МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
30 августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Комплексные системы защиты информации»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Профиль

«Безопасность открытых информационных систем»

Квалификация

Специалист по защите информации

Формы обучения

Очная

Москва, 2021 г.

Разработчик:

Профессор, к.э.н., доцент  /Ю.Н. Рагозин/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Содержание

1. Цели освоения дисциплины....4
2. Место дисциплины в структуре ООП специалитета....4
3. Структура и содержание дисциплины....4
3.1 Виды учебной работы и трудоемкость....5
4. Образовательные технологии....7
5. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов....9
6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине....9
6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы....9
6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания....10
7. Учебно-методическое и информационное обеспечение дисциплины....16
8. Материально-техническое обеспечение дисциплины....17
9. Методические рекомендации для самостоятельной работы студентов....177
10. Методические рекомендации для преподавателя....19

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Комплексные системы защиты информации» следует отнести:

- раскрыть структуру комплексной системы защиты информации (КСЗИ) в распределенных информационных системах, методику и технологию ее организации, принципы и содержание управления системой, методы обеспечения ее надежности.

К **основным задачам** освоения дисциплины «Комплексные системы защиты информации» следует отнести:

- определение принципов и этапов разработки КСЗИ открытых информационных систем;

- определение параметров и структуры КСЗИ открытых информационных систем;

- раскрытие структуры и методов управления КСЗИ открытых информационных систем;

- овладение методами оценки уязвимости защищаемой информации открытых информационных систем;

- установление состава мероприятий по обеспечению функционирования КСЗИ в открытых информационных системах;

- определение показателей эффективности КСЗИ в открытых информационных системах и методики ее оценки.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Комплексные системы защиты информации» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.2) основной образовательной программы специалитета (Б1.2.5).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Защита информации от утечки по техническим каналам», «Криптографические методы защиты информации», «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Управление информационной безопасностью».

3. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **4** зачетных единицы, т.е. **144** академических часа: из них **72** часов аудиторные занятия (лабораторные занятия – **72** час) и самостоятельная работа - **72** часов, форма контроля – экзамен в **9** семестре.

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**144**	9	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	9	1-18
2	**Самостоятельная работа**	**72**	9	1-18
3	**Промежуточная аттестация**	**Экзамен**	9	
	Итого:	**144**		

Структура и содержание дисциплины «Комплексные системы защиты информации» по срокам и видам работы отражены в приложении.

3.2. Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Сущность и задачи комплексной системы защиты информации	8			4		4

2	Факторы, влияющие на организацию КСЗИ	8			4		4
3	Моделирование процессов комплексной системы защиты информации	48			24		24
4	Обоснование требований к системе защиты информации на объекте защиты	48			24		24
5	Принципы организации и этапы разработки КСЗИ	8			8		8
6	Сущность и содержание контроля функционирования КСЗИ	16			4		4
7	Организационно-планирующие документы (нормативное обеспечение) по комплексной защите информации, разрабатываемые на предприятии	8			4		4
	Итого	**144**			**72**		**72**

3.3. Содержание разделов дисциплин

Тема 1. Сущность и задачи комплексной системы защиты информации

Комплексный подход к созданию системы защиты информации на современных предприятиях. Назначение комплексной системы защиты информации и принципы организации. Принципы построения комплексной системы защиты информации. Основные требования, предъявляемые к комплексной системе защиты информации. Разумная достаточность и экономическая эффективность защиты конкретного предприятия. Основные стратегии обеспечения безопасности информации на предприятии.

Тема 2. Факторы, влияющие на организацию КСЗИ

Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Количественные и качественные показатели ресурсообеспечения. Степень автоматизации основных процедур обработки защищаемой информации.

Тема 3. Моделирование процессов комплексной системы защиты информации

Понятие модели объекта. Значение моделирования процессов КСЗИ. Концептуальные модели. Модели управления защитой. Модели отношений доступа и действий. Потоковые модели.

Архитектурное построение комплексной системы защиты информации (кибернетическая, функциональная, информационная, организационная и структурная модели).

Тема 4. Обоснование требований к системе защиты информации на объекте защиты

Классификация систем защиты информации. Типовые подсистемы защиты информации. Классификация требований к системе защиты информации. Требования по назначению системы защиты информации. Требования к составу и структуре системы защиты информации. Требования по эффективности системы защиты информации.

Тема 5. Принципы организации и этапы разработки КСЗИ

Методологические основы организации КСЗИ. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Этапы разработки КСЗИ.

Тема 6. Сущность и содержание контроля функционирования КСЗИ

Понятие и виды контроля функционирования КСЗИ. Основные требования к контролю. Цель проведения контрольных мероприятий и методы контроля. Принципы и система контроля состояния защиты информации. Анализ и использование результатов проведения контрольных мероприятий.

Тема 7. Организационно-планирующие документы (нормативное обеспечение) по комплексной защите информации, разрабатываемые на предприятии

Краткая характеристика нормативного обеспечения информационной безопасности в Российской Федерации. Цели нормативного обеспечения безопасности информации внутри организации (предприятия). Создание нормативных документов, регламентирующих деятельность самой организации (предприятия) и персонала в области безопасности информации, регулирующих отношения с государством и с коллективом сотрудников. Распределение функций по защите информации среди персонала службы защиты информации организации (предприятия). Документы общего применения.

3.4. Тематика семинарских/практических занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные работы

Лабораторная работа №1: Составление модели угроз информационной безопасности РФ.

Лабораторная работа №2: Определение актуальных угроз безопасности персональных данных и их защита от НСД при обработке в информационных системах персональных данных (ИСПДн).

Лабораторная работа №3: Анализ и оценка рисков информационной безопасности.

Лабораторная работа №4: Технология защиты целостности сообщений с помощью электронной подписи.

Лабораторная работа №5: Контроль механизмов идентификации и аутентификации пользователей.

Лабораторная работа №6: Поиск и измерение побочных электромагнитных излучений СВТ программно-аппаратным комплексом «Навигатор-ПЗГ».

Лабораторная работа №7: Инструментальный контроль защищенности ОТСС, обрабатывающих цифровую информацию, представленную в виде электрических сигналов в эфире».

Лабораторная работа №8: Обнаружение и локализация средств негласного съёма информации, передающих данные по радиоканалу, программно-аппаратным комплексом «КРОНА +».

Лабораторная работа №9: Оценка защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны.

Лабораторная работа №10: Контроль эффективности защиты речевой информации от утечки по прямому акустическому и акустовибрационному каналам программно-аппаратным комплексом ПАК «Спрут-мини».

Лабораторная работа №11: Выявление каналов утечки информации за счет акустоэлектрических преобразований в ВТСС.

Лабораторная работа №12: Изучение содержания и последовательности работ по созданию комплексной системы защиты информационной системы.

Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по дисциплине «Защита информации в автоматизированных системах управления технологическим процессом» не предусмотрено учебным планом.

4. Образовательные технологии.

Методика преподавания дисциплины «Комплексные системы защиты информации» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение лабораторных работ по изучению каналов утечки информации по каналу ПЭМИ в АС;

- проведение лабораторных работ по изучению возможностей аппаратно-программных комплексов защиты рабочих станций АС от НСД;

- подготовка, представление и обсуждение презентаций на занятиях;

- разработка и защита инженерного проекта по комплексной защите информации на предприятии.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 30 % аудиторных занятий. Лабораторные занятия составляют 100 % от объема аудиторных занятий.

5. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- защита лабораторного практикума;

- подготовка презентаций по темам дисциплины и их защита;

- подготовка инженерных проектов по КСЗИ и их защита;

- экзамен в 9 семестре.

Темы презентаций (докладов), примерные темы инженерных проектов и перечень вопросов экзаменационных билетов приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности
ПК-1	Способен создавать и исследовать модели автоматизированных систем
ПК-2	Способен проводить анализ защищенности автоматизированных систем

ПК-3	Способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы
ПК-13	Способен разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем
ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации
ПК-4	Способен проводить анализ рисков информационной безопасности автоматизированной системы

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин, практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности

Показатель	Критерии оценивания			
	2	3	4	5
Уметь: применять соответствующий математический аппарат для формализации и решения профессиональных задач	Обучающийся демонстрирует полное неумение применять соответствующий математический аппарат для формализации и решения профессиональных задач	Обучающийся демонстрирует затруднения при применении соответствующего математического аппарата для формализации и решения профессиональных задач	Обучающийся демонстрирует полное умение применять соответствующий математический аппарат для формализации и решения профессиональных задач, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение применять соответствующий математический аппарат для формализации и решения профессиональных задач,. Допускаются незначительные неточности

ПК-1 Способен создавать и исследовать модели автоматизированных систем

Знать: типовые модели автоматизированных систем	Обучающийся демонстрирует полное отсутствие знаний типовых моделей автоматизированных систем	Обучающийся демонстрирует частичное знание типовых моделей автоматизированных систем	Обучающийся демонстрирует полное знание типовых моделей автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное знание типовых моделей автоматизированных систем. Допускаются незначительные неточности

Уметь: создавать и исследовать модели автоматизированных систем	Обучающийся демонстрирует полное неумение создавать и исследовать модели автоматизированных систем	Обучающийся демонстрирует частичное умение разрабатывать и анализировать модели автоматизированных систем	Обучающийся демонстрирует полное умение разрабатывать и анализировать модели автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение разрабатывать и анализировать модели автоматизированных систем Допускаются незначительные неточности

ПК-2 Способен проводить анализ защищенности автоматизированных систем

Уметь: проводить анализ защищенности автоматизированных систем	Обучающийся демонстрирует полную неспособность проводить анализ защищенности автоматизированных систем	Обучающийся демонстрирует частичное умение проводить анализ защищенности автоматизированных систем	Обучающийся демонстрирует полное умение проводить анализ защищенности автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение проводить анализ защищенности автоматизированных систем. Допускаются незначительные неточности

владеть: методами и методиками проведения анализа защищенности автоматизированных систем	Обучающийся демонстрирует полное отсутствие знаний методов и методик проведения анализа защищенности автоматизированных систем	Обучающийся демонстрирует частичное владение методами и методиками проведения анализа защищенности автоматизированных	Обучающийся демонстрирует полное владение методами и методиками проведения анализа защищенности автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное владение методами и методиками проведения анализа защищенности автоматизированных систем. Допускаются незначительные неточности

ПК-3 Способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

Знать: типовые модели угроз и модели нарушителя информационной	Обучающийся демонстрирует полное отсутствие знаний типовых моделей угроз и моделей нарушителя	Обучающийся демонстрирует частичное знание типовых моделей угроз и моделей нарушителя	Обучающийся демонстрирует полное знание типовых моделей угроз и моделей нарушителя	Обучающийся демонстрирует полное знание типовых моделей угроз и моделей нарушителя
безопасности автоматизированной системы	информационной безопасности автоматизированной системы	информационной безопасности автоматизированной системы	информационной безопасности автоматизированной системы, но допускает незначительные ошибки	информационной безопасности автоматизированной системы. Допускаются незначительные неточности
Уметь: разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Обучающийся демонстрирует полное неумение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Обучающийся демонстрирует частичное умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Обучающийся демонстрирует полное умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. Допускаются незначительные неточности

ПК-13 Способен разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

Знать: регламенты работ по обеспечению информационной безопасности автоматизированных систем	Обучающийся демонстрирует полное отсутствие знаний регламентов работ по обеспечению информационной безопасности автоматизированных систем	Обучающийся демонстрирует частичное знание регламентов работ по обеспечению информационной безопасности автоматизированных систем	Обучающийся демонстрирует полное знание регламентов работ по обеспечению информационной безопасности автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное знание регламентов работ по обеспечению информационной безопасности автоматизированных систем. Допускаются незначительные неточности
Уметь: разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности	Обучающийся демонстрирует полное неумение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности	Обучающийся демонстрирует частичное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности	Обучающийся демонстрирует полное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности	Обучающийся демонстрирует полное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности
автоматизированных систем	автоматизированных систем	автоматизированных систем	автоматизированных систем, но допускает незначительные ошибки	автоматизированных систем. . Допускаются незначительные неточности

ПК-14 Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

Знать: типовые политики информационной безопасности организации	Обучающийся демонстрирует полное отсутствие знаний типовых политик информационной безопасности организации	Обучающийся демонстрирует частичное знание типовых политик информационной безопасности организации	Обучающийся демонстрирует полное знание типовых политик информационной безопасности организации, но допускает незначительные ошибки	Обучающийся демонстрирует полное знание типовых политик информационной безопасности организации. Допускаются незначительные неточности
Уметь: принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Обучающийся демонстрирует полное неумение принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Обучающийся демонстрирует частичное умение принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Обучающийся демонстрирует полное умение принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации. Допускаются незначительные неточности
ПК-4 Способен проводить анализ рисков информационной безопасности автоматизированной системы				
Уметь: проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики	Обучающийся демонстрирует полное неумение проводить анализ рисков информационной безопасности и разрабатывать, руководить	Обучающийся демонстрирует частичное умение проводить анализ рисков информационной безопасности и разрабатывать, руководить	Обучающийся демонстрирует полное умение проводить анализ рисков информационной безопасности и	Обучающийся демонстрирует полное умение проводить анализ рисков информационной безопасности и разрабатывать, руководить

безопасности в распределенных информационных системах	разработкой политики безопасности в распределенных информационных системах	разработкой политики безопасности в распределенных информационных системах	разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах, но допускает незначительные ошибки	разработкой политики безопасности в распределенных информационных системах. Допускаются незначительные неточности
владеть: методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем	Обучающийся демонстрирует полное не владение методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем	Обучающийся демонстрирует частичное владение методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем	Обучающийся демонстрирует полное владение методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное владение методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем. Допускаются незначительные неточности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	*Описание*
Отлично	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.*
Хорошо	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.*
Удовлетворительно	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.*
Неудовлетворительно	*Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.*

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

1) основная литература:

1. Тумбинская М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095
2. Бутакова Н. Г. Криптографические методы и средства защиты информации: Учебное пособие / Н. Г. Бутакова, Н. В. Федоров. – Москва: ИЦ Интермедия, 2020. – 380 с. – ISBN 978-5-4383-0210-0. — Текст: электронный // Лань: электронно-библиотечная система. — https://e.lanbook.com/book/161347
3. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург: Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст: электронный //

2) дополнительная литература:

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для вузов. / Чудовской В.В. - М.: Академия, 2009 Гриф УМО.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с. - ISBN 5-93517-292-5: 204-33. Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 5-93517-292-5.

3. Семененко В.А. Информационная безопасность: учеб. пособие для вузов. - М.: МГИУ, 2010 Гриф УМО.

4. Электромагнитные каналы утечки информации http://uchebnik.online/uchebnik-predprinimatelstvo/elektromagnitnyie-kanalyi-

3) Электронные образовательные ресурсы

1. Рагозин Ю.Н. **ЭОР** - Курс: «Техническая защита информации». СДО «Мосполитеха», 2022 г., https://online.mospolytech.ru/
2. Рагозин Ю.Н., Сазыкина Т.С. **ЭОР** - Курс: «Защита информации от утечки по техническим каналам» СДО «Мосполитеха», 2024 г. https://online.mospolytech.ru/course/view.php?id=14934
3. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
   https://mospolytech.ru/obuchauschimsya/biblioteka/

   URL: https://e.lanbook.com/book/161337
4. Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/

8. Материально-техническое обеспечение дисциплины

Компьютерный класс с интерактивной доской. Специальное программное и техническое обеспечение по дисциплинам, определяющим комплексность защиты информации.

Для проведения лабораторных работ необходимы:

- анализатор спектра с демодуляторами с полосой частот 9КГц-3ГГц;
- интерфейс анализатора спектра с компьютером (GPIB, USB);
- набор электрических и магнитных антенн (полоса частот 9КГц-3ГГц);
- эквивалент сети;
- генераторы пространственного и линейного электромагнитного зашумления;
- генераторы акустического и виброакустического зашумления;
- программно-аппаратный комплекс **«СПРУТ-мини»;**

- многофункциональный поисковый прибор **ST-031 «Пиранья»;**

- измеритель спектра вторичных полей **«NR- μ»;**

- генератор виброакустического шума типа **«Соната АВ»;**

- генератор шума по сети 220В «**SEL SP 41/C»;**

- программно-аппаратный комплекс **«Навигатор-П-3Г**»;

- селективный нановольтметр типа **«UNIPAN-237».**

При проведении лабораторных работ с использованием специального программного обеспечения рекомендуется применение аттестованных тестовых программ из единой базы тестов ФСТЭК.

Для проведения презентаций по тематике дисциплины помещения должны быть оборудованы современными электронными досками.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.* В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачету и экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы (практические занятия) проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными комплексами, предназначенных для профессиональной деятельности будущего специалиста по ИБ АС.

Для повышения эффективности проведения лабораторных работ требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме лабораторной работы, дать перечень литературы по теме. Степень овладения практическими навыками студента при проведении лабораторных работ учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине предполагает выполнение студентами инженерных проектов, которые содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче тем инженерных проектов используется дифференцированный подход к студентам, учитывающий их приоритетные интересы в разработке проекта комплексной защиты информации в АС различных видов (типов). Перед выполнением студентами курсового проекта преподаватель проводит инструктаж по выполнению задания, который включает: цель проекта, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при курсовом проектировании.
Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется в рамках учебного процесса, а промежуточный контроль осуществляется при защите инженерного проекта и на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умение студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03 «Информационная безопасность автоматизированных систем»**.

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): **«Безопасность открытых информационных систем»**

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Комплексные системы защиты информации»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Темы презентаций (докладов)

Инженерный проект

Экзамен

Составители: к.э.н., профессор Рагозин Ю.Н.

Москва, 2021 год

Таблица

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Комплексные системы защиты информации					
ФГОС ВО 10.05.03 «Информационная безопасность автоматизированных систем»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	**уметь:** применять соответствующий математический аппарат для формализации и решения профессиональных задач	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: способен применять соответствующий математический аппарат для формализации и решения профессиональных задач

ПК-1	Способен создавать и исследовать модели автоматизированных систем	**знать:** типовые модели автоматизированных систем **уметь:** создавать и исследовать модели автоматизированных систем	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: Способен участвовать в разработке и анализе моделей автоматизированных систем Повышенный уровень: способен самостоятельно разрабатывать и анализировать модели автоматизированных систем

ПК-2	Способен проводить анализ защищенности автоматизированных систем	**уметь:** проводить анализ защищенности автоматизированных систем **владеть:** методами и методиками проведения анализа защищенности автоматизированных систем	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: способен принимать участие в проведении экспериментальных исследований системы защиты информации Повышенный уровень: Способен самостоятельно проводить экспериментальные исследования системы защиты информации и давать предложения по повышению ее эффективности

ПК-3	Способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**знать:** типовые модели угроз и модели нарушителя информационной безопасности автоматизированной системы **уметь:** разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Повышенный уровень: полное умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК-13	Способен разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**знать:** регламенты работ по обеспечению информационной безопасности автоматизированных систем **уметь:** разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: самостоятельно разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**знать:** типовые политики информационной безопасности организации **уметь:** принимать участие в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: знание типовых политик информационной безопасности и способнсть принимать участие в формировании политики информационной безопасности организации

ПК-4	Способен проводить анализ рисков информационной безопасности автоматизированной системы	**уметь:** проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах **владеть:** методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем	самостоятельная работа, лабораторные занятия	Защита инженерного проекта, экзамен	Базовый уровень: самостоятельно проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах.

Оценочные средства для текущей аттестации

Примерные темы презентаций (докладов):

1. Методологические основы организации КСЗИ.
2. Методика определения состава защищаемой информации.
3. Значение носителей защищаемой информации как объектов защиты.
4. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия в автоматизированных системах.
5. Факторы, влияющие на выбор компонентов КСЗИ в распределенных информационных системах.
6. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий.
7. Основные этапы разработки КСЗИ в АС.
8. Компьютерные вирусы и механизмы борьбы с ними.
9. Защита информации в распределенных АС.
10. Понятие и виды контроля функционирования КСЗИ в распределенных информационных системах.

По согласованию с преподавателем тема доклада может быть выбрана студентом самостоятельно.

Оценочные средства для промежуточной аттестации

Список экзаменационных вопросов по дисциплине КСЗИ:

1. Понятие и назначение КСЗИ. Концепция создания защищенных АС.
2. Требования, предъявляемые к КСЗИ
3. Факторы, влияющие на организацию КСЗИ
4. Основные этапы разработки КСЗИ
5. Определение компонентов КСЗИ
6. Функциональная модель КСЗИ
7. Организационная модель КСЗИ
8. Информационная модель КСЗИ
9. Классификация информации по видам тайн и степени конфиденциальности

10. Случайные и преднамеренные угрозы информации в компьютерных системах
11. Защита информации в АС от случайных угроз.
12. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий.
13. Методы и средства защиты от электромагнитных излучений и наводок.
14. Методы защиты от несанкционированного изменения структур АС.
15. Защита от внедрения аппаратных закладок на этапе разработки и производства.
16. Защита информации в АС от несанкционированного доступа.
17. Криптографические методы защиты информации.
18. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.
19. Структура и содержание документированного обеспечения стадии создания КСЗИ
20. Показатели защищенности системы защиты информации.
21. Общая технология управления КСЗИ
22. Принципы и методы планирования деятельности КСЗИ
23. Предпроектное обследование, эскизный проект, технический проект, рабочий проект КСЗИ
24. Методы анализа рисков информационной безопасности.
25. Методика определения состава защищаемой информации
26. Порядок разработки и внедрения перечней сведений конфиденциального характера на предприятии. Порядок внесения изменений и дополнений в перечень.
27. Характеристика основных стадий создания КСЗИ.
28. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования.
29. Значение моделирования процессов КСЗИ
30. Группы моделей системы защиты по проблемной ориентации (концептуальные модели, модели управления защитой, модели отношений доступа и действий, потоковые модели)
31. Общая характеристика подходов к оценке эффективности систем защиты информации.
32. Назначение методологического аппарата в обеспечении безопасности информации
33. Требования к организационной и технической составляющим КСЗИ

34. Источники и способы дестабилизирующего воздействия на информацию
35. Моделирование комплексной защиты автоматизированных систем.
36. Математическая постановка задачи разработки комплексной системы защиты информации.
37. Подходы к оценке эффективности КСЗИ.
38. Выбор показателей эффективности и критериев оптимальности КСЗИ.
39. Общая характеристика подходов к оценке эффективности систем защиты информации
40. Вероятностный подход к оценке эффективности системы защиты информации
41. Статистические и экспертные методы оценки эффективности системы защиты информации
42. Показатели защищенности системы защиты информации
43. Содержательная характеристика этапов разработки КСЗИ
44. Управление КСЗИ в условиях чрезвычайных ситуаций
45. Понятие и виды контроля функционирования КСЗИ.
46. Цель проведения контрольных мероприятий и методы контроля. Анализ и использование результатов проведения контрольных мероприятий.
47. Значение материально-технического обеспечения функционирования КСЗИ.
48. Значение нормативно-методического обеспечения функционирования КСЗИ.
49. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание.
50. Определение состава кадрового обеспечения функционирования КСЗИ.
51. Методы поиска решений внутри области компромиссов
52. Вероятностный подход к оценке эффективности КСЗИ
53. Методы оценки эффективности сложных информационных систем
54. Оценочный подход к оценке эффективности КСЗИ
55. Экспериментальный подход к оценке эффективности КСЗИ
56. Нормативно-методическое и материально-техническое обеспечение КСЗИ
57. Методы проведения экспертного опроса при оценке эффективности КСЗИ
58. Общая характеристика оптимального построения системы защиты для АС
59. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.

60. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации в АС. Подбор и обучение персонала.

Пример билета

1. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание.
2. Выбор показателей эффективности и критериев оптимальности КСЗИ.
3. Методика определения состава защищаемой информации