УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «__» мая_ 2023 г., протокол №_4/23__
Председатель _____Волков М.А.
(подпись, расшифровка подписи)
«16» ___мая_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Программно-аппаратные средства защиты информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

Форма обучения:_____очная_____
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «_01_»_____09_____2023_г.

Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____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	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____/_____/ Андреев А.С._/ *(подпись) (Ф.И.О.)* «_11_»___05_____2023_г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Основной целью освоения дисциплины «Программно-аппаратные средства защиты информации» является формирование у студентов знаний о спектре программно-аппаратных средств обеспечения информационной безопасности, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по настройке, выбору и эксплуатации программно-аппаратных средств защиты информации.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных системах;
- о защитных механизмах, реализованных в средствах защиты информационных систем;
- о современных программно-аппаратных средствах защиты информации;
- о применении средств криптографической защиты информации и средств защиты информации от НСД для решения задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Программно-аппаратные средства защиты информации» изучается в 8 семестре и относится к обязательной части дисциплин блока Б1.О специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», «Методы и средства защиты информации от утечки по техническим каналам», «Системы и сети передачи информации», позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность вычислительных сетей»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Безопасность открытых информационных систем»; «Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	**Знать:** основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **Уметь:** решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи **Владеть:** навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**Знать:** основные средства криптографической защиты информации, используемые при решении задач профессиональной деятельности **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
ОПК-13 - Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	**Знать:** порядок диагностики и тестирования систем защиты информации автоматизированных систем **Уметь:** организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем **Владеть:** навыками организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 4.

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

Вид учебной работы	**Количество часов (форма обучения ___*очная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		8 семестр		
Контактная работа обучающихся с преподавателем	90	90/90*		
Аудиторные занятия:	90	90/90*		
Лекции	36	36/36*		
Практические и семинарские занятия	36	36/36*		
Лабораторные работы (лабораторный практикум)	18	18/18*		
Самостоятельная работа	18	18		
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабораторных работ - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	экзамен 36	экзамен 36		
Всего часов по дисциплине:	144 с экзаменом	144 с экзаменом		

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинар	Лабораторные работы			
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности							
1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).	3	2				1	Тесты Т1, реферат 11
2. Анализ угроз информационной безопасности	3	2				1	Тесты Т2, реферат 12
3. Механизмы защиты. Политика безопасности в информационных системах	5	2	2			1	Тесты Т3, реф. 13, 14
4. Основные принципы в работе программно-аппаратных средств обеспечения информационной безопасности	5	2	2			1	Тесты Т4, реф. 13, 14
5. Типовая структура и основные функции программно–аппаратных средств обеспечения информационной безопасности	5	2	2			1	Тесты Т5, реферат 15
6. Методы разграничения доступа и управления доступом	3	2				1	Тесты Т6, реферат16
7. Методы обеспечения идентификации и аутентификации	5	2	2			1	Тесты Т7, реферат 17
8. Методы и средства хранения ключевой информации	9	2	2	4	4	1	Тесты Т8, реферат 5? Лаб. раб. 1
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа							
9. Защита от незаконного копирования и исполь-	5	2	2			1	Тесты Т9, реферат 1

зования программ							
10. Защита от разрушающих программных воздействий и изучения кода программ	5	2	2			1	ТестыТ10, реф. 2, 7
11. Основные подходы к защите данных от НСД	5	2	2			1	Тесты Т11, реф. 18, 3
12. Определение факта доступа к файлам. Доступ к данным со стороны процесса	7	2	4	4	4	1	Тесты Т12, реферат 16, Лаб. раб. 2
13. Особенности защиты данных от изменения	7	2	4	4	4	1	Тесты Т13, реферат 8, Лаб. раб. 3
14. Основные средства криптографической защиты	11	2	2	2	2	1	Тесты Т14, реферат 19, Лаб. раб. 4
15. ПАСОИБ в сетях передачи данных	15	2	4	4	4	1	Тесты Т15, реф. 4, 9
16. Управление безопасностью сети	5	2	2			1	Тесты Т16, реферат 10
17. Сертификация СЗИ	10	4	4			2	Тесты Т17, реферат 20
Итого:	108	36	36	18	18	18	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).

Основные понятия и определения в создании ПАСОИБ. Предмет и задачи дисциплины. Нормативно-правовая база создания и использования ПАСОИБ.

Тема 2. Анализ угроз информационной безопасности.

Понятие доступа, субъект и объект доступа. Классификация угроз информационной безопасности. Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя.

Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах.

Требования к защищенности. Оценка защищенности Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления. Политика безопасности.

Тема 4. Основные принципы в создании программно-аппаратных средств обеспечения информационной безопасности.

Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам. Порядок проектирования

ПАСОИБ. Модель системы защиты информации (СЗИ).

Тема 5. Типовая структура и основные программно–аппаратных средств обеспечения информационной безопасности

Структура ПАСОИБ. Компоненты и подсистемы. Типовые функции ПАСОИБ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ. Перспективы развития ПАСОИБ. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тема 6. Методы разграничения доступа и управления доступом

Методы ограничения доступа и управления доступом. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Идентификация и аутентификация. Парольные системы. Дискреционное управление доступом. Мандатное управление доступом. Ролевое управление доступом.

Тема 7. Методы обеспечения идентификации и аутентификации

Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Авторизация. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 8. Методы и средства хранения ключевой информации

Информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей. Магнитные диски прямого доступа. Средство TouchMemory. Типовые решения в организации ключевых систем. Открытое распределение ключей. Метод управляемых векторов. Персональные средства аутентификации и защищенного хранения данных.

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 9. Защита от незаконного копирования и использования программ.

Классификация аппаратных и программных компонентов защиты программ. Структура ПО. Способы встраивания средств защиты в ПО. Способы определения факта незаконного копирования и использования программ. Способы защиты от незаконного копирования и использования программ. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

Тема 10. Защита от разрушающих программных воздействий и изучения кода программ.

Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Тема 11. Основные подходы к защите данных от НСД.

Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам в различных ОС. Защита сетевого файлового ресурса. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных

средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса.

Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 13. Особенности защиты данных от изменения.

Защита массивов информации от изменения. Имитозащита. Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения. Подход на основе формирования имитоприставки. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭП). Особенности защиты документов и исполняемых файлов. Проблема самоконтроля исполняемых модулей. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаление программ и файлов.

Тема 14. Методы криптографической защиты.

Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 15. ПАСОИБ в сетях передачи данных.

Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак.

Тема 16. Управление безопасностью сети.

Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тема 17. Сертификация СЗИ.

Система сертификации СЗИ. Задачи сертификации ПАСОИБ на соответствие требованиям информационной безопасности. Нормативно-правовая база сертификации ПАСОИБ на соответствие требованиям информационной безопасности. Технология сертификации ПАСОИБ на соответствие требованиям информационной безопасности.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах (семинар).

1. Модели управления доступом.
2. Способы защиты конфиденциальности, целостности и доступности в КС.
3. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления.
4. Политика безопасности.

Тема 4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности (семинар).

1. Принципы разработки ПАСОИБ.
2. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
3. Проектирование ПАСОИБ.
4. Модель системы защиты информации (СЗИ).

Тема 5. Типовая структура и основные функции программно–аппаратных средств обеспечения информационной безопасности (семинар).

1. Структура ПАСОИБ. Компоненты и подсистемы.
2. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ.
3. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тема 7. Методы обеспечения идентификации и аутентификации (семинар).

1. Локальная и удаленная идентификация.
2. Способы хранения идентифицирующей информации.
3. Связь с ключевыми системами.
4. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 8. Методы и средства хранения ключевой информации (семинар).

1. Информация, используемая для контроля доступа: ключи и пароли.
2. Злоумышленник и ключи.
3. Организация хранения ключей.
4. Персональные средства аутентификации и защищенного хранения данных.

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 9. Защита незаконного копирования и использования программ (семинар).

1. Способы встраивания средств защиты в ПО.
2. Способы определения факта незаконного копирования и использования программ.
3. Способы защиты от незаконного копирования и использования программ.

Тема 10. Защита от разрушающих программных воздействий и изучения кода программ (семинар).

1. Способы изучения кода программ. Обратное проектирование ПО.
2. Способы защиты программ от изучения кода.
3. Защита от разрушающих программных воздействий.

Тема 11. Основные подходы к защите данных от НСД (семинар).

1. Оценка надежности систем ограничения доступа – сведение к задаче оценки

стойкости.

2. Организация доступа к файлам в различных ОС.
3. Защита сетевого файлового ресурса.

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса (семинар).

1. Способы определения факта доступа. Журналы доступа.
2. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
3. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя.
4. Принципы построения и функционирования электронных замков.
5. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 13. Особенности защиты данных от изменения (семинар).

1. Подходы к решению задачи защиты данных от изменения.

2. Подход на основе формирования имитоприставки (МАС), способы построения МАС.

3. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭЦП).

4. Особенности защиты документов и исполняемых файлов.

5. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаление программ и файлов.

Тема 14. Методы криптографической защиты (семинар).

1. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.
2. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 15. ПАСОИБ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак (семинар).

1. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.

2. Основные принципы защиты информации при передаче по каналам связи.

3. Программно-аппаратные средства защиты информации при передаче по каналам связи.

4. Основные принципы обнаружения сетевых атак.

5. Основные принципы защиты от сетевых атак.

Тема 16. Управление безопасностью сети (семинар).

1. Основные принципы управления безопасностью сети.

2. Программно-аппаратные средства управления безопасностью сети.

3. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тема 17. Сертификация СЗИ.

1. Система сертификации СЗИ.

2. Технология сертификации ПАСОИБ на соответствие требованиям информационной безопасности.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 8. Методы и средства хранения ключевой информации

Лабораторная работа № 1 (4 часа). «Настройка усиленной аутентификации с использованием СЗИ от НСД Dallas Lock на базе eToken».

Цель работы: Настройка и использование «eToken» для аутентификации и получение практических навыков работы с персональным средством аутентификации и защищенного хранения данных».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с персональным средством аутентификации и защищенного хранения данных».

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса.

Лабораторная работа № 2 (4 часа). «Использование электронного замка ПАК Соболь».

Цель работы: Использование «ПАК Соболь» для контроля аппаратной конфигурации ПЭВМ, получение практических навыков работы с электронным замком».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с электронным замком».

Тема 13. Особенности защиты данных от изменения.

Лабораторная работа № 3 (4 часа). «Использование СЗИ Dallas Lock».

Цель работы: Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаления программ и файлов, получение практических навыков работы с СЗИ от НСД».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с СЗИ от НСД».

Лабораторная работа № 4 (2 часа). Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”. Цель: Изучить возможности и научиться работать с комплексом средств защиты от НСД. Результат: отчет. Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей Программно-аппаратного комплекса средств защиты информации от НСД.

Тема 14. Методы криптографической защиты.

Лабораторная работа № 4 (4 часа). Назначение, возможности и порядок работы с системой SecretNet Studio.

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

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей системы SecretNet Studio.

Тема 15. ПАСОИБ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак.

Лабораторная работа № 5 (4 часа). «Использование программно-аппаратных комплексов VipNet».

Цель работы: Организация межсетевого взаимодействия защищенных сетей ViPNet. Получение практических навыков работы со средством криптографической защиты информации».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с электронным замком».

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Защита от незаконного копирования программ
2. Защита от незаконного использования программ
3. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
4. Программно-аппаратные средства защиты информации в сетях передачи данных
5. Методы и средства хранения ключевой информации
6. Защита от разрушающих программных воздействий.
7. Защита от изучения кода программ.
8. Защита данных от изменения.
9. Способы и средства обнаружения сетевых атак.
10. Программно-аппаратные средства управления безопасностью сети.
11. Классификация программно-аппаратных средств обеспечения информационной безопасности
12. Классификация угроз информационной безопасности
13. Основные принципы и механизмы защиты информации
14. Политики безопасности в информационных системах
15. Типовая структура и основные функции программно–аппаратных средств обеспечения информационной безопасности
16. Основные методы разграничения доступа и управления доступом
17. Основные методы обеспечения идентификации и аутентификации
18. Основные подходы к защите данных от НСД
19. Методы и средства криптографической защиты
20. Сертификация средств защиты информации

8.2.1 Правила оформления рефератов

1. Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные понятия и определения в создании программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ). Нормативно-правовая база создания ПАСОИБ.
2. Понятие доступа, субъект и объект доступа. Классификация угроз безопасности. Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами.
3. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности.
4. Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС.
5. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий,

защиты БД, защиты подсистем управления. Политика безопасности.

6. Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Порядок проектирования ПАСОИБ.
7. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
8. Структура ПАСОИБ. Компоненты и подсистемы. Типовые функции ПАСОИБ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ.
9. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.
10. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы. Управление доступом.
11. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами.
12. Классификация средств хранения ключей и идентифи-цирующей информации. Организация хранения ключей. Типовые решения в организации ключевых систем.
13. Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ.
14. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
15. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ
16. Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
17. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
18. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ.
19. Подходы к решению задачи защиты данных от изменения. Особенности защиты документов и исполняемых файлов.
20. Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты.
21. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
22. Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых

экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования.

23. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак.
24. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи
25. Основные принципы сертификации СЗИ.
26. Назначение, возможности и использование системы защиты от НСД «Secret Disk».
27. Назначение, возможности и порядок работы с персональными средствами аутентификации и защищѐнного хранения данных (USB-ключи и смарт-карты eToken).
28. Назначение, возможности и порядок работы с персональным средством криптографической защиты информации «ШИПКА».
29. Назначение, возможности и порядок работы с Электронным замком "Соболь".
30. Назначение, возможности и порядок работы с СЗИ «Dallas Lock».
31. Назначение, возможности и порядок работы с программно-аппаратным комплексом VipNet».
32. Состав и основные функции программно-аппаратного комплекса VipNet».

9. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности. Тема 1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ)	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, экзамен
Раздел 1. Тема 2. Анализ угроз информационной безопасности	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, экзамен
Раздел 1. Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 4. Основные принципы в работе ПАСОИБ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к	1	Тесты перед лекцией, тесты на семинаре, экзамен

	сдаче экзамена		
Раздел 1. Тема 5. Типовая структура и основные функции ПАСОИБ	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, экзамен
Раздел 1. Тема 6. Методы разграничения доступа и управления доступом	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 7. Методы обеспечения идентификации и аутентификации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 8. Методы и средства хранения ключевой информации	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа. Тема 9. Защита от незаконного копирования и использования программ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 10. Защита от разрушающих программных воздействий и изучения кода программ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 11. Основные подходы к защите данных от НСД	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 13. Особенности защиты данных от изменения	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 14. Основные средства крип-	Подготовка к занятию, подготовка рефератов,	1	Тесты перед лекцией, тесты на

тографической защиты	подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена		семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 15. ПАСОИБ в сетях передачи данных.	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 16. Управление безопасностью сети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 17. Сертификация СЗИ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 – URL: http://www.studentlibrary.ru/book/ISBN9785991204705.html

2. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам/ Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 – URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html

дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 – URL: http://www.studentlibrary.ru/book/ISBN9785991201216.html.

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». – URL: http://www.consultant.ru/document/cons_doc_LAW_2481/

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")– URL: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» – URL: http://www.consultant.ru/document/cons_doc_LAW_112701/

3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. – URL: http://gostexpert.ru/gost/gost-27002-2012

4. Солонская, О. И. Средства защиты информации : учебное пособие / О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 89 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/117115.html

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Программно-аппаратные средства защиты информации» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, ФМИиАТ. - Ульяновск: УлГУ, 2021. - 22 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10728

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / _____ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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, [2023]. – 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, [2023]. - 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, [2023]. – 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, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – 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, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - 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, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – 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.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских, лабораторных занятий: 3/317, 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

Используемые технические средства:

- система защиты конфиденциальной информации и персональных данных «Secret Disk;
- электронный замок "Соболь";
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken;
- система защиты от НСД «Dallas Lock»;
- персональное средство криптографической защиты информации «ШИПКА»;
- программно-аппаратный комплекс VipNet».

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

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: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО