контроля успеваемости и промежуточной аттестации	Учебная мебель Аудиторная доска Презентационное оборудование Стационарные компьютеры и(или) ноутбуки
Компьютерный класс (аудитория для выполнения самостоятельной работы)	Учебная мебель Аудиторная доска Презентационное оборудование Стационарные компьютеры и(или) ноутбуки
Аудитория/компьютерный класс для организации онлайн-трансляции занятий	- http://orel-ranepa.ru/, - «МТС-линк» - вебинарная площадка, обеспечивающая видео- и аудио-трансляцию, общение участников вебинара посредством чата, запись вебинара - «МТС-линк» - видео-конференцсвязь, обеспечивающая двустороннюю связь слушателей и преподавателя
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования.

Таблица 7

Перечень программного обеспечения, необходимого для реализации программы

Наименование программного обеспечения	Назначение и тип лицензии программного обеспечения
Microsoft Office	Интегрированный пакет прикладных программ. Лицензионная версия
Openoffice	Интегрированный пакет прикладных программ. Свободно распространяемый
ИПС «КонсультантПлюс» URL: http://www.consultant.ru/	Информационно-поисковая система, позволяющая работать с нормативно-правовыми актами, учебной и науч-

	ной литературой. Лицензионная версия
Лань URL: e.lanbook.com	Электронная библиотечная система. Лицензионная версия
Юрайт URL: https://urait.ru/	Электронная библиотечная система. Лицензионная версия
IPR URL: iprbookshop.ru	Электронная библиотечная система. Лицензионная версия
7-Zip	Архиватор с высокой степенью сжатия Свободная лицензия
Google Chrome	Браузер Свободная лицензия
Yandex Браузер	Браузер Свободная лицензия
Kaspersky Endpoint Security 10 для Windows	Антивирус - Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 250499 Node 2 year Educational Renewal License – лицензия до 2018-01-03 Лицензированная версия
Windows XP Professional Windows 7 Professional Windows 8 Pro Windows 8.1 Pro	Операционные системы. Лицензированная версия
http://orel-ranepa.ru/	Электронный курс «Информационная безопасность в деятельности органов государственной власти. Организация работы с персональными данными»

3.3 Учебно-методическое и информационное обеспечение программы

Нормативные правовые документы

1. Конституция Российской Федерации [Электронный ресурс] / СПС КонсультантПлюс: Законодательство: Версия Проф. – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ [Электронный ресурс] // СПС КонсультантПлюс: Законодательство: Версия Проф. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

3. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [Электронный ресурс] // СПС КонсультантПлюс: Законодательство: Версия Проф. – URL: http://www.consultant.ru/document/cons_doc_LAW_103023/

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – URL:https://www.consultant.ru/document/cons_doc_LAW_61801/

5. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/

6. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/

7. Указ Президента РФ от 7 мая 2012 г. № 601 «Об основных направлениях совершенствования системы государственного управления» [Электронный ресурс] // СПС Гарант. - URL: https://base.garant.ru/70170942/

8. Указ Президента Российской Федерации от 22 мая 2015 г. №260 «О некоторых вопросах информационной безопасности Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_179963/

9. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: https://base.garant.ru/71556224/

10. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». – URL: https://www.garant.ru/products/ipo/prime/doc/404461984/

11. Указ Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» – URL: http://publication.pravo.gov.ru/document/0001202405070015

12. Национальный проект «Экономика данных и цифровая трансформация государства» (утв. протоколом заочного голосования членов президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 г. №12пр.). – URL: https://mirs.permkrai.ru/natsionalnye-proekty/natsionalnyy-proekt-ekonomika-dannykh-i-tsifrovaya-transformatsiya-gosudarstva

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 . – Режим доступа: по подписке.

2. Максуров, А. А. Обеспечение информационной безопасности в сети Интернет : монография / А.А. Максуров. — Москва : ИНФРА-М, 2023. — 226 с. — (Научная мысль). — DOI 10.12737/1942595. - ISBN 978-5-16-018251-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1942595 . – Режим доступа: по подписке.

3. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. — 3-е изд., стер. — Москва: ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1042499 . – Режим доступа: по подписке.

4. Пашенцев, Д. А. Концепция цифрового государства и цифровой правовой среды : монография / Н.Н. Черногор, Д.А. Пашенцев, М.В. Залоило [и др.] ; под общ. ред. Н.Н. Черногора, Д.А. Пашенцева. — Москва: Институт законодательства и сравнительного правоведения при Правительстве Российской ФедерацииНорма : ИНФРА-М, 2023. — 244 с. — DOI 10.12737/1288140.

- ISBN 978-5-00156-164-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1974379. – Режим доступа: по подписке.

5. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 . – Режим доступа: по подписке.

6. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей.

7. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095 . — Режим доступа: для авториз. пользователей.

Дополнительная литература

1. Баланов, А. Н. Комплексная информационная безопасность: полный справочник специалиста : практическое пособие / А. Н. Баланов. - Москва ; Вологда : Инфра-Инженерия, 2024. - 156 с. - ISBN 978-5-9729-1771-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169705. – Режим доступа: по подписке.

2. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст: электронный. - URL: https://znanium.com/catalog/product/997108 . – Режим доступа: по подписке.

3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 . – Режим доступа: по подписке.

4. Гуриков, С. Р. Интернет-технологии: учебное пособие / С.Р. Гуриков. – 2-е изд., перераб. и доп. — Москва: ИНФРА-М, 2023. — 174 с. — (Высшее образование: Бакалавриат). – DOI 10.12737/1044018. - ISBN 978-5-16-016517-2. - Текст: электронный. - URL: https://znanium.com/ catalog/ product/1902731 . – Режим доступа: по подписке.

5. Дербин, Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. — Москва : ИНФРА-М, 2024. — 267 с. — (Выс-

шее образование). — DOI 10.12737/2084342. - ISBN 978-5-16-019050-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2084342 (– Режим доступа: по подписке.Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 . – Режим доступа: по подписке.

6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841. – Режим доступа: по подписке.

7. Калиногорский, Н. А. Основы практического применения интернет-технологий : учебное пособие / Н. А. Калиногорский. — 3-е изд., стер. — Москва : ФЛИНТА, 2020. — 182 с. - ISBN 978-5-9765-2302-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1142475 . – Режим доступа: по подписке.

8. Клишас, А. А. Современная концепция социального государства : монография / А.А. Клишас ; предисл. Т.Я. Хабриевой ; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. — Москва : Норма, 2023. — 288 с. — DOI 10.12737/1859182. - ISBN 978-5-00156-229-0. - Текст: электронный. - URL: https://znanium.com /catalog/product/1920523. – Режим доступа: по подписке.

9. Попов, И. В. Информационная безопасность: практикум / И. В. Попов, Н. И. Улендеева. - Самара: Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/2016193. – Режим доступа: по подписке.

10. Рощин, С. М. Современные интернет-технологии. Семь главных трендов: научно-популярное издание / С. М. Рощин. - 2-е изд. - Москва: Дашков и К, 2022. - 124 с. - ISBN 978-5-394-04846-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1927306. – Режим доступа: по подписке.

11. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2024. — 223 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2003474. – Режим доступа: по подписке.

Интернет-ресурсы

1. Федеральный центр информационных образовательных ресурсов http://fcior.edu.ru/catalog/osnovnoe_obshee
2. Интернет-университет информационных технологий (ИНТУИТ.ру) http://www.intuit.ru
3. Электронно-библиотечная система «Лань» // www.e.lanbook.com

4. Электронно-библиотечная система ЮРАЙТ // www.biblio-online.ru
5. Каталог сайтов интернета. Интернет. - URL: https://8500.ru/cat/site-internet.html
6. Интернет: подборка сайтов. - URL: https://megapoisk.com/internet_sites
7. Портал государственных услуг Российской Федерации https://www.gosuslugi.ru/
8. Электронные ресурсы по теме «Безопасный интернет». - URL: https://45.мвд.рф/citizens/информационная-безопасность/электронные-ресурсы-по-теме-безопасный-и
9. Сетевая безопасность — основы и 12 учебных ресурсов. - URL: https://toadmin.ru/сетевая-безопасность-основы-и-12-учеб/
10. Официальный сайт компании «Консультант Плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/
11. Информационно-правовой портал [Электронный ресурс]. – Режим доступа: http://www.garant.ru

Справочные системы

1. www.nnir.ru / - Российская национальная библиотека
2. www.nns.ru / -Национальная электронная библиотека
3. www.rsi.ru / - Российская государственная библиотека
4. www.aport.ru / - Поисковая система
5. www.rambler.ru / - Поисковая система
6. www.yandex.ru / - Поисковая система
7. http://www.consultant.ru/ - справочная правовая система «Консультант Плюс»
8. http://www.garant.ru/ - информационно-правовой портал «Гарант»

4. Оценка качества освоения программы

4.1. Формы и объем текущего контроля

Текущий контроль успеваемости – опрос по выполненным заданиям для практических занятий и контактной самостоятельной работы.

Примерные задания для практических занятий и контактной самостоятельной работы

Задание 1. Законодательная и нормативная база информационной безопасности

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации:

федеральные информационные системы и региональные информационные системы, созданные на основании соответственно Федеральных зако-

нов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

1. 149-ФЗ от 27 июля 2006 г.
2. 98-ФЗ от 29 июля 2004 г.
3. Указ Президента РФ от 17 марта 2008 г. № 351
4. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
5. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
6. СТР-К
7. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
8. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
9. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
11. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
17. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Задание 2. Определение рисков, связанных с использованием цифровых платформ государственных услуг

Риски использования цифровых платформ государственных услуг	Меры по преодолению рисков

Задание 3. Определение защищаемых информационных активов

1) Создать схему территориального расположения структурных подразделений

2) Для выбранного структурного подразделения определить информационные активы. Заполнить таблицу.

Наименование структурного подразделения

Вид актива	Наименование актива	Владелец	Гриф конфиденциальности	Угрозы	Уязвимости

Задание 4. Определение каналов утечки для защищаемых информационных активов

Определить зоны доступа к информационным активам, наиболее опасные каналы утечки информации, способы и средства противодействия утечке. Заполнить таблицу

№ п/п	Информационные активы	В какой зоне должны находиться	Наиболее опасные каналы утечки для каждого актива	Способ противодействия утечке	Средство противодействия утечке

Задание 5. Модель угроз

Составить перечень угроз для заданного объекта по образцу. Заполнить таблицу

Перечень угроз

№ угрозы	Источник угрозы	Среда распространения	Носитель информации

Задание 6. Анализ примеров нарушений информационной безопасности через сеть Интернет

Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ-инфраструктуру компании. Как предотвратить потерю информации? Что следует предпринять для устранения данных нарушений?

Для каждого из перечисленных объектов указать не менее 3 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами. Обозначить источ-

ник каждой из приведенных угроз.

Объект защиты	Наименование угрозы	Источник угрозы	Последствия	Как избежать угрозы
Сайт в сети интернет				
Рабочее место				
Домашний компьютер				

Задание 7. Оценка безопасности выбранного пароля

Дать количественную оценку длины пароля, если вероятность несанкционированного вскрытия (взлома) пароля $P = 10^{-6}$, скорость V подбора (перебора и ввода) паролей V = 10 паролей/мин, вероятное время T непрерывной работы злоумышленника по подбору пароля одна неделя, число символов, из которых может состоять пароль (этот параметр называется мощностью алфавита паролей) для пароля, стоящего из одних цифр, A =10; для заглавных (или строчных) букв латинского алфавита A = 26; для заглавных и строчных латинских букв A= 52; для заглавных, строчных латинских букв и арабских цифр A = 62; для пароля, состоящего из цифр и строчных (или заглавных) букв A = 36; для всех печатных символов (включая знаки препинания и специальные символы) A=95. Выполнить оценку безопасности выбранного пароля почтового ящика.

Задание 8. Сравнительный анализ антивирусных программ

Провести сравнительный анализ антивирусных программ, заполнить таблицу (по вариантам)

Критерии сравнения	Антивирус1	Антивирус2	Антивирус3
Вид лицензии			
Язык интерфейса			
Антивирусный сканер и антивирусный монитор			
Защита персональных данных			
Эвристический алгоритм			
Наличие фаервола			
Защита E-mail			
Возможность работы в облаке			
Система обнаружения и предотвращения вторжений			
Антиспам			
Веб-защита			

Поведенческий блокиратор			
Виды сканирования			
Частота обновления			
Скорость сканирования			
Действия при обнаружении вируса			

Задание 9. Законодательная и нормативная база защиты персональных данных

Отметьте в списке 11 нормативных документов, которые относятся к данному объекту информатизации:

совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1. 152-ФЗ от 27 июля 2006 г.
2. 149-ФЗ от 27 июля 2006 г.
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. Пост. Правительства РФ № 211 от 21 марта 2012 г.
8. Пост. Правительства РФ № 953 от 24 ноября 2009 г.
9. СТР-К
10. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
11. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
12. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
13. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
14. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
15. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
16. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
17. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
20. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
23. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Задание 10. Анализ состава персональных данных

Проанализировать ИСПДн, функционирующие на объекте. Привести текстовое описание каждой ИСПДн. Построить таблицу с результатами анализа.

Анализ существующих ИСПДн объекта

Наименование ИСПДн	Краткое описание	Действия оператора ИПДн	Вид автоматизированной обработки
«Кадры»	Ведение личных дел		
…….			

Задание 10. Характеристика документов, содержащих ПнД

Определить состав, категории и объем обрабатываемых ПДн, источники и носители. Дать характеристику всех документов объекта, содержащих ПДн. Результаты занести в таблицу.

Характеристика обрабатываемых ПДн объекта

Перечень ПДн	Источник ПДн	Объем ПДн	Вид носителя ПДн	Категория ПДн
Фамилия, имя, отчество, адрес места жительства, ИНН, паспортные данные, фотография, сведения о болезни	Трудовая книжка сотрудника, трудовой договор, личная карточка, больничные листы	< 100 000	Документы на бумажном носителе, жесткий диск компьютера	Иные, биометричекие, специальные, общедоступные
……..				

Примерные вопросы для текущего контроля

1. Цифровое и электронное государство.
2. Электронное правительство. Сущность и этапы развития.
3. Современные направления создания информационных систем в государственном и муниципальном управлении
4. Госсектор: опора на открытые стандарты
5. Государственные информационные ресурсы (по типу информации)
6. Влияние цифрового государства на возрастание публичности государственных служащих.
7. Роль информационных технологий в повышении эффективности государственного и муниципального управления.
8. Компетенции цифровой экономики
9. Цифровые технологии в государственном управлении.
10. Прикладные автоматизированные системы в госуправлении
11. Порталы органов государственной власти
12. Модели и платформы предоставления государственных услуг
13. Понятие, цели и принципы создания цифрового профиля
14. Обеспечение информационной безопасности цифрового профиля
15. Сетевые технологии, используемые в сети Интернет.
16. Адресация в информационных сетях.
17. Протоколы прикладного уровня: HTTP, SMTP, POP3, IMAP, FTP, DNS, Telnet.
18. Интернет протоколы. Стек протокола TCP/IP.
19. Процедуры обмена сообщениями.
20. Протокол FTP. Режим установления связи для обмена файлами.
21. World Wide Web. HTTP, HTML.
22. Веб-браузер. Наиболее популярные Веб-браузеры (Microsoft Internet Explorer, Mozilla Firefox, Opera, Netscape), их возможности.
23. Веб-порталы (определение, назначение, свойства, типы, примеры порталов). Основные отличия сайта от портала. Примеры порталов.
24. Наиболее популярные почтовые клиенты (Microsoft Outlook, Mozilla Thunderbird, The Bat), их возможности (установка, настройки, фильтры, адресная книга, поиск и пр.).
25. Основные параметры настройки почтовых фильтров.
26. Спам. Виды спама. Способы борьбы со спамом. Возможности почтовых клиентов по борьбе со спамом.
27. Организация и проведение видеоконференций в сети Интернет.
28. Защита информации. Объект защиты. Цель защиты информации.
29. Эффективность защиты информации.
30. Безопасность в информационных сетях. Классификация сетевых атак.
31. Сетевая разведка и анализ сетевого трафика.
32. Вредоносные программы.
33. Безопасность в информационных сетях. Отказ в обслуживании.
34. Безопасность в информационных сетях. Спам и фишинг.
35. Идентификация и аутентификация. Качество пароля.

36. Безопасность в информационных сетях. Защита от сетевых атак. Межсетевые экраны.
37. Антивирусные программы
38. Профилактические мероприятия для защиты компьютерных сетей от вредоносного ПО
39. Защита данных в автономном компьютере.
40. Резервное копирование
41. Проблема защиты электронной информации.
42. Основные положения теории информационной безопасности информационных систем
43. Коммерческая тайна как атрибут рыночной экономики. Информация как важнейший ресурс и рыночный товар.
44. Концепция информационной безопасности
45. Стандарты и спецификации в области информационной безопасности. Цели сертификации и выгоды от ее проведения.
46. Законодательный уровень информационной безопасности
47. Административный уровень информационной безопасности.
48. Основные программно-технические меры информационной безопасности.
49. Идентификация и аутентификация, управление доступом
50. Внутренняя политика безопасности операционных систем семейства Windows.
51. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
52. Место информационной безопасности экономических систем в национальной безопасности страны
53. Основные технологии построения защищенных ИС
54. Анализ способов нарушений информационной безопасности
55. Информационная безопасность в условиях функционирования в России глобальных сетей
56. Модели безопасности и их применение
57. Понятие угрозы информации. Классификация угроз
58. Политики аудита информационной безопасности
59. Три вида возможных нарушений информационной системы. Защита от нарушений
60. Использование защищенных компьютерных систем
61. Система прав доступа. Ролевой и мандатный доступ
62. Сетевая защита и брандмауэр
63. Протоколирование и аудит защиты информации
64. Система антивирусной защиты.
65. Виды противников или «нарушителей».
66. Экранирование, анализ защищенности компьютерных систем
67. Управление рисками информационной безопасности
68. Распространённые методы НСД в сетях
69. Методы криптографии. Криптография с открытым ключом Симмет-

ричные криптосистемы.
70. Электронная цифровая подпись.
71. Обеспечение защиты операционных систем от атак по компьютерным сетям
72. Пароли и распределение прав пользователей. Политика паролей
73. Реестр. Политика безопасности
74. Комплексность защиты информации и необходимость комплексной защиты. Принципы комплексного подхода к обеспечению информационной безопасности.
75. Мероприятия по защите сведений конфиденциального характера. Режим коммерческой тайны, его установление и содержание. Меры по охране конфиденциальности.
76. Ограничение доступа к информации, составляющей коммерческую тайну. Контроль за соблюдением режима конфиденциальности.
77. Конфиденциальное делопроизводство. Организация контроля за обращением с информацией работников предприятия.
78. Гражданско-правовое регулирование отношений, связанных с передачей информации, составляющей коммерческую тайну, сторонним организациям и физическим лицам.
79. Регулирование вопросов, связанных с обращением на предприятии коммерческой тайны, в рамках трудовых отношений.
80. Недобросовестная конкуренция. Методы несанкционированного получения защищаемой информации. Каналы утечки конфиденциальных сведений, модель нарушителя.
81. Организация работ по технической защите конфиденциальной информации.
82. Проблемы обеспечения безопасности при использовании новых информационных технологий. Безопасность в виртуальной среде.
83. Лицензирование деятельности по технической защите конфиденциальной информации и использованию средств криптографической защиты. Ответственность за деятельность без лицензии.
84. Цели и задачи технической защиты конфиденциальной информации. Структура подразделений технической защиты информации.
85. Подходы к созданию комплексной системы защиты конфиденциальной информации в организации.
86. Методы оценки защищенности информации от утечки по техническим каналам.
87. Обзор средств контроля защищенности.
88. Рекомендации по проектированию, созданию и эксплуатации комплексных систем защиты конфиденциальной информации.
89. Необходимость технологии обнаружения атак. Методы обнаружения атак. Механизмы реагирования.
90. Методы выявления уязвимостей. Системы анализа защищенности.
91. Построение системы охраны объекта. Многорубежная защита.
92. Классификация групп технических средств охраны: охранное телеви-

дение; ограждение и физическая изоляция; запирающие устройства; система контроля доступа.

93. Основные этапы работ по обеспечению безопасности ПДн в ИСПДн

94. Уровни защищенности персональных данных при их обработке в ИСПДн в зависимости от угроз безопасности этим данным и классификация ИСПДн.

95. Каналы утечки информации при обработке персональных данных в информационных системах.

96. Разработка (проектирование) системы защиты персональных данных (СЗПДн)

97. Разработка и внедрение организационных мер и организационно-распорядительных документов по обеспечению защиты персональных данных

4.2. Формы и объем итоговой аттестации

Цель итоговой аттестации: определение соответствия уровня готовности выпускников Программы требованиям, предъявляемым к их профессиональной деятельности, направленной на формирование компетенций в области обеспечения информационной безопасности общества, государственных и муниципальных органов власти, личности, задач по управлению рисками информационной безопасности в условиях институциональных изменений и цифровых трансформаций, с учетом динамики социально-экономических процессов и новых требований к качеству управления.

Форма итоговой аттестации: тестирование (максимальная балл - 25).

К итоговой аттестации допускаются слушатели, в полном объеме выполнившие учебный план.

Трудоемкость итоговой аттестации: 2 академических часа.

Примеры оценочных материалов в рамках итоговой аттестации

1. Система считается безопасной, если…

а) она абсолютно недоступна для взлома
б) она управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право доступа
в) все пользователи удовлетворены работой системы

2. Система считается надежной, если…

а) она обеспечивает одновременную обработку информации разной степени секретности (конфиденциальности) группой пользователей без нарушения прав доступа
б) она абсолютно недоступна для взлома
в) администратор удовлетворен работой системы

3. Защита от несанкционированного получения информации – это…

а) конфиденциальность
б) целостность
в) доступность

4. Пароль, придуманный пользователем, который не изменяется от сеанса к сеансу называется…

а) простым
б) сложным
в) динамическим

5. Способ заражения программ, при котором код вируса приписывается к концу файла заражаемой программы, и тем или иным способом осуществляется переход вычислительного процесса на команды этого фрагмента, называется методом…

а) приписывания
б) оттеснения
в) вытеснения

6. Пароль пользователя, который изменяется для каждого нового сеанса работы или нового периода действия, называется…

а) статическим
б) динамическим
в) простым

7. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется…

а) идентификатором
б) ключом
в) электронной подписью

8. Наука, занимающаяся проблемой защиты информации путем ее преобразования – это…

а) криптология
б) криптография
в) криптоанализ

9. особ заражения программ, при котором код вируса располагается в начале зараженной программы, а тело самой программы приписывается к концу, называется методом…

а) оттеснения
б) вытеснения
в) стирания

10. При использовании метода «запрос-ответ» система для подтверждения подлинности пользователя…

а) последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ
б) использует аппаратную проверку биометрических характеристик пользователя
в) последовательно задает ему ряд вопросов на сообразительность

11. Процесс преобразования открытых данных в зашифрован-

ные при помощи шифра называется…

а) зашифрованием

б) расшифрованием

в) декодированием

12. Наука о методах защиты информации с помощью шифров – это…

а) криптология

б) криптоанализ

в) криптография

13. Для обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности необходимо использовать антивирусное ПО. Какие программы относятся к антивирусным?

а) Norton AntiVirus, AVP, DrWeb

б) MS-DOS, MS Word, AVP

в) MS Word, MS Excel, Norton Commander

14. Stealth-вирусы…

а) это макровирусы

б) используют механизм перехвата управления при возникновении прерывания

в) заражают все программы на диске

15. Система шифрования Российский стандарт ГОСТ 28147-89 является системой шифрования…

а) симметричной

б) с открытым ключом

в) асимметричной

16. Из перечисленных: 1) симметричные, 2) асимметричные, 3) открытые 4) закрытые – различают системы шифрования…

а) 1, 2

б) 1, 3

в) 1, 4

17. Защита от несанкционированного изменения информации – это…

а) целостность

б) конфиденциальность

в) доступность

18. Защита от несанкционированного блокирования доступа к информационным ресурсам – это…

а) целостность

б) доступность

в) безопасность

19. Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе – это…

а) идентификатор

б) пароль
в) шифр

20. Система шифрования DES является системой шифрования…

а) симметричной
б) с открытым ключом
в) с закрытым ключом

21. Системы шифрования, в которых для зашифрования и расшифрования используется один и тот же ключ, называются системами шифрования…

а) симметричными
б) асимметричными
в) открытыми

22. Основными составляющими информационной безопасности являются…

а) конфиденциальность, целостность, доступность
б) своевременность, актуальность, полнота
в) релевантность, толерантность

23. Из перечисленного: 1) организационно-правовая основа, 2) технико-математические аспекты, 3) юридические аспекты – организационно-правовое обеспечение защиты информации включает в себя…

а) 1, 2, 3
б) 2, 3
в) 1, 3

24. На законодательном уровне информационной безопасности особого внимания заслуживают…

а) правовые акты и стандарты
б) разделение обязанностей и минимизация привилегий
в) документирование и регламентные работы

25. Процесс преобразования зашифрованных данных в открытые при помощи ключа называется…

а) кодированием
б) расшифрованием
в) зашифрованием

26. В асимметричных системах шифрования…

а) открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
б) для зашифрования и расшифрования используется один ключ
в) секретный и открытый ключи доступны всем желающим

27. При поиске информации в сети Интернет, необходимой для решения учебных и практических задач, необходим доступ к файлу, созданному в прикладном программном обеспечении. Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении– это…

а) пароль

б) идентификатор
в) шифр

28. Что такое аутентификация при использовании поискового аппарата электронных библиотечных систем?

а) правила выбора и использования пароля
б) объекты идентификации и установления подлинности в информационной системе
в) особенности разделения привилегий и разграничения доступа

29. Для реализации требований информационной безопасности при поиске информации в сети Интернет, необходимой для решения учебных и практических задач, необходимо использовать…

а) антивирусные программы
б) операционную систему
в) прикладное ПО

30. Программные средства, применяемые для реализации требований информационной безопасности при поиске и представлении информации – это…

а) специальные программы и системы защиты информации в информационных системах различного назначения
б) текстовые, табличные и графические редакторы
в) системное программное обеспечение

31. При доступе к информационным массивам идентификация позволяет…

а) субъекту назвать себя (сообщить свое имя)
б) выявлять нетипичное поведение пользователей
в) разграничивать сетевой доступ путем фильтрации

32. Установка лицензионного программного обеспечения является …

а) обязательным критерием информационной безопасности
б) необязательным критерием информационной безопасности
в) бесполезной тратой корпоративных денежных средств

33. Из перечисленных: 1) аутентификация и авторизация, 2) цифровая подпись, 3) межсетевые экраны, 4) мониторинг и аудит - для защиты информационных ресурсов операционных систем используются средства…

а) 1, 4
б) 1, 2, 3, 4
в) 3, 4

34. Динамические средства, следящие за событиями в сети и фиксирующие аномалии в работе, предупреждающие администратора об угрозах, анализирующие полученную информацию и восстанавливающие разрушенные данные, называют средствами…

а) мониторинга
б) сканирования
в) экранирования

35. При ролевом управлении доступом…

а) роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям
б) роли не определяются
в) роли могут быть приписаны многие пользователи; один пользователь может быть приписан только к одной роли

36. Программы тестирования систем на предмет наличия в них «дыр» в механизме безопасности называют…

а) сканерами
б) аудиторами
в) мониторами

37. Контроль защищенности – это…

а) установка сигнализации
б) попытка «взлома» информационной системы, осуществляемая силами самой организации или уполномоченными лицами
в) создание вирусов и запуск их в Интернет

38. Несанкционированное отправление данных от имени другого пользователя относится к атакам на…

а) протоколы информационного обмена
б) сменные элементы системы защиты
в) постоянные элементы системы защиты

39. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется…

а) идентификатором
б) ключом
в) электронной подписью

40. Задача логического управления доступом состоит в том, чтобы…

а) для каждой пары «субъект-объект» определить множество допустимых операций
б) проверять подлинность пользователя
в) фильтровать сообщения, передаваемые по каналам связи

41. Уровень безопасности данных, определяющий, каким пользователям или процессам разрешен доступ к данным, называют…

а) меткой безопасности
б) первичным ключом
в) вторичным ключом

42. Активный аудит безопасности – это…

а) оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации
б) проверка бухгалтерской отчетности компьютерного центра
в) помощь правоохранительных органов

43. Совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и

правильную интерпретацию, называется…

а) протоколом
б) уставом
в) конституцией

44. Фоновое резервирование информации обеспечивает…

а) восстановление любых потерянных данных после реализации как случайных, так и преднамеренных угроз
б) восстановление только системной информации
в) восстановление только информации пользователей

45. Пассивный аудит – это…

а) помощь правоохранительных органов
б) анализ последствий нарушения информационной безопасности и выявление злоумышленников
в) проверка бухгалтерской отчетности компьютерного центра

46. Средства защиты объектов файловой системы основаны на…

а) определении прав пользователя на операции с файлами и каталогами
б) задании атрибутов файлов и каталогов, независящих от прав пользователей
в) управлении данными

47. Подсистема управления доступом выполняет функции…

а) бесперебойного питания устройств в сети
б) подключения устройств к сети
в) по работе с идентификаторами и паролями

48. Из перечисленных: 1) перехват передаваемых данных, 2) подключение к линии связи, 3) внедрение несанкционированного маршрутизатора - к нападениям на протоколы информационного обмена относятся…

а) 1, 2, 3
б) 1, 2
в) 3

49. Бомбардировка запросами, когда программа злоумышленника постоянно направляет ОС запросы, реакция на которые требует привлечения значительных ресурсов, относится к атакам типа…

а) отказ в обслуживании
б) сбор «мусора»
в) подбор пароля

50. Защищенные виртуальные каналы связи, представляющие собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети, называются…

а) межсетевыми экранами
б) криптозащищенными туннелями
в) бастионами

4.3. Критерии оценки итоговой аттестации

Таблица 8

Шкала оценивания выполненных тестовых зданий по итоговой аттестации

Шкала оценивания	Критерии оценки
Не зачтено (0-14)	Оценка «не зачтено» ставится слушателям, которые при тестировании демонстрируют недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по разделам программы; компетенции, предусмотренные рабочей программой, не сформированы.
Зачтено (15-25)	Оценка «зачтено» ставится слушателям, которые при тестировании демонстрируют систематическое и глубокое знание программного материала; владеют понятийным аппаратом. Допускаются отдельные погрешности и неточности при ответе на вопросы тестовых зданий. Компетенции, предусмотренные рабочей программой, сформированы на достаточном уровне.

Характеристика результатов освоения программы

В результате освоения программы у слушателя сформированы компетенции, представленные в таблице 9.

Таблица 9

Критерии оценивания образовательных компетенций

Профессиональные компетенции	Ключевой индикатор оценивания	Критерии оценивания
ПКс-1	Уверенно использует информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применяет технологии электронного правительства и предоставления государственных (муниципальных) услуг с учетом требований информационной безопасности	Владеет навыками использования информационно-коммуникационных технологий, государственных и муниципальных информационные систем. Умеет применять технологии электронного правительства и предоставления государственных (муниципальных) услуг с учетом требований информационной безопасности
ПКс-2	Знает и применяет национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области защиты информации	Знает национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области защиты информации Умеет применять национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области защиты информации
ПКс-3	Выполняет работы по обследованию объектов критической информационной инфраструктуры и разработке тре-	Знает методику обследования объектов критической информационной инфраструктуры Умеет разрабатывать требования

	бований по защите информации	по защите информации
ПКс- 4	Участвует в разработке документации по организации системы защиты информации на объектах критической информационной инфраструктуры	Знает принципы организации системы защиты информации на объектах критической информационной инфраструктуры. Умеет разрабатывать документацию по организации системы защиты информации на объектах критической информационной инфраструктуры.
ПКс- 5	Осуществляет выбор и применяет средства защиты информации	Знает правовые, инженерно-технические и программные меры по обеспечению информационной безопасности. Умеет выбирать и применять средства защиты информации
ПКс-6	Использует законодательные и нормативные правовые акты субъекта РФ в области защиты информации и обеспечения безопасности персональных данных	Знает законодательные и нормативные правовые акты субъекта РФ в области защиты информации и обеспечения безопасности персональных данных и умеет их использовать в конкретной ситуации
ПКс-7	Описывает мероприятия по воздействию на риски информационной безопасности	Знает методику выявления рисков информационной безопасности. Умеет организовывать мероприятия по воздействию на риски информационной безопасности