УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Основы информационной безопасности**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	3 - очная форма обучения

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Обучить студентов принципам обеспечения информационной безопасности, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности автоматизированных систем;

содействовать фундаментализации образования, формированию научного миро-воззрения и развитию системного мышления.

Задачи освоения дисциплины:

Дать основы:

методологии создания систем защиты информации;

методов, средств и приемов ведения информационных войн;

обеспечения информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы информационной безопасности» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-6, ОПК-10, ОПК-16.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Подготовка к сдаче и сдача государственного экзамена, Теория информации, Научно-исследовательская работа, Организационное и правовое обеспечение информационной безопасности, Защита информации от утечки по техническим каналам, Ознакомительная практика, Проектная деятельность, Программно-аппаратные средства защиты информации, Криптографические протоколы, Теоретико-числовые методы в криптографии, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Организация электронно вычислительных машин и вычислительных систем.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-16 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	**знать**: Значение информации, информационных технологий и информационной безопасности в современном обществе для обеспечения объективных потребностей личности, общества и государства **уметь**: Анализировать роль информации на основных этапах исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма **владеть**: Навыками оценки анализа роли информации на основных этапах исторического развития России
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	**знать**: Порядок организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **уметь**: Организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **владеть**: Навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	**знать**: Основные компоненты систем защиты информации автоматизированных систем **уметь**: Правильно использовать основные средства криптографической защиты информации при решении задач профессиональной деятельности **владеть**: Навыками правильного использования основных средств криптографической защиты информации при решении задач профессиональной деятельности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		5
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	36	36
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Оценивание реферата, Тестирование	Оценивание реферата, Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	-	-
Всего часов по дисциплине	108	108

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Информационная безопасность в системе национальной безопасности РФ							
Тема 1.1. Понятие национальной безопасности	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 1.2. Национальн	4	2	0	0	0	2	Тестирование,

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
ые интересы России в информационной сфере							Оценивание реферата
Тема 1.3. Угрозы информационной безопасности Российской Федерации	10	2	0	4	0	4	Тестирование, Оценивание реферата
Тема 1.4. Источники угроз информационной безопасности РФ	4	2	0	0	0	2	Тестирование, Оценивание реферата
Раздел 2. Информационная война, методы и средства ее ведения							
Тема 2.1. Информационная безопасность и информационное противоборство	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 2.2. Приемы информационного воздействия в информационной войне	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 2.3. Типовая стратегия информационной войны	4	2	0	0	0	2	Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах							
Тема 3.1. Классификация автоматизированных систем и требования по защите информации	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 3.2. Структура системы защиты информации от НСД. Назначение и функции элементов	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 3.3. Модели управления доступом	6	2	0	0	0	4	Тестирование, Оценивание реферата
Раздел 4. Основные методы обеспечения информационной безопасности							
Тема 4.1. Основные понятия криптографической защиты информации	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 4.2. Симметричные криптографические системы	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 4.3. Асимметричные криптографически	4	2	0	0	0	2	Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
е системы							
Тема 4.4. Идентификация и аутентификация	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 4.5. Разграничение и контроль доступа к информации	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 4.6. Технологии межсетевых экранов	6	2	0	0	0	4	Тестирование, Оценивание реферата
Тема 4.7. Виртуальные частные сети	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 4.8. Методы обнаружения вторжений (атак)	6	2	0	0	0	4	Тестирование, Оценивание реферата
Раздел 5. Средства защиты информации от несанкционированного доступа							
Тема 5.1. Система SecretNet Studio	6	0	0	4	0	2	Тестирование, Оценивание реферата
Тема 5.2. Система защиты от НСД «Dallas Lock».	6	0	0	4	0	2	Тестирование, Оценивание реферата
Тема 5.3. Электронный замок "Соболь"	4	0	0	2	0	2	Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 5.4. Встроенный межсетевой экран	4	0	0	2	0	2	Тестирование, Оценивание реферата
Тема 5.5. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд»	4	0	0	2	0	2	Тестирование, Оценивание реферата
Итого подлежит изучению	108	36	0	18	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Информационная безопасность в системе национальной безопасности РФ

Тема 1.1. Понятие национальной безопасности

Сущность и содержание национальной безопасности. Основные задачи в области обеспечения национальной безопасности. Объект и субъект безопасности. Виды безопасности: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.

Тема 1.2. Национальные интересы России в информационной сфере

Место и роль России в глобальном информационном пространстве. Национальные интересы России в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

Тема 1.3. Угрозы информационной безопасности Российской Федерации

Проблемы обеспечения информационной безопасности. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Классификация угроз безопасности информационных и телекоммуникационных средств и систем. Модель действий нарушителя

Тема 1.4. Источники угроз информационной безопасности РФ

Внешние источники угроз. Внутренние источники угроз. Классификация источников угроз и уязвимостей информационной безопасности

Раздел 2. Информационная война, методы и средства ее ведения

Тема 2.1. Информационная безопасность и информационное противоборство

Понятие информационной войны. Проблемы информационных войн. Субъекты информационного противоборства. Цель информационного противоборства. Составные части и методы информационного противоборства.

Тема 2.2. Приемы информационного воздействия в информационной войне

Информационная война как целенаправленное информационное воздействие информационных систем. Способы перепрограммирования информационных систем. Проблема начала информационной войны

Тема 2.3. Типовая стратегия информационной войны

Обобщенный алгоритм информационной войны. Основные аспекты информационной войны. Последствия информационной войны.

Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах

Тема 3.1. Классификация автоматизированных систем и требования по защите информации

Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации.

Тема 3.2. Структура системы защиты информации от НСД. Назначение и функции элементов

Направления защиты от НСД. Основные способы НСД. Принципы защиты информации от НСД. Структура системы защиты информации от НСД, назначение и функции элементов.

Тема 3.3. Модели управления доступом

Правила разграничения доступа. Мандатная и дискреционная модели управления доступом. Ролевая и атрибутные модели

Раздел 4. Основные методы обеспечения информационной безопасности

Тема 4.1. Основные понятия криптографической защиты информации

В данной лекции определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы

Тема 4.2. Симметричные криптографические системы

Обобщенная схема симметричной криптосистемы. Алгоритм шифрования DES. Стандарт шифрования ГОСТ Р34.12-2015. Особенности применения алгоритмов симметричного шифрования

Тема 4.3. Асимметричные криптографические системы

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Функция хэширования. Электронная подпись

Тема 4.4. Идентификация и аутентификация

Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и электронные подписи. Методы аутентификации

Тема 4.5. Разграничение и контроль доступа к информации

Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации; по способам ее обработки: считать, записать, внести изменения, выполнить команду; по условному номеру терминала; по времени обработки и др. Разделение привилегий на доступ к информации.

Тема 4.6. Технологии межсетевых экранов

Рассмотрена технология межсетевых экранов (МЭ) - одна из самых первых технологий защиты корпоративных сетей от внешних угроз. Показано, что МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты.

Функции МЭ

Тема 4.7. Виртуальные частные сети

Основные понятия и функции виртуальных частных сетей (VPN). Варианты по-строения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.

Тема 4.8. Методы обнаружения вторжений (атак)

Краткая история вторжений (атак) на интрасети. Основные понятия. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений.

Раздел 5. Средства защиты информации от несанкционированного доступа

Тема 5.1. Система SecretNet Studio

Назначение, возможности и порядок работы с системой SecretNet Studio

Тема 5.2. Система защиты от НСД «Dallas Lock».

Назначение, возможности, установка и порядок работы с СЗИ от НСД «Dallas Lock»

Тема 5.3. Электронный замок "Соболь"

Назначение, возможности, установка и порядок работы с Электронным замком "Соболь".

Тема 5.4. Встроенный межсетевой экран

Содержание лабораторной работы включает в себя следующие положения: 1. Если исследуемый МЭ – встроенный брандмауэр используемой операционной системы, то надо просто зайти в него. 2. Если исследуемый МЭ – не является встроенным, то необходимо его загрузить. 3. Произвести выборочное администрирование МЭ, изменяя те или иные параметры. Фиксировать изменения фильтрации трафика. 4. Подготовить отчёт.

Тема 5.5. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд»

Назначение, возможности, установка и использование программно-аппаратного комплекса средств защиты информации от НСД «Аккорд–АМДЗ».

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия

Цели: Анализ информационных активов, используемых компанией и выработка концептуальных основ деятельности по обеспечению корпоративной информационной безопасности. Результат: отчет.

Содержание: 1. Установить номенклатуру информационных активов и оценить их значимость для выбранной компании (в соответствии с вариантом) в целом и для ее структурных подразделений. 2. Выявить виды и разновидности тайн, которые используются в деятельности рассматриваемой компании (в соответствии с вариантом). 3. Оценить риски информационной безопасности для рассматриваемой компании (в соответствии с вариантом).

Результаты: 1.a. Определите базовые уязвимости и угрозы в сфере информационной безопасности для деятельности компании. 1.b. Для каждого структурного подразделения определить защищаемые информационные активы. 2. Определить примерный перечень сведений, составляющих коммерческую (служебную, банковскую) тайну компании. 3.Определите наиболее опасные каналы утечки информации, способы и средства противодействия выявленным утечкам.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263

Назначение, возможности и порядок работы с системой SecretNet Studio

Цели: Изучить возможности и научиться работать с системой SecretNet Studio. Результат: отчет.

Содержание: 1. Ознакомление с теоретической частью «Secret Net Studio». 2. Установка программного обеспечения средства защиты информации «Secret Net Studio» на локальный ПК. 3. Подготовка средства защиты информации к инициализации. 4. Инициализация «Secret Net Studio». 5. Подготовка к эксплуатации. 6. Настройка и эксплуатация «Secret Net Studio». 7. Удаление программного обеспечения «Secret Net Studio».

Результаты: 1. Изучить «Secret Net Studio» и научиться устанавливать, настраивать, эксплуатировать и корректно удалять СЗИ с компьютера. 2. Подготовить письменный отчет о проделанной работе и защитить его у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263

Назначение и возможности программно-аппаратного комплекса средств защиты информации от несанкционированного доступа Dallas Lock -K (C)

Цели: Изучить программно-аппаратный комплекс средств защиты информации от несанкционированного доступа Dallas Lock -K (C) и получить навыки установки, настройки и практического использования комплекса.

Содержание: 1. Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске C имеется необходимое свободное пространство для установки системы защиты. 3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты. 4. Рекомендуется произвести дефрагментацию диска. 5. Проверить компьютер на отсутствие компьютерных вирусов. 6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы. 7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки. 8. Осуществить основные операции установки, настройки, эксплуатации и удаления Dallas Lock в соответствии с учебным пособием.

Результаты: 1. Изучить и продемонстрировать основные возможности Dallas Lock как системы защиты информации от НСД. 2. Составить отчет о проделанной работе и защитить его у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263

Назначение, возможности и порядок работы с Электронным замком "Соболь".

Цели: Изучить возможности и научиться работать с электронным замком "Соболь". Результат: отчет.
Содержание: 1. Ознакомление с теоретической частью электронного замка "Соболь". 2. Установка программного обеспечения комплекса "Соболь". 3. Подготовка комплекса к инициализации. 4. Инициализация электронного замка "Соболь". 5. Подготовка электронного замка к эксплуатации. 6. Настройка и эксплуатация комплекса "Соболь". 7. Удаление программного обеспечения электронного замка "Соболь".
Результаты: - изучить электронный замок «Соболь» и научиться устанавливать, настраивать и эксплуатировать его; - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263
НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ВСТРОЕННЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ
Цели: 1. Изучить возможности встроенных межсетевых экранов (МЭ) на примере выбранного МЭ. 2. Научиться администрировать выбранный МЭ.
Содержание: 1. Если исследуемый МЭ – встроенный брандмауэр используемой операционной системы, то надо просто зайти в него. 2. Если исследуемый МЭ – не является встроенным, то необходимо его загрузить. 3. Произвести выборочное администрирование МЭ, изменяя те или иные параметры. Фиксировать изменения фильтрации трафика.
Результаты: 1. Изучить и продемонстрировать основные возможности МЭ. 2. Составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263
НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД “АККОРД–АМДЗ”
Цели: Изучить возможности и научиться работать с комплексом средств защиты от несанкционированного доступа (НСД).
Содержание: 1. Ознакомление с теоретической частью СЗИ НСД «Аккорд- АМДЗ». 2. Установка платы контроллера и программного обеспечения комплекса, включающая три основных этапа: - установка платы контроллера в свободный слот ПЭВМ и регистрацию администратора безопасности информации (БИ) (супервизора), в том числе, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ; - регистрация пользователей, назначение пользователям личных ТМ-идентификаторов, паролей и времени доступа; - назначение списка дисков, файлов, разделов реестра, контролируемых на целостность. 3. Инициализация СЗИ НСД «Аккорд- АМДЗ»: - регистрация супервизора (администратора безопасности информации); - регистрация нового пользователя. 4. Эксплуатация комплекса «Аккорд- АМДЗ». 5. Снятие средств защиты комплекса «Аккорд- АМДЗ».
Результаты: 1. Изучить СЗИ НСД «Аккорд- АМДЗ» и научиться устанавливать, настраивать и эксплуатировать его. 2. Составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4263

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы рефератов

Тема 1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
Тема 2. Виды защищаемой информации

Тема 3. Угрозы информационной безопасности Российской Федерации
Тема 4. Интересы личности (общества, государства) в информационной сфере
Тема 5. Интересы личности (общества, государства) в информационной сфере
Тема 6. Внешние и внутренние источники угроз информационной безопасности государства
Тема 7. Виды защищаемой информации
Тема 8. Внешние и внутренние источники угроз информационной безопасности государства
Тема 9. Информационное оружие, его классификация и возможности
Тема 10. Внешние и внутренние источники угроз информационной безопасности государства.
Тема 11. Информационное оружие, его классификация и возможности
Тема 12. Внешние и внутренние источники угроз информационной безопасности государства
Тема 13. Информационное оружие, его классификация и возможности
Тема 14. Компьютерная система как объект информационной безопасности
Тема 15. Компьютерная система как объект информационной безопасности
Тема 16. Внешние и внутренние источники угроз информационной безопасности государства
Тема 17. Основные понятия криптографической защиты информации
Тема 18. Симметричные криптографические системы. Достоинства и недостатки
Тема 19. Асимметричные криптографические системы. Достоинства и недостатки
Тема 20. Основные методы обеспечения инф. безопасности. Идентификация и аутентификация
Тема 21. Основные методы обеспечения информационной безопасности. Разграничение и контроль доступа к информации
Тема 22. Виртуальные частные сети (VPN).
Тема 23. Основные методы обеспечения информационной безопасности. Межсетевые экраны
Тема 24. Методы обнаружения вторжений (атак).
Тема 25. Основные методы обеспечения информационной безопасности. Разграничение и контроль доступа к информации
Тема 26. Основные методы обеспечения информационной безопасности. Разграничение и контроль доступа к информации
Тема 27. Основные методы обеспечения инф. безопасности. Идентификация и аутентификация
Тема 28. Основные методы обеспечения информационной безопасности. Межсетевые экраны
Тема 29. Модели управления доступом
Тема 30. Основные методы обеспечения инф. безопасности. Идентификация и аутентификация.
Тема 31. Понятие национальной безопасности
Тема 32. Национальные интересы России в информационной сфере

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Основные элементы национальной безопасности Российской Федерации

2. Основные элементы национальной безопасности Российской Федерации

3. Классификация видов национальной безопасности Российской Федерации

4. Информационная безопасность. Основные принципы и составляющие Государственной политики обеспечения информационной безопасности Российской Федерации

5. Место и роль России в глобальном информационном пространстве. Интересы личности в информационной сфере

6. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере

7. Проблемы обеспечения информационной безопасности

8. Понятие угрозы информации. Угрозы конфиденциальности, целостности и доступности

9. Классификация угроз информации

10. Модель действий нарушителя

11. Источники угроз информационной безопасности РФ. Внешние источники угроз

12. Источники угроз информационной безопасности РФ. Внутренние источники угроз

13. Классификация источников угроз и уязвимостей информационной безопасности

14. Понятие информационной войны. Проблемы информационных войн

15. Субъекты и цели информационного противоборства.Составные части и методы информационного противоборства

16. Информационное оружие, его классификация и возможности

17. Информационная война как целенаправленное информационное воздействие информационных систем

18. Приемы информационного воздействия в информационной войне. Способы перепрограммирования информационных систем

19. Типовая стратегия информационной войны. Основные аспекты и последствия информационной войны

20. Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники

21. Документы Гостехкомиссии при Президенте Российской Федерации. Классификация информационных систем по уровню их защищенности

22. Документы Гостехкомиссии при Президенте Российской Федерации. Требования к информационным системам по обеспечению безопасности информации

23. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД.

Принципы защиты информации от НСД

24. Структура системы защиты информации от НСД, назначение и функции элементов

25. Правила разграничения доступа к информации. Мандатная модель управления доступом

26. Правила разграничения доступа к информации. Дискреционная модель управления доступом

27. Основные понятия криптографической защиты информации. Историческая справка об основных этапах развития криптографии как науки

28. Основные требования к криптографическим системам защиты информации. Пример простейшего шифра

29.

30. Обобщенная схема симметричной криптосистемы. Стандарт шифрования «Магма». Особенности применения алгоритмов симметричного шифрования

31. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Функция хэширования

32. Обобщенная схема асимметричнойкриптосистемышифрованиясоткрытым ключом. Электронная подпись

33. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации

34. Пароли, сертификаты и цифровые подписи. Методы аутентификации

35. Понятие разграничения доступа. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации

36. Технология межсетевых экранов (МЭ). Виды МЭ

37. Технология межсетевых экранов (МЭ). Виды МЭ

38. Основные понятия и функции виртуальных частных сетей (VPN)

39. Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности виртуальных частных сетей (VPN)

40. Основные методы обнаружения вторжений (атак)

41. Назначение, возможности и порядок работы с системой SecretNet Studio

42. Назначение, возможности установка и порядок работы с системой защиты от НСД «Dallas Lock»

43. Назначение, возможности и порядок работы с Электронным замком "Соболь"

44. Назначение, возможности и использование встроенных межсетевых экранов

45. Назначение, возможности и использование программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Информационная безопасность в системе национальной безопасности РФ			
Тема 1.1. Понятие национальной безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 1.2. Национальные интересы России в информационной сфере	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 1.3. Угрозы информационной безопасности Российской Федерации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 1.4. Источники угроз информационной безопасности РФ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Раздел 2. Информационная война, методы и средства ее ведения			
Тема 2.1. Информационная безопасность и информационное противоборство	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 2.2. Приемы информационного воздействия в информационной войне	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 2.3. Типовая стратегия информационной войны	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах			
Тема 3.1. Классификация автоматизированных систем и требования по защите информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 3.2. Структура системы защиты информации от НСД. Назначение и функции элементов	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 3.3. Модели управления доступом	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Раздел 4. Основные методы обеспечения информационной безопасности			
Тема 4.1. Основные понятия криптографической защиты информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 4.2. Симметричные криптографические системы	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 4.3. Асимметричные криптографические системы	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 4.4. Идентификация и аутентификация	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 4.5. Разграничение и контроль доступа к информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 4.6. Технологии межсетевых экранов	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Тема 4.7. Виртуальные частные сети	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 4.8. Методы обнаружения вторжений (атак)	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Раздел 5. Средства защиты информации от несанкционированного доступа			
Тема 5.1. Система SecretNet Studio	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 5.2. Система защиты от НСД «Dallas Lock».	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения	2	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
	дисциплины.		
Тема 5.3. Электронный замок "Соболь"	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 5.4. Встроенный межсетевой экран	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 5.5. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд»	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам : учебное пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2015. - 586 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204248.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0424-8. / .— ISBN 0_251025

2. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 1 / А. М. Иванцов, В. Г. Козловский ; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 776 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1396. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_36065

3. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Часть 2 / А. М. Иванцов, В. Г. Козловский ; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 1,41 МБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/8697. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_42171

дополнительная

1. Гродзенский Я.С. Информационная безопасность : учебное пособие / Я.С. Гродзенский ; Гродзенский Я.С. - Москва : РГ-Пресс, 2020. - 144 с. - URL: https://www.studentlibrary.ru/book/ISBN9785998808456.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9988-0845-6. / .— ISBN 0_260443

2. Галатенко В.А. Стандарты информационной безопасности : учебник / В.А. Галатенко ; Галатенко В.А. - Москва : ИНТУИТ, 2016. - . - URL: https://www.studentlibrary.ru/book/ISBN5955600531.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 5-9556-0053-1. / .— ISBN 0_257176

3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В.Ф. Шаньгин ; Шаньгин В.Ф. - Москва : ДМК-пресс, 2012. - 592 с. - URL: https://www.studentlibrary.ru/book/ISBN9785940748335.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-94074-833-5. / .— ISBN 0_485556

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Основы информационной безопасности» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, Фак. математики, информ. и авиац. технологий. - 2020. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 403 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/4263. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_37894.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст

: электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для

проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО