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)
«01» 06 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность распределенных информационных систем

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*6*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС – Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

к.ф.-м.н., доцент	 (подпись)	А.Ю. Лошманов
(должность, степень, ученое звание)		(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС	 (подпись)	А.Ю. Лошманов
(наименование кафедры)		(ФИО)

1 Общие положения

Рабочая программа дисциплины «Введение в профессиоанльную деятельность» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства науки и высшего образования Российской Федерации № 1457 от 26.11.2020, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:

Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857.

Задачи дисциплины	Ознакомить студентов с порядком создания информационных систем на базе АРМ, в защищенном исполнении. Овладение основными теоретическими и практическими навыками проектирования и эксплуатации распределенных информационных систем
Основные разделы / темы дисциплины	1. Теоретические основы построения защищенных распределенных информационных систем. 2. Лабораторные аспекты построения защищенных распределенных информационных систем.

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

Процесс изучения дисциплины «Информационная безопасность распределенных информационных систем» 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

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
ПК-6: Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	ПК-6.1 Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	ПК-6.2 Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	ПК-6.3 Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность распределенных информационных систем» изучается на 4 курсе в 8 семестре.

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к дисциплинам по выбору.

Дисциплина «Информационная безопасность распределенных информационных систем» основывается на знаниях, умениях и навыках, полученных при изучении дисциплин по выбору: «Администрирование распределенных информационных систем»

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 6 з.е., 216 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	216
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	116
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	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
Раздел 1. Теоретические основы построения защищенных распределенных информационных систем					
Нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты	Лекция	3	Традиционная	ПК-6	ПК-6.1
Федеральные органы исполнительной власти и их требования по построению защищенных распределенных информационных систем	Лекция	4	Интерактивная (презентация)	ПК-6	ПК-6.1
Требования и рекомендации по построению информационных систем в виде изолированных рабочих мест	Лекция	5	Интерактивная (презентация)	ПК-6	ПК-6.1
Организационно-распорядительная документация по обеспечению информационной безопасности распределенных информационных систем	Лекция	4	Традиционная	ПК-6	ПК-6.1
Настройка защищенных каналов доступа в распределенных информационных системах	Лабораторная работа	16	Традиционная	ПК-6	ПК-6.2, 6.3
Текущий контроль по разделу 1					
Итого по разделу 1	Лекции	16			

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
	Лабораторные работы	16			
	Самостоятельная работа	58			
	Самостоятельная работа обучающихся (подготовка к лабораторным занятиям)	4	Освоение электронных материалов по дисциплине.	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (изучение теоретических разделов дисциплины)	4	Чтение основной и дополнительной литературы, конспектирование	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (подготовка и оформление РГР и КР)	50	Чтение основной и дополнительной литературы, конспектирование, оформление	ПК-6	ПК-6.2, 6.3
Раздел 2. Лабораторные аспекты построения защищенных распределенных информационных систем.					
Информационные системы как совокупность распределенных автоматизированных рабочих мест объединенных в локальные вычислительные сети	Лекция	5	Интерактивная (презентация)	ПК-6	ПК-6.1
Методы и средства защиты информационных систем с доступом к глобальной сети информационного обмена Internet	Лекция	5	Традиционная	ПК-6	ПК-6.1
Межсетевое экранирование и системы обнаружения и предотвращения вторжений, системы углубленного анализа пакетов	Лекция	3	Традиционная	ПК-6	ПК-6.1
Описание информационных систем в соответствии	Лекция	3	Традиционная	ПК-6	ПК-6.1

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
с OSI. Использование шлюзов доступа, SSH, SSL.					
Использование шлюзов доступа в распределенных информационных системах	Лабораторная работа	16	Традиционная	ПК-6	ПК-6.2, 6.3
Текущий контроль по разделу 2					
Итого по разделу 2	Лекции	16			
	Лабораторные работы	16			
	Самостоятельная работа	58			
	Самостоятельная работа обучающихся (подготовка к лабораторным занятиям)	4	Освоение электронных материалов по дисциплине.	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (изучение теоретических разделов дисциплины)	4	Чтение основной и дополнительной литературы, конспектирование	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (подготовка и оформление РГР, собеседование)	50	Чтение основной и дополнительной литературы, конспектирование, оформление	ПК-6	ПК-6.2, 6.3
Промежуточная аттестация по дисциплине в 8-м семестре		36	Экзамен	ПК-6	
ИТОГО по дисциплине в 8-м семестре	Лекции	32	-	-	-
	Лабораторные работы	32	-	-	-
	Контроль	36			
	Самостоятельная работа обучающихся	116	-	-	-
ИТОГО: общая трудоемкость дисциплины 216 часа					

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	8
Подготовка к занятиям семинарского типа	8
Подготовка и оформление контрольной работы, работа над курсовой работой	100
	116

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.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 5).

Таблица 5 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
Промежуточная аттестация в форме экзамена				
1	Лабораторная работа 1	2 – 3 недели семестра	10 баллов	10 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 6 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
2	Лабораторная работа 2	4 – 5 недели семестра	10 баллов	
3	Расчетно-	10 – 15	10 баллов	10 баллов – студент правильно и

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
	графическая работа	недели семестра		полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 6 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
4	Курсовая работа	2 – 16 недели семестра	50 баллов	50 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 30 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 10 баллов - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
ИТОГО Текущий контроль:		-	80 баллов	-
12	Вопросы экзамена (2 вопроса по 10 баллов)	сессия	20	0 баллов – ответ на вопрос билета отсутствует или не верен 8 баллов – дан не полный ответ, допущены ошибки 14 баллов – дан полный ответ, допущены неточности 20 баллов – дан полный ответ, приведены примеры
ИТОГО Промежуточная аттестация (экзамен)		-	20 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64% от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65-74% от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75-84% от максимально возможной суммы баллов – «хорошо» (средний уровень); 85-100% от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

Задания для текущего контроля

ЛАБОРАТОРНАЯ РАБОТА №1

Настройка защищенных каналов доступа в распределенных информационных системах.
Пример задания.
Сеть предприятия содержит 3 АРМ и сервер. Настроить защищенный канал доступа к демилитаризованной зоне предприятия. На границе расположить АПКШ Континент.

ЛАБОРАТОРНАЯ РАБОТА №2

Использование шлюзов доступа в распределенных информационных системах
Пример задания.
Сеть предприятия содержит 3 АРМ и один сервер. Настроить доступ к сети предприятия используя шлюз. На границе расположить АПКШ Континент.

РАСЧЕТНО-ГРАФИЧЕСКАЯ РАБОТА

Задание 1

Использование межсетевых экранов в распределенных информационных системах

Пример задания.

Сеть предприятия содержит 3 АРМ и один сервер. Настроить защиту периметра предприятия с использованием межсетевого экрана VipNet Personal Firewall. Защищенная сеть 172.12.26.0/24. Доступ разрешен только из 192.168.1.0/24.

Задание 2

Использование систем обнаружения вторжений в распределенных информационных системах.

Пример задания.

Сеть предприятия содержит 3 АРМ и один сервер. Настроить систему обнаружения вторжений для защиты от всевозможных атак. Смоделировать несколько атак на сеть предприятия. Описать каким образом система обнаружения вторжений регистрирует атаки. Защищенная сеть 172.12.26.0/24. Доступ разрешен только из 192.168.1.0/24.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ КУРСОВЫХ РАБОТ

1 Теоретические основы задачи ограничения доступа к Enterprise приложению.
2 Абстракции Spring Security.
3 Настройка конфигурации Spring Security на практике.
4 Применение Spring Security для ограничения доступа к различным частям приложения.

СПИСОК ТЕОРЕТИЧЕСКИХ ВОПРОСОВ НА ЭКЗАМЕН

1. Нормативные документы по метрологии в области информационной безопасности программных средств.
2. Нормативные документы по стандартизации в области информационной безопасности программных средств.
3. Нормативные документы по сертификации в области информационной безопасности программных средств.

4. Нормативные документы по метрологии в области информационной безопасности аппаратных средств.
5. Нормативные документы по стандартизации в области информационной безопасности аппаратных средств.
6. Нормативные документы по сертификации в области информационной безопасности аппаратных средств.
7. Федеральные органы исполнительной власти и их требования в области информационное безопасности распределенных информационных систем.
8. Изолированные АРМ и система защиты.
9. Организационно распорядительные и инструктивные документы в области обеспечения информационной безопасности распределенных информационных систем.
10. Защищенные каналы передачи информации. Лабораторные аспекты реализации передачи информации за пределы контролируемых зон.
11. Распределенные территориально АРМ и система защиты информации.
12. Трансграничная передачи данных.
13. Методы защиты информационных систем с доступом к глобальной сети Internet.
14. Средства защиты информационных систем с доступом к глобальной сети Internet.
15. Межсетевое экранирование
16. Системы обнаружения и предотвращения вторжений.
17. Системы углубленного анализа пакетов, циркулирующих в распределенных информационных системах.
18. Специализированные протоколы передачи данных, защита траффика в сетях с использованием средств криптографической защиты информации.
19. Использование шлюзов доступа к демилитаризованным зонам в распределенных информационных системах.
20. Современные производители и средства обеспечения информационной безопасности в распределенных информационных системах.

СПИСОК ПРАКТИЧЕСКИХ ЗАДАНИЙ НА ЭКЗАМЕН

21. Опишите систему защиты периметра сети предприятия. Сеть содержит 5 АРМ и сервер. Есть удаленные подключения через сеть интернет. Обязательно описать IP адреса как внешние, так и внутренние.
22. Опишите систему защиты периметра сети предприятия. Сеть содержит 10 АРМ и сервер. Обязательно описать IP адреса как внешние, так и внутренние.

5 Учебно-методическое и информационное обеспечение дисциплины (модуля)

5.1 Основная литература

1. Компьютерные сети: Учебное пособие [Электронный ресурс]/ Кузин А.В., Кузин Д.А. - 3-е изд., перераб. и доп. - 2015. - 192 с.: // ZNANIUM.COM: электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/536468, ограниченный, Загл. с экрана.

2. Сети связи и системы коммутации: Учебное пособие [Электронный ресурс]/ Паринов А.В., Ролдугин С.В., Мельник В.А. 2015. - 178 с.// ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/923309, ограниченный, Загл. с экрана.

3. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2022. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст: электронный.

- URL: https://znanium.com/catalog/product/1714105 (дата обращения: 15.11.2021). – Режим доступа: по подписке.

5.2 Дополнительная литература

1. Интеллектуальные интерактивные системы и технологии управления удаленным доступом: методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intrane: Учебное пособие [Электронный ресурс] / Ботуз С.П., - 3-е изд., доп, 2014. - 340 с. // ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/884094, ограниченный, Загл. с экрана.

2. Панько, С. П. Радиотехнические системы специального назначения. Системы связи : учебник / С. П. Панько, Е. Н. Гарин, В. В. Сухотин. - Красноярск : Сиб. федер. ун-т, 2019. - 340 с. - ISBN 978-5-7638-4014-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1830724 (дата обращения: 15.11.2021). – Режим доступа: по подписке.

5.3 Методические указания для студентов по освоению дисциплины

1. Ожиганов А.А. Распределенные информационные системы [Электронный ресурс]: учебное пособие / А.А. Ожиганов. — Электрон.текстовые данные. — СПб: Университет ИТМО, 2016. — 142 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

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

1 Электронно-библиотечная система ZNANIUM.COM. Договор ЕП 44 № 003/10 эбс ИКЗ 191272700076927030100100120016311000 от 17 апреля 2019 г.

2 Электронно-библиотечная система IPRbooks. Лицензионный договор № ЕП44 № 001/9 на предоставление доступа к электронно-библиотечной системе IPRbooks ИКЗ 191272700076927030100100090016311000 от 27 марта 2019 г.

3 Электронно-библиотечная система eLIBRARY.RU. Договор № ЕП 44 № 004/13 на оказание услуг доступа к электронным изданиям ИКЗ 912727000769270301001001500163110000 от 15 апреля 2019 г.

4 Информационно-справочные системы «Кодекс»/ «Техэксперт». Соглашение о сотрудничестве № 25/19 от 31 мая 2019 г.

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

1. Распределенные информационные системы. // Национальный открытый университет «Интуит» [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/courses/13837/1234/info - свободный.

5.6 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 7 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты / условия использования
Microsoft Windows Seven	Лицензионный сертификат № 46243844 от 09.12.2009
OpenOffice	Свободная лицензия, условия использования по ссылке: https://www.openoffice.org/license.html
Microsoft Visual Studio 2008/2010/2012/2013/2017	(в составе лицензии dreamspark)
КриптоПРО CSP 3.6 или выше	3636B-F0000-01760-NKN4A на 4 АРМ

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.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель может проводить инструктаж по выполнению задания. В инструктаж включается:

· цель и содержание задания;

· сроки выполнения;

· ориентировочный объем работы;

· основные требования к результатам работы и критерии оценки;

· возможные типичные ошибки при выполнении.

Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

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.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

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 рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

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

10.1 Учебно-лабораторное оборудование

Таблица 8 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
компьютерные классы ФКТ	Лаборатория защищенных автоматизированных систем	8 ПЭВМ. Комплект мультимедийного оборудования DALLAS LOCK 8.0-C 50197-9111-268 на 5 клиентов, СКАНЕР-ВС НПЭШ.00606-01, Регистрационный номер: ЭФ2204-180334, Количество ip-адресов – 8, DALLAS LOCK 8.0-C 47488-9375-279 на 5 клиентов включая центр управления, Сканер-ВС 12/3 специальная версия для учебных заведений, Secret Net Studio 8 13A6E7 на 10 клиентов включая центр управления, КриптоПро CSP (включает КриптоПро TLS) DU36X-K0000-00XKY-NXA3M-XXXXX, Ideco Hardware Appliance – 10 зарегистрированных пользователей

10.2 Технические и электронные средства обучения

При проведении занятий используется аудитория, оборудованная проектором (стационарным или переносным) для отображения презентаций. Кроме того, при проведении лекций и практических занятий необходим компьютер с установленным на нем браузером и программным обеспечением для демонстрации презентаций.

Для реализации дисциплины подготовлены следующие презентации:

1 Высшее образование в РФ.
2 Виды учебных занятий, виды контроля занятий.
3 Разработка интеллект-карт.

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 установлении 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.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине
Информационная безопасность распределенных информационных систем

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*116*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*ИБАС*

[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 индикаторами достижения компетенций

Процесс изучения дисциплины «Криптографические методы защиты информации» 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

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
ПК-6: Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	ПК-6.1 Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	ПК-6.2 Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов	ПК-6.3 Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Показатели оценки**
Все темы	ПК-2, 22	Лабораторные работы 1-2, Расчетно-графическая работа, курсовая работа	Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических

			документов

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 разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
Раздел 1. Теоретические основы построения защищенных распределенных информационных систем					
Нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты	Лекция	3	Традиционная	ПК-6	ПК-6.1
Федеральные органы исполнительной власти и их требования по построению защищенных распределенных информационных систем	Лекция	4	Интерактивная (презентация)	ПК-6	ПК-6.1
Требования и рекомендации по построению информационных систем в виде изолированных рабочих мест	Лекция	5	Интерактивная (презентация)	ПК-6	ПК-6.1
Организационно-распорядительная документация по обеспечению информационной безопасности распределенных информационных систем	Лекция	4	Традиционная	ПК-6	ПК-6.1
Настройка защищенных каналов	Лабораторная работа	16	Традиционная	ПК-6	ПК-6.2, 6.3

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
доступа в распределенных информационных системах					
Текущий контроль по разделу 1					
Итого по разделу 1	Лекции	16			
	Лабораторные работы	16			
	Самостоятельная работа	58			
	Самостоятельная работа обучающихся (подготовка к лабораторным занятиям)	4	Освоение электронных материалов по дисциплине.	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (изучение теоретических разделов дисциплины)	4	Чтение основной и дополнительной литературы, конспектирование	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (подготовка и оформление РГР и КР)	50	Чтение основной и дополнительной литературы, конспектирование, оформление	ПК-6	ПК-6.2, 6.3
Раздел 2. Лабораторные аспекты построения защищенных распределенных информационных систем.					
Информационные системы как совокупность распределенных автоматизированных рабочих мест объединенных в локальные вычислительные сети	Лекция	5	Интерактивная (презентация)	ПК-6	ПК-6.1
Методы и средства защиты информационных систем с доступом к глобальной сети информационного обмена Internet	Лекция	5	Традиционная	ПК-6	ПК-6.1
Межсетевое экранирование и системы обнаружения и предотвращения	Лекция	3	Традиционная	ПК-6	ПК-6.1

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
вторжений, системы углубленного анализа пакетов					
Описание информационных систем в соответствии с OSI. Использование шлюзов доступа, SSH, SSL.	Лекция	3	Традиционная	ПК-6	ПК-6.1
Использование шлюзов доступа в распределенных информационных системах	Лабораторная работа	16	Традиционная	ПК-6	ПК-6.2, 6.3
Текущий контроль по разделу 2					
Итого по разделу 2	Лекции	16			
	Лабораторные работы	16			
	Самостоятельная работа	58			
	Самостоятельная работа обучающихся (подготовка к лабораторным занятиям)	4	Освоение электронных материалов по дисциплине.	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (изучение теоретических разделов дисциплины)	4	Чтение основной и дополнительной литературы, конспектирование	ПК-6	ПК-6.2, 6.3
	Самостоятельная работа обучающихся (подготовка и оформление РГР, собеседование)	50	Чтение основной и дополнительной литературы, конспектирование, оформление	ПК-6	ПК-6.2, 6.3
Промежуточная аттестация по дисциплине в 8-м семестре		36	Экзамен	ПК-6	
ИТОГО по дисциплине в 8-м семестре	Лекции	32	-	-	-
	Лабораторные работы	32	-	-	-
	Контроль	36			
	Самостоятельная работа обучающихся	116	-	-	-
ИТОГО: общая трудоемкость дисциплины 216 часа					

Задания для текущего контроля

ЛАБОРАТОРНАЯ РАБОТА №1

Настройка защищенных каналов доступа в распределенных информационных системах.
Пример задания.
Сеть предприятия содержит 3 АРМ и сервер. Настроить защищенный канал доступа к демилитаризованной зоне предприятия. На границе расположить АПКШ Континент.

ЛАБОРАТОРНАЯ РАБОТА №2

Использование шлюзов доступа в распределенных информационных системах
Пример задания.
Сеть предприятия содержит 3 АРМ и один сервер. Настроить доступ к сети предприятия используя шлюз. На границе расположить АПКШ Континент.

РАСЧЕТНО-ГРАФИЧЕСКАЯ РАБОТА

Задание 1

Использование межсетевых экранов в распределенных информационных системах

Пример задания.

Сеть предприятия содержит 3 АРМ и один сервер. Настроить защиту периметра предприятия с использованием межсетевого экрана VipNet Personal Firewall. Защищенная сеть 172.12.26.0/24. Доступ разрешен только из 192.168.1.0/24.

Задание 2

Использование систем обнаружения вторжений в распределенных информационных системах.

Пример задания.

Сеть предприятия содержит 3 АРМ и один сервер. Настроить систему обнаружения вторжений для защиты от всевозможных атак. Смоделировать несколько атак на сеть предприятия. Описать каким образом система обнаружения вторжений регистрирует атаки. Защищенная сеть 172.12.26.0/24. Доступ разрешен только из 192.168.1.0/24.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ КУРСОВЫХ РАБОТ

1 Теоретические основы задачи ограничения доступа к Enterprise приложению.
2 Абстракции Spring Security.
3 Настройка конфигурации Spring Security на практике.
4 Применение Spring Security для ограничения доступа к различным частям приложения.

СПИСОК ТЕОРЕТИЧЕСКИХ ВОПРОСОВ НА ЭКЗАМЕН

1. Нормативные документы по метрологии в области информационной безопасности программных средств.
2. Нормативные документы по стандартизации в области информационной безопасности программных средств.
3. Нормативные документы по сертификации в области информационной безопасности программных средств.

4. Нормативные документы по метрологии в области информационной безопасности аппаратных средств.
5. Нормативные документы по стандартизации в области информационной безопасности аппаратных средств.
6. Нормативные документы по сертификации в области информационной безопасности аппаратных средств.
7. Федеральные органы исполнительной власти и их требования в области информационное безопасности распределенных информационных систем.
8. Изолированные АРМ и система защиты.
9. Организационно распорядительные и инструктивные документы в области обеспечения информационной безопасности распределенных информационных систем.
10. Защищенные каналы передачи информации. Лабораторные аспекты реализации передачи информации за пределы контролируемых зон.
11. Распределенные территориально АРМ и система защиты информации.
12. Трансграничная передачи данных.
13. Методы защиты информационных систем с доступом к глобальной сети Internet.
14. Средства защиты информационных систем с доступом к глобальной сети Internet.
15. Межсетевое экранирование
16. Системы обнаружения и предотвращения вторжений.
17. Системы углубленного анализа пакетов, циркулирующих в распределенных информационных системах.
18. Специализированные протоколы передачи данных, защита траффика в сетях с использованием средств криптографической защиты информации.
19. Использование шлюзов доступа к демилитаризованным зонам в распределенных информационных системах.
20. Современные производители и средства обеспечения информационной безопасности в распределенных информационных системах.

СПИСОК ПРАКТИЧЕСКИХ ЗАДАНИЙ НА ЭКЗАМЕН

1. Опишите систему защиты периметра сети предприятия. Сеть содержит 5 АРМ и сервер. Есть удаленные подключения через сеть интернет. Обязательно описать IP адреса как внешние, так и внутренние.
2. Опишите систему защиты периметра сети предприятия. Сеть содержит 10 АРМ и сервер. Обязательно описать IP адреса как внешние, так и внутренние.

Лист регистрации изменений к РПД

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