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: CN=Щеголев Александр Владимирович, T=Заместитель начальника – начальник отдела, O=ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ", OU="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ"", CN="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ"", CNILS=-13800729986, ИНН=ЮЛ500830587, E=lq@ovel.ranepa.ru, G=Александр Владимирович, SN=Щеголев, C=RU
Основание: я подтверждаю этот документ своей квалифицированной подписью
Местоположение: Среднерусский институт управления

«УТВЕРЖДАЮ»

И.о. директора института - филиала

А.В. Щеголев

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышение квалификации

Информационная безопасность
72 часа

Орел, 2026

Разработчик
кандидат педагогических наук, доцент,
доцент кафедры «Математика
и информационные технологии»
(ученая степень и (или) ученое звание, должность, структурное подразделение)


(подпись)

А.А. Музалевская
(И.О.Фамилия)

Руководитель программы
кандидат педагогических наук, доцент,
доцент кафедры «Математика
и информационные технологии»
(ученая степень и (или) ученое звание, должность, структурное подразделение)


(подпись)

А.А. Музалевская
(И.О.Фамилия)

Программа повышения квалификации рассмотрена на заседании ученого совета Среднерусского института управления – филиала РАНХиГС и рекомендована к реализации, протокол № 1 от «24» января 2026г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ 4
1.1. Цель реализации программы 4
1.2. Нормативные правовые акты 4
1.3. Планируемые результаты обучения 6
1.4. Категория слушателей 8
1.5. Формы и технологии обучения 8
1.6. Период обучения, срок освоения и режим занятий 8
1.7. Документ о квалификации 8
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. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ 14
3.1 Материально-техническое и программное обеспечение реализации программы 14
3.3 Учебно-методическое и информационное обеспечение программы 16
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ 22
4.1. Формы и объем текущего контроля 31
4.2. Формы и объем итоговой аттестации 30
4.3. Критерии оценки итоговой аттестации 38
5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ 38

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Цель реализации программы «Информационная безопасность» 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. Нормативные правовые акты

Программа повышения квалификации «Информационная безопасность» 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.

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

Перечень профессиональных компетенций в рамках имеющейся квалификации и профессиональных компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	**Общепрофессиональные/профессиональные компетенции ОПК, ПК или трудовые функции (ПСК и СК)** ***(формируются и (или) совершенствуются)***	**Практический опыт**	**Знания**	**Умения**
1	**2**	**3**	**4**	**5**
Регулирование в сфере обеспечения информационной и сетевой безопасности	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	опыт использования в профессиональной деятельности ИКТ, государственных и муниципальных информационных систем, применение технологий электронного правительства и предоставления государственных (муниципальных) услуг с учетом требований информационной безопасности	знать методы и средства получения, обработки и передачи информации основные мировые и отечественные тенденции развития и структуры направлений информационной и сетевой безопасности	уметь учитывать требования информационной безопасности в профессиональной деятельности при использовании ИКТ, государственных и муниципальных информационных систем, технологий электронного правительства и предоставления государственных (муниципальных) услуг
	ПКс-2 способен применять национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области защиты информации	опыт применения национальных, межгосударственных и международных стандартов и методических документов ФСТЭК РФ в об-	знать национальные, межгосударственные и международные стандарты и методические документы ФСТЭК РФ в	уметь применять национальные, межгосударственные и международные стандарты и методические документы ФСТЭК России в области

		ласти защиты информации	области защиты информации	защиты информации
	ПКс-3 способен выполнять работы по обследованию объектов критической информационной инфраструктуры и разработке требований по защите информации	опыт обследования объектов КИИ и разработки требований по защите информации	знать порядок обследования объектов КИИ и методику разработки требований по защите информации	уметь определять объекты защиты; проводить анализ угроз безопасности информации, оценку рисков безопасности информации, строить модель угроз безопасности информации; категорировать объекты КИИ
	ПКс- 4 способен участвовать в разработке документации по организации системы защиты информации на объектах критической информационной инфраструктуры	опыт работы со сведениями, составляющими государственную или служебную тайну	знать порядок работы со сведениями, составляющими государственную или служебную тайну	уметь работать со сведениями, составляющими государственную или служебную тайну
	ПКс- 5 способен применять в профессиональной деятельности средства защиты информации	опыт применения в профессиональной деятельности средств защиты информации	знать принципы работы программно-аппаратных средств защиты информации, принципы алгоритмов защиты, основы защиты от разрушающих программных воздействий	уметь применять в профессиональной деятельности средства защиты информации
Осуществление мероприятий по вопросам информационной	ПКс-6 способен использовать в профессиональной деятельности законодательные и нормативные правовые акты субъекта РФ в области защиты информации и обеспечения безопасности персональных данных	опыт применения в профессиональной деятельности муниципальных правовых актов в области защиты информации и обеспечения безопасности персональных данных	знать муниципальные правовые акты в области защиты информации и обеспечения безопасности персональных данных	уметь применять муниципальные правовые акты в области защиты информации и обеспечения безопасности персональных данных
	ПКс-7 способен организовывать мероприятия по воздействию на риски ин-	опыт организации мероприятий по воздействию на	знать порядок организации и обеспечении безопасности	уметь организовывать мероприятия по воздействию на риски

без-опас-ности	формационной безопасности	риски информационной безопасности	хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом	информационной безопасности

1.4. Категория слушателей

К слушателям программы ДПО следует отнести муниципальных 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 и технологии обучения

Форма обучения – очно-заочная с применением дистанционных образовательных технологий (ДОТ). Очная часть аудиторная, без применения дистанционных образовательных технологий.

1.6. Период обучения, срок освоения и режим занятий

Трудоемкость программы повышения квалификации составляет 72 ак.часа, из них лекций 16 ак.часов; практических занятий 18 ак.часов; самостоятельной работы с применением дистанционных образовательных технологий 36 ак.часов; итоговая аттестация - 2 ак.часа.

Срок освоения программы составляет 2 недели. Режим занятий устанавливается по согласованию с заказчиком.

Итоговую аттестацию проводит преподаватель, реализующий программу.

1.7. Документ о квалификации

По окончании обучения слушателям выдается удостоверение о повышении квалификации федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации».

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 ДОТ (СР)/ТКУ ДОТ	УЗ ДОТ (СР)/ТКУ ДОТ
Неделя 2	УЗ/ТКУ	УЗ/ТКУ	УЗ ДОТ (СР)/ТКУ ДОТ	УЗ ДОТ (СР)/ТКУ ДОТ	УЗ/ТКУ/ИА

УЗ – учебные занятия;

ТКУ – текущий контроль успеваемости;

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий (СР- самостоятельная работа);

ТКУ ДОТ – текущий контроль успеваемости с применением дистанционных образовательных технологий

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.

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 (в т.ч. электронное обучение (ЭО), 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	Практические (семинарские занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции/ в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
1.	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	**Раздел 1. Информационная безопасность в деятельности органов государственной и муниципальной власти**	**50**	**26**	**12**	**14**				**24**					**24**	**Т**			
1.1	Тема 1. Порядок создания, развития, эксплуатации государственных информационных систем	6	2	2					4					4	Т			ПКс-1
1.2.	Тема 2. Нормативное регулирование информационной безопасности. Методические документы и национальные стандарты	10	6	2	4				4					4	Т			ПКс-6
1.3	Тема 3. Объекты защиты и угрозы безопасности информации	10	6	2	4				4					4	Т			ПКс-3
1.4	Тема 4. Система защиты данных информационных систем	8	4	2	2				4					4	Т			ПКс- 4 ПКс- 5

1.5	Тема 5. Обеспечение информационной безопасности при использовании муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов	10	6	2	4				4					4	Т			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	Т			ПКс-2
2.	**Раздел 2. Организация работы с персональными данными**	**20**	**8**	**4**	**4**				**12**					**12**	**Т**			
2.1	Тема 1. Обеспечение безопасности при обработке персональных данных	14	6	4	2				8					8	Т			ПКс-1 ПКс-3 ПКс- 5 ПКс-6
2.2	Тема 2. Аттестация информационных систем по требованиям защиты персональных данных	6	2		2				4					4	Т			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/темы* и его наименование	**Содержание *модуля/раздела/дисциплины/темы***
Раздел 1. Информационная безопасность в деятельности органов государственной и муниципальной 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 и муниципальной власти. Стратегические и нормативно-правовые документы, определяющие применение информационных технологий в системе государственного и муниципального 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 и муниципальные услуги в электронном виде. Подходы к повышению качества предоставления государственных и муниципальных 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	Объекты и субъекты информационной защиты. Свойства информации как объекта защиты. Риски угроз информационным

угрозы безопасности информации	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 муниципальными 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. Обеспечение безопасности при обработке 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 данных, 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 и муниципальной 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. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Риски и уязвимости обработки персональных данных в государственных и муниципальных учреждениях, модель угроз. Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации. Состав и содержание мер по обеспечению безопасности персональных данных. Организационно-административные меры защиты персональных данных. Политика конфиденциальности. Программно-технические средства защиты. Особенности использования средств криптографической защиты информации в рамках построения системы защиты персональных данных в организации. Основные мероприятия по обеспечению защиты персональных данных.
Тема 2. 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. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. 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 5

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 6

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 научной 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 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»

3.2 Учебно-методическое и информационное обеспечение программы

Раздел 1. Информационная безопасность в деятельности органов государственной и муниципальной власти

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

5. 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/

6. 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/

7. 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/

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

9. 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/

10. 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

11. 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. 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. — (Высшее 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/

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»

Раздел 2. Организация работы с персональными данными

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. 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/
6. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: https://base.garant.ru/71556224/
7. 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/

Основная литература

1. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 108 с. — ISBN 978-5-507-50458-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/437192. — Режим доступа: для авториз. пользователей.
2. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст

: электронный. - URL: https://znanium.ru/catalog/product/2169702 . – Режим доступа: по подписке.

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. 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.

3. 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.

4. 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.

5. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. – Москва : РГУП, 2025. - 220 с. – ISBN 978-5-00209-188-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2228306 . – Режим доступа: по подписке.

6. Нормативное сопровождение информационной безопасности : учебное пособие / С. И. Фокина, А. В. Выволокина, А. Ю. Гарькушев, А. В. Липис. – Москва ; Вологда : Инфра-Инженерия, 2025. - 136 с. – ISBN 978-5-9729-2530-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2225338 . – Режим доступа: по подписке.

7. 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.

8. Цифровизация гражданских правоотношений: проблемы теории и практики : монография / Т.Ю. Астапова, Н.В. Бандурина, М.Ю. Барышников [и др.] ; под общ. редакцией д-ра юрид. наук, доц. Н.В. Бандуриной, д-ра юрид. наук, проф. М.Н. Илюшиной. — Москва : ИНФРА-М, 2026. — 216 с. — (Науч-

ная мысль). — DOI 10.12737/2222623. - ISBN 978-5-16-021348-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2222623 . – Режим доступа: по подписке.

Интернет-ресурсы

1. Федеральный центр информационных образовательных ресурсов - URL: http://fcior.edu.ru/catalog/osnovnoe_obshee
2. Роскомнадзор - Портал персональных данных - URL: https://rkn.gov.ru/activity/personal-data/portal/
3. Федеральная служба по техническому и экспортному контролю - URL: https://fstec.ru/
4. Сервис подготовки документов по защите персональных данных - URL: https://b-152.ru/docs
5. Электронно-библиотечная система «Лань» // www.e.lanbook.com
6. Электронно-библиотечная система ЮРАЙТ // www.biblio-online.ru
7. Портал государственных услуг Российской Федерации - URL: https://www.gosuslugi.ru/
8. Сетевая безопасность — основы и 12 учебных ресурсов. - URL: https://toadmin.ru/сетевая-безопасность-основы-и-12-учеб/

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 проводится в виде письменного тестирования по каждой теме на последнем практическом занятии, его результаты учитываются при промежуточной аттестации.

Примерные вопросы для текущего контроля

Раздел 1. Информационная безопасность в деятельности органов государственной и муниципальной власти

Тема 1. Порядок создания, развития, эксплуатации государственных информационных систем

1. Государственные информационные системы – это:

а) системы, создаваемые государством для собственных нужд

б) системы, создаваемые с целью реализации полномочий государственных органов

в) системы, доступ к которым имеют только государственные органы

2. Какие показатели должны оцениваться при создании в органах государственной власти ИТ-инфраструктуры?

а) развитость, доступность, плотность инфраструктуры

б) наличие портала государственных услуг

в) стандарты и стоимость подключения к инфраструктуре

3. Что является основанием для начала эксплуатации ГИС?

а) наступление срока, установленного правовым актом государственного органа о вводе системы/очереди системы в эксплуатацию

б) приказ государственного органа о вводе системы/очереди системы в эксплуатацию

в) полное развертывание системы на месте ее будущей эксплуатации

4. Приоритетом формирования электронного государства в современной России не является …

а) формирование единого пространства доверия электронной цифровой подписи

б) внедрение системы голосования через Интернет

развитие системы межведомственного электронного взаимодействия

5. Назовите проблемы, входящие в перечень основных проблем развития электронного государства в современной России

а) проблема деградации образования

б) проблема информационной безопасности

в) проблема зависимости страны от импорта компьютерной техники

Тема 2. Нормативное регулирование информационной безопасности. Методические документы и национальные стандарты

1. Правовое обеспечение ИБ означает …

а) защиту интересов физических и юридических лиц

б) защиту интересов государства и общества

в) все вышеперечисленное

2. На законодательном уровне информационной безопасности особого внимания заслуживают

а) правовые акты и стандарты

б) разделение обязанностей и минимизация привилегий

в) документирование и регламентные работы

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

а) 1, 2

б) 2, 3

в) 1, 3

4. К правовым методам обеспечения информационной безопасности не относят:

а) разработку современных методов и средств защиты информации

б) определение ответственности физических и юридических лиц

в) повышение степени защищенности законных интересов граждан

5. Из скольких уровней состоит правовое обеспечение информационной безопасности?

а) двух уровней

б) трех уровней

в) четырех уровней

Тема 3. Объекты защиты и угрозы безопасности информации

1. Защищаемая информация – это

а) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации

в) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов

2. Основные объекты информационной безопасности -

а) информационные системы, психологическое состояние пользователей

б) компьютерные сети, базы данных

в) бизнес-ориентированные, коммерческие системы

3. Основными субъектами информационной безопасности являются:

а) руководители, менеджеры, администраторы компаний

б) органы права, государства, бизнеса

в) сетевые базы данных, фаерволлы

4. Основными рисками информационной безопасности являются:

а) искажение, уменьшение объема, перекодировка информации

б) техническое вмешательство, выведение из строя оборудования сети

в) потеря, искажение, утечка информации

5. Угроза – это…

а) потенциальная возможность определенным образом нарушить информационную безопасность

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

6. Что составляет основу политики безопасности?

а) выбор каналов связи

б) способ управления доступом

в) управление риском

7. Что является задачей анализа модели политики безопасности на основе анализа угроз системе?

а) максимизация затрат для взлома

б) максимизация ресурса для взлома

в) минимизация вероятности преодоления системы защиты

8. Наиболее распространены средства воздействия на сеть офиса:

а) слабый трафик, информационный обман, вирусы в интернет

б) вирусы в сети, логические мины (закладки), информационный перехват

в) компьютерные сбои, изменение администрирования, топологии

9. Наиболее распространены угрозы информационной безопасности корпоративной системы:

а) покупка нелицензионного по

б) ошибки эксплуатации и неумышленного изменения режима работы системы

в) сознательного внедрения сетевых вирусов

10. Наиболее распространены угрозы информационной безопасности сети:

а) распределенный доступ клиент, отказ оборудования

б) моральный износ сети, инсайдерство

в) сбой (отказ) оборудования, нелегальное копирование данных

Тема 4. Система защиты данных информационных систем

1. Наиболее важным при реализации защитных мер политики безопасности является:

а) аудит, анализ затрат на проведение защитных мер

б) аудит, анализ безопасности

в) аудит, анализ уязвимостей, риск-ситуаций

2. По способу осуществления всех мер обеспечения безопасности подразделяются на:

а) правовые и морально-этические

б) административные, физические, аппаратные и программные

в) все вышеперечисленное

3. Система защиты должна гарантировать, что любое движение данных:

а) идентифицируется, авторизуется, обнаруживается, документируется

б) контролируется, кодируется, фиксируется, шифруется

в) анализируется, идентифицируется, шифруется, учитывается

4. Организационное обеспечение информационной безопасности –

это..?

а) реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.

б) совокупность средств, обеспечивающих удобства работы пользователей

в) нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения

5. Для чего осуществляется разграничение доступа пользователей к ресурсам?

а) для того, чтобы запретить доступ каких-либо пользователей к информации

б) для того, чтобы каждый пользователь имел доступ только к той информации, на которую он уполномочен

в) для того чтобы доступ к ресурсам не казался слишком простым

6. Какими услугами ограничивается применение средств защиты физического уровня?

а) аутентификации

б) конфиденциальности

в) контроля доступа

7. Минимизация утечки информации через персонал это …

а) организационно-технические средства защиты информации

б) организационно-экономические меры

в) организационно-административные меры

8. Что является объектом программно-аппаратной защиты информации?

а) машинные носители информации

б) компьютерные системы

в) человек

9. Как определена услуга защиты «предотвращение неавторизованного использования ресурсов»?

а) причастность

б) аутентификация

в) контроль доступа

10. Какой метод защиты от вредоносных программ включает в себя использование специального программного обеспечения для сканирования системы на наличие угроз?

а) firewall

б) антивирусное ПО

в) обновления операционной системы

Тема 5. Обеспечение информационной безопасности при использовании муниципальными служащими социальных сетей, почтовых и иных интернет-сервисов

1. Уголовная и административная ответственность может

наступить при работе в сети Интернет за:

а) разглашение своих персональных данных

б) использование и распространение вредоносных компьютерных программ

в) нарушение этических норм

2. Какой пароль является наиболее безопасным для защиты аккаунта пользователя?

а) 1 234 567

б) +7 963 773-17-89

в) oPQ0nz$Hx4%!

3. Что является наиболее надежным механизмом для защиты содержания сообщений?

а) специальный аппаратный модуль

б) специальный режим передачи сообщения

в) криптография

4. Электронно-цифровая подпись – это

а) реквизит электронного документа, предназначенный для защиты данного документа от подделки, позволяющий идентифицировать владельца, а также установить отсутствие искажения информации в электронном документе

б) отсканированная подпись руководителя организации и помещенная в электронный документ для заверения подлинности данного документа

в) такой подписи не бывает т.к. подлинность документа заверяется личной подписью руководителя организации и печатью

5. Какой Интернет-протокол является безопасным?

а) ftp://

б) https://

в) http://

6. Спам - это:

а) ненужные адресату электронные послания, рекламные письма и т. п., рассылаемые отдельными фирмами по Интернету или электронной почте

б) вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

в) вредоносная программа, главной задачей которой может быть повреждение системы, на которой она установлена, перехват информации с компьютера и саморепликация — способность к размножению

7. Фишинг – это

а) разглашение открытой в СМИ информации

б) воровство конфиденциальной информации о пользователе, в частности, с помощью подложных писем

в) специальное приложение для перехода к рекламе

8. Когда получен спам по e-mail с приложенным файлом, следует:

а) прочитать приложение, если оно не содержит ничего ценного – удалить

б) сохранить приложение в парке «Спам», выяснить затем IP-адрес

в) удалить письмо с приложением, не раскрывая (не читая) его

9. Информационными угрозами в сети Интернет НЕ являются:

а) несанкционированный доступ к сети организации

б) сбор и мониторинг сетевой информации в интересах третьих лиц

в) использование брандмауэра

10. Для защиты электронной почты в Интернете используются:

а) антивирусные программы

б) специальные протоколы (REM, CryptoAPi и др.)

в) наиболее простое обозначение электронной почты (фамилия, паспортные данные и т.п.

Тема 6. Сертификация средств защиты информации. Аттестация информационных систем по требованиям защиты информации

1. Деятельность по подтверждению соответствия СЗИ требованиям безопасности информации – это

а) аттестация

б) сертификация

в) верификация

2. Что удостоверяет сертификат соответствия в сфере защиты информации?

а) право организации заниматься деятельностью в сфере защиты информации

б) соответствие помещений организации требованиям пожарной безопасности

в) соответствие параметров программных средств требованиям технических

3. Как называется процедура сертификации объектов информатизации?

а) сертификация

б) лицензирование

в) аттестация

4. Кто утверждает паспорт на объект информатизации, прошедший аттестацию?

а) председатель аттестационной комиссии

б) руководитель организации

в) руководитель органа по сертификации

5. Требования ФСТЭК по защите конфиденциальной информации …

а) подбираются с учетом структуры СЗИ, состава и мест размещения ее элементов. Если защищаемая ИС проектируется в составе центра обработки данных (ЦОД) рекомендуется использовать уже имеющиеся в ЦОД средства, меры защиты данных

б) направлены на исключение неправомерного доступа, копирования,

передачи или распространения сведений. Для обеспечения требований по безопасности конфиденциальной информации проводится оценка возможных уязвимостей ИС для внешних и внутренних нарушителей, возможных средств реализации этих уязвимостей

в) должны обеспечивать необходимый уровень безопасности при взаимодействии защищаемых ИС с другими ИС, при обработке и хранении информации. При этом предлагаемые на этапе проектирования меры должны быть реализуемы в конкретной ИС

Раздел 2. Организация работы с персональными данными

Тема 1. Обеспечение безопасности при обработке персональных данных

1. Целью Федерального закона от 27.07.2006 № 152-ФЗ является:

а) контроль за обработкой персональных данных операторами персональных данных

б) обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

в) соответствие законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981года

2. Что такое персональные данные?

а) любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)

б) информация о частной жизни физического лица, доступ к которой он решил ограничить

в) сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных

3. Что понимается под понятием «Конфиденциальность персональных данных»?

а) обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных

б) обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом

в) обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных или наличия иного законного основания

4. Информационная система персональных данных – это

а) пользователь, средства автоматизации, базы данных

б) контролируемое пространство, в котором происходит обработка персональных данных

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

средств

5. Какие меры по обеспечению безопасности персональных данных при неавтоматизированной обработке являются обязательными в соответствии с постановлением Правительства РФ от 15.09.2008г. № 687?

а) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

б) использование средств контроля и управлении доступом;

в) должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним. перечень мер, необходимых для обеспечения таких условий, порядок их принятия, устанавливаются оператором

Тема 2. Аттестация информационных систем по требованиям защиты персональных данных

1. Аттестация информационных систем персональных данных (ИСПДн) — это …

а) процедура проверки системы защиты персональных данных на соответствие требованиям законодательства и установленным нормам безопасности

б) процедура сертификации объектов информатизации

в) деятельность по подтверждению соответствия ИСПДн требованиям безопасности информации

2. Цель аттестации информационных систем персональных данных (ИСПДн) -

а) подтверждение надёжности защиты персональных данных и соответствие системы нормативным требованиям

б) подтверждение соответствия сертифицированных средств защиты информации требованиям безопасности информации

в) обеспечение защиты персональных данных

3. Кто проводит аттестацию ИСПДн?

а) оператор персональных данных

б) регулятор в области защиты информации

в) организации, имеющие лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации

4. Кем регламентируются конкретные требования по защите ИСПДн?

а) Правительством РФ

б) регуляторами в области защиты информации

в) лицензиатом ФСТЭК России

5. Кто проводит организационные (разработка модели угроз, техническое задание на систему защиты, технический проект, технический паспорт на СЗИ, комплект эксплуатационной и организационно-распорядительной документации) и технические (внедрение средств защиты информации и их

настройка по требованиям безопасности) мероприятия по подготовке к аттестации ИСПДн по требованиям безопасности информации?

а) оператор персональных данных

б) регулятор в области защиты информации

в) организации, имеющие лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации

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: итоговое тестирование (25 баллов).

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

Трудоемкость итоговой аттестации: 2 академических часа.

Итоговая аттестация может проводится с применением ЭО и ДОТ.

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 зашифрованные 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 7

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.

Итоговую аттестацию проводит преподаватель, реализующий программу.

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы компетенции:

Таблица 8

Индикаторы сформированности компетенций

Компетенция (код, содержание)	**Индикаторы**
ПКс-1	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 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	Знает методику обследования объектов критической информационной инфраструктуры Умеет разрабатывать требования по защите информации
ПКс- 4	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	Знает правовые, инженерно-технические и программные меры по обеспечению информационной безопасности. Умеет выбирать и применять средства защиты информации
ПКс-6	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	Знает методику выявления рисков информационной безопасности. Умеет организовывать мероприятия по воздействию на риски информационной безопасности