МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

/Д. Г. Демидов/

«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Комплексные системы защиты информации»

по направлению подготовки 10.05.03

«Информационная безопасность автоматизированных систем»

Образовательная программа (профиль):

«Безопасность открытых информационных систем»

Квалификация (степень) выпускника

Специалист по защите информации

Форма обучения

Очная

Год приема – 2021

Москва 2021 г.

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 распределенных информационных систем;

- определение параметров и структуры КСЗИ распределенных информационных систем;

- раскрытие структуры и методов управления КСЗИ распределенных информационных систем;

- овладение методами оценки уязвимости защищаемой информации распределенных информационных систем;

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

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

2. **Место дисциплины в структуре ООП специалитета**

Дисциплина «Комплексные системы защиты информации» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1.52) основной образовательной программы специалитета.

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

3. **Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.**

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	**Уметь:** применять соответствующий математический аппарат для формализации и решения профессиональных задач
ПК-1	Способен создавать и исследовать модели автоматизированных систем	**знать:** типовые модели распределенных информационных систем **уметь:** создавать и исследовать модели распределенных информационных систем
ПК-2	Способен проводить анализ защищенности автоматизированных систем	**уметь:** проводить анализ защищенности распределенных информационных систем **владеть:** методами и методиками проведения анализа защищенности распределенных информационных систем
ПК-3	Способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**знать:** типовые модели угроз и модели нарушителя информационной безопасности распределенных информационных систем **уметь:** разрабатывать модели угроз и модели нарушителя информационной безопасности распределенных информационных систем
ПК-13	Способен разрабатывать проекты документов, регламентирующих работу по	**знать:**

	обеспечению информационной безопасности автоматизированных систем	регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем **уметь:** разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных 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
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

4. 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.

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

Содержание разделов дисциплины

Девятый семестр

Тема 1. Основные понятия и положения защиты информации в АС.

Тема 2. Случайные и преднамеренные угрозы информации в компьютерных системах

Тема 3. Методы и средства защиты информации в автоматизированных системах

Правовые и организационные методы защиты информации в АС. Защита информации в АС от случайных угроз. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий. Методы и средства защиты от электромагнитных излучений и наводок. Методы защиты от несанкционированного изменения структур АС. Защита от внедрения аппаратных закладок на этапе разработки и производства. Защита информации в АС от несанкционированного доступа. Криптографические методы защиты информации. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.

Тема 4. Построение комплексных систем защиты информации в АС

Понятие и сущность КСЗИ. Назначение и задачи КСЗИ. Основные факторы, влияющие на организацию КСЗИ. Основные требования, предъявляемые к КСЗИ. Концепция создания защищенных АС. Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию. Моделирование комплексной защиты автоматизированных систем (КЗАС). Математическая постановка задачи разработки комплексной системы защиты информации. Подходы к оценке эффективности КЗАС. Выбор показателей эффективности и критериев оптимальности КЗАС.

Тема 5. Управление КЗАС в условиях чрезвычайных ситуаций

Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации. Факторы, влияющие на принятие решений в условиях чрезвычайной ситуации. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.

Тема 6. Сущность и содержание контроля функционирования КЗАС

Понятие и виды контроля функционирования КЗАС. Цель проведения контрольных мероприятий и методы контроля. Анализ и использование результатов проведения контрольных мероприятий.

Тема 7. Материально-техническое, нормативно-методическое и кадровое обеспечение КЗАС

Значение материально-технического обеспечения функционирования КЗАС. Определение состава материально-технического обеспечения. Значение нормативно-методического обеспечения функционирования КЗАС. Состав нормативно-методических документов по обеспечению функционирования КЗАС, их назначение, структура и содержание. Определение состава кадрового обеспечения функционирования КЗАС. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. Разработка

нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.

5. 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;

- проведение занятий лекционного типа с использованием интерактивной доски;

- 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.

6. 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	Обучающийся демонстрирует частичное умение проводить анализ защищенности автоматизированных систем	Обучающийся демонстрирует полное умение проводить анализ защищенности автоматизированных систем, но допускает	Обучающийся демонстрирует полное умение проводить анализ защищенности автоматизированных систем. Допускаются

	автоматизированных систем		незначительные ошибки	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 безопасности автоматизированной системы	Обучающийся демонстрирует полное отсутствие знаний типовых моделей угроз и моделей нарушителя информационной безопасности автоматизированной системы	Обучающийся демонстрирует частичное знание типовых моделей угроз и моделей нарушителя информационной безопасности автоматизированной системы	Обучающийся демонстрирует полное знание типовых моделей угроз и моделей нарушителя информационной безопасности автоматизированной системы, но допускает незначительные ошибки	Обучающийся демонстрирует полное знание типовых моделей угроз и моделей нарушителя 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 автоматизированных систем	Обучающийся демонстрирует полное неумение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Обучающийся демонстрирует частичное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Обучающийся демонстрирует полное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности 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 безопасности в распределенных информационных системах	Обучающийся демонстрирует полное неумение проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Обучающийся демонстрирует частичное умение проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Обучающийся демонстрирует полное умение проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение проводить анализ рисков информационной безопасности и разрабатывать, руководить 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	Обучающийся демонстрирует полное владение методами и методиками проведения анализа рисков информационной безопасности распределенных информационных систем. Допускаются незначительные неточности

			незначительные ошибки	

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

а) основная литература:

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для вузов. / Чудовской В.В. - М.: Академия, 2009 Гриф УМО **(60 экз.)**

2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации :учеб. пособие для вузов. - М.: Горячая линия-Телеком, Любое издание Гриф МО **(60 экз.)**

б) дополнительная литература:

1. Рагозин Ю.Н. Инженерно-техническая защита информации: учебное пособие/ИЦ Санкт-Петербург, 2018 – 168 с. **(50 экз)**

2. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - М.: МГИУ, 2010 Гриф УМО **(210 экз.)**

в) программное обеспечение и интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины

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

Техническое обеспечение

Анализатор спектра Agilent Technologies E4403B (с демодуляторами) или аналогичный прибор с полосой частот 9КГц-3ГГц. Интерфейс анализатора спектра с компьютером (GPIB, USB). Набор антенн электрических и магнитных антенн (полоса частот 9КГц-3ГГц). Эквивалент сети. Генератор линейного зашумления. Программно-аппаратные комплексы «Спрут-мини» и «Навигатор». Многофункциональный поисковый прибор ST- 031 «Пиранья». Детектор нелинейных переходов «NR-m» (нелинейный локатор). Поисковый программно - аппаратный комплекс «Крона+».

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»**.

Программу составил:

доцент кафедры «Информационная безопасность» к.э.н., доц. Рагозин Ю.Н.

Программа утверждена на заседании кафедры

“Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой

«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

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., доцент 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.

Инженерный проект

Цели и задачи инженерного проектирования

Инженерный проект (ИП) выполняется на базе теоретических знаний и практических навыков, полученных студентом в процессе освоения учебной дисциплины «Комплексные системы защиты информации» и оформляется в соответствии с установленными требованиями.

Основными целями курсового проектирования являются:

- овладение методами анализа угроз безопасности информации и соответствующих им уязвимостей на конкретном объекте информатизации;

- овладение навыками практической самостоятельной работы при разработке технических проектов на создание комплексных систем защиты информации предприятия (организации);

- развитие навыков самостоятельной работы с методическими материалами и литературой.

Целевой задачей ИП является разработка аналитического обоснования создания КСЗИ на конкретном объекте информатизации (предприятии, организации).

При инженерном проектировании студент должен проявлять большую самостоятельность по предложению вариантов решения поставленных задач. Инициатива по выбору окончательного решения должна принадлежать студенту. За принятые решения, а также за правильность всех расчетов и графического материала полностью отвечает автор работы.

Типовая структура инженерного проекта

Структура оформленного ИП должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам, и включать следующие части:

- титульный лист;

- оглавление (содержание) – наименование всех глав и параграфов инженерного проекта (с обязательным указанием страниц);

- введение, обосновывающее актуальность и значение защиты информации, а также цель инженерного проекта;

- основную часть из трех глав (аналитической, теоретической и практической), раскрывающую главное содержание курсового проекта. Каждая глава, как правило, подразделяется на несколько параграфов;

- заключение;

- библиографический список;

- приложение (при необходимости, объем не ограничивается).

Во **введении** обосновывается актуальность темы, её практическая значимость. Формулируется цель и конкретные задачи, связанные с вопросами проектирования. Также рекомендуется указать, на каких материалах базируется проект.

Объем введения должен быть не более двух страниц.

В **аналитической главе** приводятся исходные данные об объекте защиты:

- тип объекта, вид его деятельности и защищаемая информация;

- его дислокация, структура и поэтажные планы;

- технические характеристики ограждающих конструкций и перекрытий;

- состав и размещение основных технических средств и систем (ОТСС);

- состав и размещение вспомогательных технических средств и систем (ВТСС).

Составляется план инженерных коммуникаций здания (в масштабе) с указанием границы контролируемой зоны, места расположения трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций и силовых кабелей с указанием мест установки распределительных устройств.

Анализируются угрозы безопасности информации с построением модели злоумышленника, выявляются уязвимости объекта защиты, через которые возможна

реализация угроз (проводится анализ возможных каналов несанкционированного доступа к информации, технических каналов утечки информации с объекта защиты).

Аналитическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием главных направлений проектных решений.

Теоретическая глава посвящается теоретическим и методологическим основам построения КСЗИ, концепции создания системы защиты информации по теме инженерного проекта и соответствующие им нормативно-методические документы по защите информации. Рассматриваются модели КСЗИ (функциональная, информационная и организационная).

В теоретической части студент имеет право сделать собственные предложения по развитию, совершенствованию, модернизации, адаптации математических моделей, алгоритмов, аналитических выражений к особенностям рассматриваемых задач, может предложить собственные концепции решения задач, собственные подходы к тем или иным аспектам проблематики.

Теоретическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием решений по главным направлениям работы.

Объем теоретической части проекта может составлять 10 – 15 страниц.

Проектная часть должна содержать материал соответствующий исключительно конкретным особенностям объекта защиты и задачам разработки. Здесь должны быть реализован технический и/или рабочий проект.

В проектной части проводится анализ и сравнение характеристик промышленно выпускаемых средств защиты информации с дальнейшим обоснованием их выбора (например, по показателю «эффективность-стоимость») для нейтрализации выявленных уязвимостей объекта защиты. Проводится анализ организаций, имеющих лицензии на разработку технических проектов КСЗИ объектов информатизации. Описывается разработанная система защиты информации и приводится предлагаемая план-схема размещения пассивных и активных средств защиты информации и содержание необходимых организационных мероприятий.

Объем практической части инженерного проекта может составлять 15 - 20 страниц.

В **заключении** в сжатой форме делаются теоретические выводы по первой и третьей главам о предлагаемых решениях задач инженерного проектирования, дается оценка (при возможности) их реализуемости в практике конкретной организации (предприятия).

Объем заключения составляет, как правило, 1 - 2 страницы.

В **библиографическом списке** перечисляются все источники информации, использованные студентом при написании инженерного проекта, в том числе ссылки на материалы из сети INTERNET.

Список наименований должен содержать не менее 10 источников. Оформление списка должно выполняться по правилам, установленным государственным стандартом ГОСТ 7.1.84 «Библиографическое описание документа».

В **приложения** (таблицы, схемы, рисунки, графики большого формата, фрагменты которых используются в основном тексте) помещают материалы, которые носят

вспомогательный, поясняющий характер. Материалы приложения должны иметь порядковые номера. Объем приложения не лимитируется.

Защита инженерного проекта

Студент должен тщательно подготовиться к защите инженерного проекта.

Законченный ИП должен быть отредактирован, вычитан, подписан студентом и представлен руководителю.

После проверки ИП руководитель решает вопрос о допуске студента к защите, делая об этом соответствующую запись на титульном листе курсового проекта. Защита ИП осуществляется в форме собеседования.

По результатам защиты ИП руководитель принимает решение об оценке проекта.

Критерии оценки инженерного проекта

Оценка инженерного проекта определяется исходя из двух критериев: качества ИП и ответов на вопросы.

Оценка качества инженерного проекта

№ п/п	Наименование критерия	Оценка качества курсового проекта			
		«отлично»	**«хорошо»**	**«удовлетв.»**	**«неудовл.»**
1.	Содержание инженерного проекта	Достаточно полно разработаны все вопросы задания на ИП. Имеются обоснованные выводы по главам и в целом по проекту	Не более 20% вопросов задания на ИП разработаны недостаточно полно. Обоснованные выводы по главам и в целом по ИП в основном имеются	Более половины вопросов задания на ИП разработаны недостаточно полно. Обоснованные выводы по главам и в целом по ИП имеются частично	Не разработан (исследован) хотя бы один вопрос задания на ИП. Выводы по главам и в целом по ИП отсутствуют
2.	Обоснованность и доказательность принятых решений	Все предложения (решения) математически, логически или экспериментальн о обоснованы (доказаны)	В основном предложения (решения) математически, логически или экспериментальн о обоснованы (доказаны)	Предложения (решения) математически, логически или экспериментальн о обоснованы (доказаны) частично	Отсутствует математическое, логическое или экспериментальн о обоснованное доказательство принятых решений и разработанных предложений
3.	Соответствие чертежей, рисунков и схем требованиям ГОСТ и ЕСКД	Полностью соответствует	В основном соответствует	Частично соответствует	Не соответствует
4.	Практическое значение выполненного проекта	Имеется	В основном имеется	Частично имеется	Отсутствует

5.	Грамотность изложения и качество оформления ИП	Оформлен аккуратно. Имеются несущественные стилистические ошибки, исправления (не более одного исправления на лист)	Оформлен в основном аккуратно. Имеются несущественные стилистические и грамматические ошибки, исправления (не более трех исправлений на лист)	Оформлен небрежно. Имеются стилистические и грамматические ошибки, большое количество исправлений	Оформлен небрежно. Имеются грубые стилистические и грамматические ошибки,
6.	Самостоятельность выполнения (владение материалом), использование научной, технической и справочной литературы	Полностью самостоятельно	В основном самостоятельно	Частично самостоятельно	КП выполнен не самостоятельно

Для выставления оценки **«отлично»** необходимо, чтобы оценка по трем пунктам (включая 1 и 2) была «отлично», а по остальным - не ниже «хорошо».

Для выставления оценки **«хорошо»** необходимо, чтобы оценка по трем пунктам (включая 1 и 2) была не ниже «хорошо», а по остальным - не ниже «удовлетворительно».

При получении хотя бы по одному из пунктов неудовлетворительной оценки общая оценка не может быть выше, чем **«удовлетворительно».**

Оценка **«неудовлетворительно»** выставляется при оценке «неудовлетворительно» по 1 и 2 или по трем и более пунктам критериев.

Ответ на вопрос оценивается на:

- «отлично» - если ответ правильный, уверенный, четкий и полный;

- «хорошо» - если ответ, в основном полный, правильный и уверенный, но допущены незначительные погрешности, исправленные после дополнительных вопросов;

- **«удовлетворительно»** - если ответ неполный, неуверенный, нечеткий, отдельные положения неправильные, но путем наводящих вопросов, в основном, достигается необходимая полнота ответов;

- **«неудовлетворительно»** - если ответ сумбурный, неправильный, содержит существенные, принципиальные ошибки, а студент не понимает сущности излагаемого вопроса или не дает на него ответ.

Общая оценка за ответы на вопросы слагается из оценок, полученных за отдельные ответы, и определяется следующим образом:

- «отлично» - если отсутствуют неудовлетворительные оценки и средний балл за все оценки – не менее 4,5;

- «хорошо» - если отсутствуют неудовлетворительные оценки и средний балл за все оценки – не менее 3,5;

- «удовлетворительно» - если более половины всех оценок не ниже «удовлетворительно»;

- «неудовлетворительно» - если не выполняются требования для получения «удовлетворительной» оценки.

Итоговая оценка инженерного проекта определяется следующим образом:

- «отлично» - если по всем критериям выставлены оценки не ниже «хорошо», причем не менее, чем по двум (включая 1) критериям – «отлично»;

- «хорошо» - если по всем критериям выставлены оценки не ниже «удовлетворительно», причем не менее, чем по двум (включая 1) критериям не ниже «хорошо»;

- «удовлетворительно» - если по всем критериям выставлены оценки не ниже «удовлетворительно»;

- «неудовлетворительно» - если не выполняются требования для получения «удовлетворительной» оценки.

Примерные темы инженерных проектов, которые могут быть предложены студентам:

1. Разработка комплексной системы защиты информации в автоматизированной системе ООО «Вымпел» от промышленного шпионажа и диверсий.
2. Разработка комплексной системы защиты информации от несанкционированного доступа и от утечки по техническим каналам в распределенной АС предприятии ЗАО «Заслон».
3. Разработка комплексной системы защиты информации в кабинете генерального директора.
4. Разработка комплексной системы защиты информации при ее обработке, передаче и хранении на ПЭВМ в кабинете главного бухгалтера ООО «Аргус» .
5. Разработка комплексной системы защиты информации в локальной сети предприятия ООО «Динамо».
6. Разработка комплексной системы защиты конфиденциальной информации в АСУ ТП предприятия ЗАО «Циклон» и другие подобные варианты.

Оценочные средства для промежуточной аттестации

Список экзаменационных вопросов по дисциплине КСЗИ:

1.Случайные и преднамеренные угрозы информации в компьютерных системах

2. Защита информации в АС от случайных угроз.

3. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий.

4. Методы и средства защиты от электромагнитных излучений и наводок.

5. Методы защиты от несанкционированного изменения структур АС.

6. Защита от внедрения аппаратных закладок на этапе разработки и производства.

7. Защита информации в АС от несанкционированного доступа.

8.Криптографические методы защиты информации.

9. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.

10. Понятие и назначение КСЗИ. Концепция создания защищенных АС. Требования, предъявляемые к КСЗИ

11. Факторы, влияющие на организацию КСЗИ

12. Основные этапы разработки КСЗИ

13. Определение компонентов КСЗИ

14. Функциональная модель КСЗИ

15. Организационная модель КСЗИ

16. Информационная модель КСЗИ

17. Классификация информации по видам тайн и степени конфиденциальности

18. Методика определения состава защищаемой информации

19. Порядок разработки и внедрения перечней сведений конфиденциального характера на предприятии. Порядок внесения изменений и дополнений в перечень.

20. Характеристика основных стадий создания КСЗИ.

21. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования.

22. Моделирование комплексной защиты автоматизированных систем.

23. Математическая постановка задачи разработки комплексной системы защиты информации.

24. Подходы к оценке эффективности КСЗИ.

25. Выбор показателей эффективности и критериев оптимальности КСЗИ.

26. Общая характеристика подходов к оценке эффективности систем защиты информации

27. Вероятностный подход к оценке эффективности системы защиты информации

28. Статистические и экспертные методы оценки эффективности системы защиты информации

29. Показатели защищенности системы защиты информации

30. Содержательная характеристика этапов разработки КСЗИ

31. Управление КСЗИ в условиях чрезвычайных ситуаций

32. Понятие и виды контроля функционирования КСЗИ.

33. Цель проведения контрольных мероприятий и методы контроля. Анализ и использование результатов проведения контрольных мероприятий.

34. Значение материально-технического обеспечения функционирования КСЗИ.

35. Значение нормативно-методического обеспечения функционирования КСЗИ.

36. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание.

37. Определение состава кадрового обеспечения функционирования КСЗИ.

38. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.

39. 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

Структура и содержание дисциплины «Комплексные системы защиты информации»

по направлению подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	И.П.	ДЗ	Реферат	К/р	Э	З
1	Основные понятия и положения защиты информации в АС. Предмет и объект защиты	9	1			4	4			+					
2	Случайные и преднамеренные угрозы информации в компьютерных системах	9	2-3			4	4			+					
3.		9	4-8			20	20			+					

	Правовые и организационные методы защиты информации в АС. Защита информации в АС от случайных угроз. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий. Методы и средства защиты от электромагнитных излучений и наводок. Методы защиты от несанкционированного изменения структур АС. Защита от внедрения аппаратных закладок на этапе разработки и производства. Защита информации в АС от несанкционированного доступа. Криптографические методы защиты информации. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.														
4	**Тема 4. Построение комплексных систем защиты информации в АС** Понятие и сущность КСЗИ. Назначение и задачи КСЗИ. Основные факторы, влияющие на организацию КСЗИ. Основные требования, предъявляемые к КСЗИ. Концепция создания защищенных АС. Общее содержание работ по организации КСЗИ в распределенных информационных системах.	9	9-12			16	16			+					

	Характеристика основных стадий создания КСЗИ. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию. Моделирование комплексной защиты распределенных информационных систем. Математическая постановка задачи разработки комплексной системы защиты информации. Подходы к оценке эффективности КСЗИ. Выбор показателей эффективности и критериев оптимальности КСЗИ.														
5	Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации. Факторы, влияющие на принятие решений в условиях чрезвычайной ситуации. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.	9	13-14			8	8			+					
6	Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий и методы контроля. Анализ и	9	15-16			8	8			+					

	использование результатов проведения контрольных мероприятий.														
7	Значение материально-технического обеспечения функционирования КСЗИ в распределенных информационных системах Определение состава материально-технического обеспечения. Значение нормативно-методического обеспечения функционирования КСЗИ. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание. Определение состава кадрового обеспечения функционирования КСЗИ. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.	9	17-18			8	8			+					
8	***Форма аттестации***	9												Э	
9	**Всего часов по дисциплине**					**72**	**72**								