Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«25» 05 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Организационное и правовое обеспечение информационной безопасности

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019, 2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*7*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2020

Разработчик рабочей программы:

Доцент ИБАС — Власов В.А.

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС — Лошманов А.Ю.

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Обеспечение информационной безопасности распределенных информационных систем» по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Задачи дисциплины	Приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем, формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.
Основные разделы / темы дисциплины	1. Проектирование системы защиты ИСПДн (Информационной системы обрабатывающей персональные данные) 2. Модели угроз и нарушителя 3. Создание системы защиты ИСПДн

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);	З1(ПК-16) Основные нормативно-технические документы по автоматизированным системам	У1(ПК-16) Использовать нормативно-технические документы при аттестации автоматизированных систем	Н1(ПК-16) Проведения экспериментально-исследовательских работ при аттестации объектов информатизации
Способность участвовать в формировании политики информационной безопасности организа-	З1(ПК-22) О структуре политики информационной безопасности в организации	У1(ПК-22) Разрабатывать политику информационной безопасности в организации	Н1(ПК-22)) Участия в проведении проверок политики информационной без-

ции и контролировать эффективность ее реализации (ПК 22)			опасности

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается на 4 курсе(ах) в 7 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик Разработка и эксплуатация защищенных автоматизированных систем. Знания, умения и навыки, сформированные при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности», будут востребованы при изучении последующих дисциплин «Стандартизация защищенных автоматизированных систем», «Управление инновационными проектами»

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 з.е., 180- акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	180
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	64
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	80
Промежуточная аттестация обучающихся – Экзамен	36

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 1 Проектирование системы защиты ИСПДн (Информационной системы обрабатывающей персональные данные) Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения	10		10	25

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Общий порядок проектирования ИСПДн. Руководящие документы Гостехкомиссии России (ФСТЭК России). Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Формирование уведомление об автоматизированной обработке персональных данных Формирование комплекта документов для выполнения требований Роскомнадзора по обеспечению информационной безопасности персональных данных в ИСПДн класса К1				
Раздел 2 Модели угроз и нарушителя Понятие модели угроз. Понятие модели нарушителя. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз и моделей нарушителя в автоматизированных системах Практические подходы к разработке моделей угроз и моделей нарушителя Понятие персональных данных. Понятие ИСПДн. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России). Проведение аудиторской проверки Роскомнадзора	10		10	25
Раздел 3 Создание системы защиты ИСПДн Практические рекомендации по разработке моделей угроз и моделей нарушителя. Основные категории средств защиты ИСПДн. Рекомендации по выбору средств защиты. Сертификация средств защиты ИСПДн. Особенности лицензирования соответствующих видов деятельности. Аттестация ИСПДн. Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса	12		12	30

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Органы государственной власти, осуществляющие контроль в области защиты информации. Основные функции и полномочия. Состав и комплектность документов на ИСПДн. Законодательная база в области обеспечения информационной безопасности персональных данных. Требования по НСД, АС, МЭ для ИСПДн различных классов. Требования по шифрованию ПДн при передаче по открытым каналам связи.				
ИТОГО по дисциплине	**32**		**32**	**80**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	15
Подготовка к занятиям семинарского типа	15
Подготовка и оформление РГР	50
	80

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-Амуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2014. - 207с. - Библиогр.: с.201-207. - 273-00.

2. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./НовиковВ.К. - М.: Гор. линия-Телеком, 2015.- 176с.:60x88 1/16 (О) ISBN 978-5-9912-0525-2, 500 экз. - Режим доступа: http://znanium.com/catalog/product/536932

3. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - М.:Гор. линия-Телеком, 2016. - 248 с.: 60x90 1/16. - (Специальность) (Обложка) ISBN 978-5-9912-0470-5 - Режим доступа: http://znanium.com/catalog/product/973806

4. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.И. Коваленко. - М.: Гор. линия-Телеком, 2012. - 140 с.: ил.; 60x88 1/16. - (Специальность). (обложка) ISBN 978-5-9912-0261-9, 500 экз. - Режим доступа: http://znanium.com/catalog/product/358911

8.2 Дополнительная литература

1. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60x90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246-3 - Режим доступа: http://znanium.com/catalog/product/167284

2. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2012. — 98 c. — 9965-756-05-8. — Режим доступа: http://www.iprbookshop.ru/67055.html

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

4. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8 - Режим доступа: http://znanium.com/catalog/product/491597

5. Об информации, информационных технологиях и о защите информации: [Электронный ресурс] : федер. закон от 27 июля 2007 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Организационное и правовое обеспечение информационной безопасности» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять

	ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Организация и технология защиты конфиденциальной информации в информационных системах» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты РГР;

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+
3. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. 1. Об информации, информационных технологиях и о защите информации: [Электронный ресурс] : федер. закон от 27 июля 2007 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
2. 2. О персональных данных : [Электронный ресурс] : федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. 3. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
4. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендозанную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению расчетно-графической работы

Теоретическая часть расчетно-графической работы выполняется по установленным темам с использованием практических материалов. К каждой теме расчетно-графической работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои пред-

ложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV
201/5	Лаборатория технических средств и методов защиты информации	специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок: Соната АВ с оконечными устройствами (виброизлучатели, акустические излучатели), генератор шума электромагнитного поля ВетоМ, генератор ЛГШ 503, генератор Соната РС-1 Технические средства контроля эффективности защиты информации от утечки по указанным каналам: Комплект измерительных антенн Альбатрос 3, селективный микровольтмерт SMV 8,5, селективный микровольтметр SMV 11, комплекс Спрут-мини-А в комплекте с программным обеспечением, Unipan 233, ПЭВМ семества Secret, Поисковый прибор ST033P Пиранья в комплекте с программным обеспечением. иное дополнительное оборудование: нелинейный локатор NR-m, генератор сигналов АКИП 3410, комплект измерительных антенн Альбатрос, пробник напряжения СРФ-1, антенны DP-1 и DP-3, генераторы сигналов

		серии Г3 и Г4. Комплект тестовых программ Зебра для Windows, для МСВС лицензия номер 592

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_201_, оснащенная оборудованием, указанным в табл. 6:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 203 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установления полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Организационное и правовое обеспечение информационной безопасности автоматизированных систем

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019, 2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*7*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);	З1(ПК-16) Основные нормативно-технические документы по автоматизированным системам	У1(ПК-16) Использовать нормативно-технические документы при аттестации автоматизированных систем	Н1(ПК-16) Проведения экспериментально-исследовательских работ при аттестации объектов информатизации
Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК 22)	З1(ПК-22) О структуре политики информационной безопасности в организации	У1(ПК-22) Разрабатывать политику информационной безопасности в организации	Н1(ПК-22)) Участия в проведении проверок политики информационной безопасности

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
1. Проектирование системы защиты ИСПДн (Информационной системы обрабатывающей персональные данные)	ПК-16	Лабораторная работа	Умение провести аудит и спроектировать систему защиты ИСПДн.
2. Модели угроз и нарушителя	ПК-22	Лабораторная работа	Умение Разработать модель угроз и модель нарушителя

3. Создание системы защиты ИСПДн	ПК-16	Лабораторная работа	Умение предложить рекомендации по системе защиты информации для заданной ИСПДн
Разработка комплекта документов.	ПК-16 ПК-22	Расчетно-графическая работа	Показывает умения и навыки по разработке комплекта документов на информационную систему обрабатывающую персональные данные
Темы 1,2,3.	ПК-16 ПК-22	Экзамен	Показывает знания и умения по всем 3 темам.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
4 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания,

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Лабораторная работа 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Расчетно-графическая работа 1	В течение семестра	15 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите. 10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
		45 баллов		
Текущий контроль:			45 баллов	
ИТОГО:			45 баллов	

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Лабораторные работы

Варианты для выполнения лабораторных работ совпадают с вариантами для расчетно-графической работы.

Тема № 1 Проектирование системы защиты ИСПДн (Информационной системы обрабатывающей персональные данные).

Задание 1: Провести аудит типовой автономной ИСПДн

Задание 2: Спроектировать систему защиты типовой автономной ИСПДн.

Тема № 2 Модели угроз и нарушителя.

Задание 1: Разработать модель угроз для типовой автономной ИСПДн;

Задание 2: Разработать модель нарушителя типовой автономной ИСПДн.

Тема № 3 Разработка комплекта документов.

Задание 1 Разработать документ, отвечающий за парольную защиту в ИСПДн.

Задание 2: Разработать инструкцию администратора безопасности информационной системы.

Задание для расчетно-графической работы

Контрольная работа по дисциплине «Организационное и правовое обеспечение информационной безопасности» проводится в интерактивной форме – форме деловых игр, отражающих проведение реальных аудиторских проверок «регуляторов». Всего в семестре устанавливается несколько контрольных точек по неделям:

2-я неделя – подача уведомления в «Роскомнадзор»(передача уведомления преподавателю).

5-я неделя – аудиторская проверка «Роскомнадзора».

10-я неделя – аудиторская проверка «ФСТЭК РФ».

15-я неделя – аудиторская проверка «ФСБ РФ».

Схемы контролируемой зоны, расположения средств вычислительной техники, средств защиты, электропитания и заземления необходимо согласовывать с преподавателем. В личном кабинете необходимо разместить спецификации.

Ко второй неделе необходимо подготовить уведомление об обработке персональных данных. Пример уведомления приведен в рабочей программе далее, к 5-ой неделе комплект документов в соответствии со спецификацией приведенной в в рабочей программе далее для Роскомнадзора, к 10 неделе комплект документов в соответствии со спецификацией приведенной в в рабочей программе далее для ФСТЭК, к 15 неделе комплект документов в соответствии со спецификацией приведенной в в рабочей программе далее для ФСБ. В каждом варианте обязательно в организации обеспечением информационной безопасности которой занимается студент ведется автоматизированная обработка более чем 100 000 субъектов персональных данных. Обязательно есть необходимость использовать технические средства защиты информации от утечек по техническим каналам, средства защиты от несанкционированного доступа, средства криптографической защиты информации. Ответственным за обеспечение информационной безопасности в организации назначается студент.

Нужно учесть, что если количество ИСПДн в организации больше одной, то некоторые документы представляются по каждой ИСПДн в отдельности. Спецификации подаваемых документов подлежат обязательному согласованию с преподавателем.

Варианты заданий

№	Наименование организации	ФИО Руководителя	Средства защиты от НСД	Криптографические средства	Количество ИСПДн	Технические средства защиты
1	Медико-диагностический центр	Скорая Снежана Сергеевна	1	111	1	А
2	Аппарат Президента	Путин Владимир Владимирович	2	112	2	Б
3	Налоговая	Денежная Виктория Павловна	3	113	1	А
4	Пенсионный фонд	Бабулина Ирина Витальевна	4	111	2	Б
5	КнАГТУ	Ученый Александр Иванович	5	112	1	А
6	Архив библиотеки	Белых Сергей Сергеевич	1	113	2	Б
7	Администрация города	Медведев Илья Игоревич	2	111	1	А

8	Амурский судостроительный завод	Шорохов Сергей Иванович	3	114	2	Б
9	Отдел социальной помощи населению	Добрый Сергей Иванович	4	113	1	А
10	Завод Вымпел	Быстрый Иван Андреевич	5	111	2	Б
11	МОУ СОШ 18	Птичкина Надежда Юрьевна	1	112	1	А
12	ЗАО МТС	Большаков Андрей Михайлович	2	114	2	Б
13	Отдел записи актов гражданского бракосочетания	Силин Антон Федорович	3	111	1	А

Перечень средств защиты от НСД

1. Secret Net 6.5
2. Dallas Lock 7.7
3. Accord
4. Аура
5. Страж NT

Перечень средств криптографической защиты

1. АПКШ Континент клиентская часть Континент АП.
2. ФПСУ/IP клиентская часть ФПСУ/IP клиент.
3. CheckPoint Connectra клиентская часть Connectra client.
4. VipNet HW 1000 клиентская часть VipNet Client.

Перечень технических средств защиты

1. Соната, ЛГШ-1000, Корунд.
2. Барон, Вето-М, Прокруст 2000.

Примеры документов и могут быть свободно скачаны с сайта университета. По согласованию с преподавателем задания для выполнения могут быть изменены или расширены. Примеры документов и перечень приведены в приложении А.

Вопросы для защиты лабораторных работ и расчетно-графической работы

1. Органы государственной власти, осуществляющие контроль в области защиты информации.
2. Основные функции и полномочия.
3. Состав и комплектность документов на ИСПДн.
4. Законодательная база в области обеспечения информационной безопасности персональных данных.
5. Требования по НСД.

6. Требования к АС
7. Требования к МЭ для ИСПДн различных классов.
8. Требования по шифрованию ПДн при передаче по открытым каналам связи.
9. Практические рекомендации по разработке моделей угроз и моделей нарушителя.
10. Основные категории средств защиты ИСПДн.
11. Рекомендации по выбору средств защиты.
12. Сертификация средств защиты ИСПДн.
13. Особенности лицензирования соответствующих видов деятельности.
14. Аттестация ИСПДн.
15. Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса.
16. Понятие персональных данных.
17. Понятие ИСПДн.
18. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).
19. Требования к ИСПДн.
20. Классификация АС.
21. Обезличивание персональных данных.
22. Типовые модели угроз и модели нарушителя.
23. Понятие модели угроз. Понятие модели нарушителя.
24. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз и моделей нарушителя в автоматизированных системах.
25. Практические подходы к разработке моделей угроз и моделей нарушителя.
26. Общий порядок проектирования ИСПДн.
27. Руководящие документы Гостехкомиссии России (ФСТЭК России).
28. Понятие автоматизированной системы.
29. Особенности автоматизированных систем в защищенном исполнении.
30. Основные виды АС в защищенном исполнении.
31. Особенности обработки персональных данных без использования средств автоматизации.
32. Угрозы безопасности персональных данных.
33. Утечка по техническим каналам как угроза безопасности персональных данных.
34. Ключевые объекты инфраструктуры.
35. Лицензирование деятельности по защите персональных данных и конфиденциальной информации.
36. Системы резервного копирования и способы его осуществления.
37. Применение СЗИ от НСД для ИСПДн класса К1.
38. Основные требования к РКІ.

39. Конфиденциальность, целостность, доступность. Методы и способы обеспечения.
40. Целостность. ЭЦП.

Приложение А.

Перечень документов для сдачи при проверке Роскомнадзор

Номер, п/п	Наименование
1.	Уведомление об обработке ПДн
2.	Положение о подразделении по защите ПДн
3.	Положение о порядке организации и проведения работ по обеспечению безопасности ПДн при их обработке Положение о ПДн
4.	Положение о ПДн
5.	Положение об обработке ПДн без средств автоматизации
6.	Положение об обращении с информацией конфиденциального характера
7.	Положение о разграничении прав доступа
8.	Распоряжение об утверждении перечня сотрудников, допущенных к обработке ПДН и перечня помещений, предназначенных для обработки ПДН
9.	Перечень сотрудников, допущенных к обработке ПДн
10.	Перечень помещений
11.	Приказ об утверждении Положения об обеспечении пропускного и внутриобъектового режимов
12.	Положение об обеспечении пропускного и внутриобъектового режимов
13.	Приказ о введении в действие системы контроля и управления доступом
14.	Инструкция пользователей карт доступа, предназначенных для прохода через СКУД
15.	Приказ о доступе работников к информационным ресурсам
16.	Приказ о порядке хранения конфиденциальной информации на электронных носителях
17.	Приказ о назначении ответственных в подразделениях организации за эксплуатацию средств защиты информации
18.	Приказ о формировании системы обеспечения безопасности информации
19.	Приказ о местах хранения персональных данных ИСПДн-1
20.	Приказ о местах хранения персональных данных ИСПДн-2 (ПДн сотрудников)
21.	Акт приема зачета по знанию нормативной базы, определяющей порядок работы с ПДН
22.	Список сотрудников, ознакомленных с законодательными актами и нормативными документами, определяющими порядок работы с ПДН
23.	Приказ об утверждении перечня должностных лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование ПДН
24.	Приказ о проведении внутренней проверки
25.	Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах
26.	Инструкция пользователя ИСПДн

27.	Журнал учета обращений субъектов ПДн
28.	Личная карточка сотрудника по форме Т-2
29.	Документ, регламентирующий разбирательство в случае несоблюдения условий защиты ПДн
30.	Заявление субъекта ПДн на отзыв согласия
31.	Концепция информационной безопасности
32.	Политика информационной безопасности
33.	Приказ о назначении лиц. ответственных за обеспечение безопасности персональных
34.	Журнал учета однократного пропуска
35.	Положение об электронном журнале

Перечень документов при проверке ФСТЭК

Номер, п/п	Наименование
1.	О создании комиссии по оценке угроз безопасности информационной системы персональных данных
2.	Положение о комиссии по классификации информационных систем персональных данных
3.	План мероприятий по защите персональных данных в информационных системах персональных данных
4.	Частная модель угроз безопасности персональных данных
5.	Перечень информационных систем персональных данных
6.	Описание технологического процесса обработки персональных данных в информационных системах
7.	Отчет о результатах проведения внутренней проверки
8.	Акт классификации информационной системы персональных данных АИС «Клиенты»
9.	Акт классификации информационной системы персональных данных АИС «СЭОД»
10.	Акт классификации информационной системы персональных данных АИС «Отдел кадров»
11.	Акт классификации информационной системы персональных данных АИС «Бухгалтерия»
12.	Аттестат соответствия АИС «Клиенты»
13.	Аттестат соответствия АИС «СЭОД»
14.	Аттестат соответствия АИС «Отдел кадров»
15.	Аттестат соответствия АИС «Бухгалтерия»
16.	Приказ о закреплении контролируемой зоны
17.	Схема контролируемой зоны помещения
18.	Приказ о создании комиссии по оценке угроз безопасности информационной системы персональных данных
19.	Протокол оценки вероятности реализации угроз
20.	Программа и методика проведения аттестационных испытаний
21.	Частное техническое задание на систему защиты ПДн
22.	Протокол испытаний автоматизированной системы на соответствие требованиям по безопасности информации
23.	Акт внедрения средств защиты информации
24.	Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним
25.	Типовая заявка на подключение к сети интернет
26.	Политика безопасности рабочих станций и серверов
27.	Политика использования паролей
28.	*Журнал учета парольных карт*
29.	Политика идентификации пользователей в локальной вычислительной сети

30.	Инструкция о порядке отнесения информационных ресурсов к защищаемым
31.	Инструкция по внесению изменений в списки пользователей и наделению их полномочиями
32.	Инструкция по защите речевой информации при проведении конфиденциальных совещаний
33.	Инструкция по организации антивирусной защиты
34.	Инструкция по организации парольной защиты
35.	Инструкция пользователя в случае обнаружения компьютерных атак
36.	Памятка пользователю АС в части обеспечения безопасности информации
37.	Приказ об утверждении Временного порядка резервного копирования, архивного хранения и восстановления данных информационных систем
38.	Инструкция о порядке организации резервного копирования, архивного хранения и восстановления данных информационных систем
39.	Инструкциян о безопасной эксплуатации СКЗИ
40.	Инструкция администратора безопасности ИСПДн
41.	Инструкция администратора по информационной безопасности
42.	Инструкция пользователю по соблюдению режима защиты информации при работе на АРМ и в ЛВС
43.	Журнал учета средств криптографической защиты информации
44.	Журнал учета информационных ресурсов
45.	Журнал учета внешних носителей
46.	Инструкция МЭ
47.	Перечень сертифицированных межсетевых экранов
48.	Журнал периодического инструктажа
49.	Распоряжение об утверждении перечня сотрудников, допущенных к обработке персональных данных и перечня помещений, предназначенных для обработки персональных данных
50.	Перечень закрепленных ПЭВМ, предназначенных для обработки персональных данных и назначении лиц допущенных к обработке
51.	Перечень помещений
52.	Приказ о порядке использования в помещениях организации радиотелефонов, сотовых и пейджинговых устройств при проведении конфиденциальных совещаний
53.	Журнал доведения инструкций
54.	Журнал учета распорядительных документов
55.	Приказ об утверждении перечня программного обеспечения и обрабатываемых персональных данных
56.	Перечень программного обеспечения обрабатываемых персональных данных
57.	Типовая форма плана устранения недостатков и замечаний
58.	Журнал учета и содержания средств защиты
59.	Регламент обмена документами с использованием СЭД
60.	Инструкция по обеспечению мер пожарной безопасности
61.	Инструкция пользователю системы электронного документооборота
62.	Приказ о назначении ответственных за внедрение, дальнейшее сопровождение

	и эксплуатацию ПО
63.	ПРОТОКОЛ испытаний автоматизированной системы «Клиенты» на соответствие требованиям по безопасности информации
64.	Инструкция правила пользования ресурсами ЛВС
65.	Перечень внутренних и публичных сетевых ресурсов ЛВС
66.	Заявка на подключение к сети Интернет
67.	ПРОТОКОЛ Измерения сопротивления заземления на объектах ВТ
68.	ПРИКАЗ О вводе в эксплуатацию АС
69.	Журнал учета работы в сети интернет
70.	Журнал **периодического инструктажа на рабочем месте**
71.	Перечень технических средствзащиты информации
72.	Перечень сертифицированных средств защиты от несанкционированного доступа
73.	Перечень СКЗИ
74.	Перечень IDS
75.	Перечень сертифицированных средств антивирусной защиты
76.	*Акт уничтожения съемных носителей персональных данных*
77.	ПРЕДПИСАНИЕ НА ЭКСПЛУАТАЦИЮ объекта вычислительной техники
78.	Приказ Об усилении пожарной безопасности
79.	Журнал инструктажа Пользователей с правилами работы с сетью Интернет и средствами электронной почты
80.	Типичные угрозы при работе с сетью Интернет и электронной почтой
81.	Общие меры предосторожности при работе с сетью Интернет и электронной почтой
82.	ПАМЯТКА по подготовке и контролю парольной карты
83.	*ИНСТРУКЦИЯ пользователю автоматизированных систем в случае возникновения внештатных ситуаций*
84.	ВЕДОМОСТЬ приема зачета по знанию нормативной базы, определяющей порядок работы с персональными данными
85.	План по контролю состояния систем защиты СКЗИ, НСД, технической
86.	*Журнал учета обращений органов с запросами ПДн работников*
87.	АТТЕСТАТ СООТВЕТСТВИЯ требованиям по безопасности информации автоматизированной системы
88.	Инструкция пользования ГШ-2500
89.	О разрешении аттестационной комиссии к информации «для служебного пользования

Перечень документов при проверке ФСБ

Номер, п/п	Наименование
1.	Приказ о создании режимно-секретного отдела
2.	Положение с режимно-секретном отделе
3.	Должностная инструкция начальника режимно-секретного отдела
4.	Перечень обрабатываемых сведений, содержащих гостайну
5.	Положение об обработке сведений, составляющих гостайну
6.	Инструкция по обработке информации, содержащую гостайну
7.	Список сотрудников, ознакомленных с документами, составляющими гостайну
8.	Матрица доступа сотрудников в помещение режимно-секретного отдела
9.	Модель нарушителя
10.	Акт об отсутствии в помещении режимно-секретного отдела средств вычислительной техники
11.	**Технический паспорт на выделенное помещение**
12.	**Аттестат соответствия №1 Режимно-секретный отдел**
13.	**Инструкция о порядке обращения с выделенным помещением**
14.	*Список сотрудников, допущенных в выделенное помещение*
15.	*Список лиц допущенных к серверную*
16.	План мероприятий по защите секретной информации
17.	Приказ об организации доступа к средству обработки секретной информации
18.	Приказ об обязательном повышении квалификации сотрудников допущенных к работе со средствами криптографической защиты
19.	Перечень криптографических средств
20.	Приказ о создании систем криптографической защиты
21.	Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ
22.	Инструкция об уничтожении информации
23.	Инструкция по использованию средств защиты информации
24.	Порядок проведения служебного расследования
25.	Заявка на запись на внешний носитель
26.	**Журнал движения средств ввода**
27.	Журнал регистрации попыток НСД
28.	Акт категорирования ВП
29.	**Журнал учета времени работы со средством ввода секретной информации**
30.	Журнал учета уничтожения информации

31.	Журнал учета парольных карт
32.	*Журнал поступающих документов*
33.	Журнал передачи документов
34.	Должностные обязанности администратора безопасности
35.	Политика управления парольной защитой
36.	Памятка по подготовке и контролю парольной карты
37.	Акт спецобследования ВП
38.	Приказ о вводе в эксплуатацию объекта ВТ
39.	Приказ о назначении комиссии по категорированию и проведению специального обследования объектов ВТ
40.	Перечень сертифицированных антивирусов
41.	Журнал учета времени работы на СВТ
42.	Журнал движения СВТ
43.	Протоколы инструментального контроля (АВАК, АЭП, ПЭМИН)
44.	Схема РСО
45.	Схема СВТ
46.	Схема проводки
47.	Схема телефонки
48.	Схема пожарной сигнализации
49.	Схема охранной сигнализации
50.	Журнал приёма-передачи СВТ и учёта времени обработки информации

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД