АННОТАЦИИ ПРОГРАММ ДИСЦИПЛИН

Направление подготовки:

10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью
Год начала обучения:

2022

Уровень образования:

Магистратура

Квалификация (степень) выпускника:

Магистр

Форма обучения:

очная

«Математические методы информационной безопасности»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Математические методы информационной безопасности» следует отнести:

- сформировать у студентов теоретические представления об основных современных методах анализа данных;
- выработать навыки практического применения методов, как к самостоятельно собираемым данным, так и к базам данных; освоение стандартов оформления результатов научно-исследовательских работ.

К **основным задачам** освоения дисциплины «Математические методы информационной безопасности» следует отнести:

- выработать навыков и умений формировать информационные ресурсы, обрабатывать содержащиеся в информационных системах данные с целью анализа социально-экономических задач и процессов для принятия управленческих решений в информационной безопасности;
- выработать у студентов представления о том, какие теоретические модели заложены в различных методах анализа данных;
- сформировать умение сопоставлять эти модели с задачами конкретного исследования и правильно выбирать метод в соответствии с его целями, задачами, гипотезами и имеющимися данными; развитие умений оценки достоверности и значимости полученных результатов; знать, как распознать программные, сетевые, аппаратно-технические атаки на объекты информатизации;
- овладеть методами анализа научной и практической значимости проводимых исследований.

В результате освоения дисциплины «Математические методы информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;	**уметь:** • проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно— технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
ПК-5. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты"	**знать:** • фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества. **уметь:** • анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества. **владеть:**

	• навыками анализа фундаментальных и прикладных проблемы информационной безопасности.
ПК-7. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	**знать:** • методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента; **уметь:** • проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента; **владеть:** • навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Математические методы информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.1).

Дисциплина «Построение и совершенствование систем управления информационной безопасностью» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Инфокогнитивные технологии».

Дисциплина обеспечивает изучение дисциплин «Методология и методы научных исследований в области защиты информации», и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 18 часов, лабораторные занятия – 54 часа, самостоятельная работа студентов – 72 часа, форма контроля – дифференцированный зачёт) в 1 семестре.

Структура и содержание дисциплины «Математические методы информационной безопасности» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**72**	1	1-18
	В том числе:			
1.1	Лекции	18	1	1-18
1.2	Семинарские/практические занятия			-
1.3	Лабораторные занятия	54	1	1-18
2	**Самостоятельная работа**	**72**	1	1-18
3	**Промежуточная аттестация**		1	6-17
	Зачет/диф. зачет/экзамен	диф. зачет	1	По расписанию
	Итого	**144**		

«Защита информации в системах обработки данных»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

Сформировать компетенции обучающегося в области защиты информации в системах обработки данных различных уровней и типов.

К **основным задачам** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

- Рассмотреть базовые дискреционные модели безопасности
- Рассмотреть базовую модель изолированной программной среды
- Рассмотреть базовые мандатные модели безопасности
- Рассмотреть базовые модели ролевого управления доступом
- Рассмотреть базовые модели безопасности информационных потоков
- Рассмотреть различные ДП-модели

Обучение по дисциплине **«Защита информации в системах обработки данных»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ИПК-4.1. Знает: программы и методики испытаний средств и систем обеспечения информационной безопасности в соответствии с нормативными актами. ИПК-4.2. Умеет: разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности ИПК-4.3. Владеет: навыками проведения испытаний средств и систем обеспечения информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах обработки данных» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы магистратуры (Б1.1.2)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Управление информационной безопасностью», «Построение и совершенствование систем управления информационной безопасностью», «Производственная практика (научно-исследовательская работа)»,

«Производственная практика (проектно-технологическая)», «Производственная практика (преддипломная)».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных(е) единиц(ы) (144 часов) во втором семестре.

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

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

«Организационное и правовое обеспечение информационной безопасности»

Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации;
- обеспечение основ правовой подготовки специалистов в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения безопасности информации.

К **основным задачам** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- овладение студентами практическими навыками использования организационных и правовых принципов и норм для защиты информации.

Обучение по дисциплине **«Организационное и правовое обеспечение информационной безопасности»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Умеет: обосновывать требования к системе обеспечения информационной безопасности; разрабатывать проект технического задания на ее создание.
ПК-14. Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ИПК-14.1. Знает: правовые нормативные актами и нормативными методическими документами ФСБ России, ФСТЭК России. ИПК-14.2. Умеет: организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности. ИПК-14.3. Владеет: навыками управления организации работ по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы магистратуры (Б1.1.3)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Управление информационной безопасностью», «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных(е) единиц(ы) (108 часов) в первом семестре.

1.1. Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**54**	2	1-18
	В том числе:			
1.1	Лекции	18	2	1-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	36	2	1-18
2	**Самостоятельная работа**	**54**	2	1-18
3	**Промежуточная аттестация**	**Диф. зачет**	Диф. зачет	19-21
	Итого:	**108**		

«Стандартизация и сертификация в информационной безопасности»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Стандартизация и сертификация в информационной безопасности» следует отнести:

- Развитие делового и логического мышления студентов, ознакомление студентов с основами теории, необходимыми для решения прикладных задач по метрологической и сертификационной деятельности средств информационной безопасности.

К **основным задачам** освоения дисциплины «Стандартизация и сертификация в информационной безопасности» следует отнести:

- Изучение основных вопросов современной теории подготовки нормативных документов;
- Изучение основ стандартизации;
- Воспитание делового и логического мышления на примере решения задач создания и принципов организации в области применения стандартов.

В результате освоения дисциплины «Стандартизация и сертификация в информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**знать:** • состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; **уметь:** • проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; **владеть:** • средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-10. Способен проводить аттестацию объектов информатизации по требованиям безопасности информации	**знать:** • как проводить аттестацию объектов информатизации по требованиям безопасности информации; **уметь:** • проводить аттестацию объектов информатизации по требованиям безопасности информации; **владеть:**

	• принципами проведения аттестации объектов информатизации по требованиям безопасности информации
ПК-14. Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	**знать:** • как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами; **уметь:** • организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами; **владеть:** • принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами

2 Место дисциплины в структуре образовательной программы

Дисциплина «Стандартизация и сертификация в информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы магистра (Б1.1.4).

Дисциплина «Стандартизация и сертификация в информационной безопасности» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Управление информационной безопасностью» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, т.е. **108** академических часов (лекции – 18 часов, лабораторные занятия – 36 часов, самостоятельная работа студентов – 54 часа, форма контроля – диф. зачет) в 1 семестре.

Структура и содержание дисциплины «Стандартизация и сертификация в информационной безопасности» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**54**	1	1-18
	В том числе:			
1.1	Лекции	18	1	-
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	36	1	1-18
2	**Самостоятельная работа**	**54**	1	1-18
3	**Промежуточная аттестация**		1	6-17
	Зачет/диф. зачет/экзамен	диф. зачет	1	По расписанию
	Итого	**108**		

«Проектирование организационно-распорядительных документов по обеспечению информационной безопасности»

1. Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины - получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем для успешной профессиональной деятельности.

Задачи дисциплины:

-изучение основ управления информационной безопасности информационных систем (ИС);

- изучение и анализ классификации угроз информационной безопасности ИС;

-изучение принципов действия основных видов сетевых атак и методов борьбы с ними;

- изучение структуры политики безопасности организации и основных этапов ее разработки;

- анализ оценочных стандартов в информационной безопасности;

- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;

- анализ методик и технологий управления рисками;

- изучение современных методов и средств анализа и управления рисками ИС компаний;

- анализ правовых мер обеспечения информационной безопасности;

- анализ организационных мер обеспечения безопасности компьютерных ИС;

- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;

- изучение основных требований и рекомендаций по защите информации в ИС;

- изучение основных юридических законов в области защиты информации.

Планируемые результаты обучения

В результате освоения дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИУК-5.1. Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, и обосновывает актуальность их использования при социальном и профессиональном взаимодействии. ИУК-5.2. Выстраивает социальное и профессиональное взаимодействие с учетом общих и специфических черт различных культур и религий, особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других наций и

	конфессий, различных социальных групп. ИУК-5.3. Обеспечивает недискриминационной взаимодействия при профессиональных задач, демонстрируя понимание особенностей различных культур и наций. создание среды выполнении
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-12. Способен организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ИПК-12.1. Знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно- технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-12.2. Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; -администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-12.3. Владеет: - навыками обоснования, выбора, реализации и контроля результатов

	управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные систем
ПК-13. Способен организовать управление информационной безопасностью	ИПК-13.1. Знает: современные подходы к управлению ИБ и направлениям их развития; основные стандарты, регламентирующие управление ИБ; принципы построения СУИБ; принципы разработки процессов управления ИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; подходы к интеграции СУИБ в общую систему управления предприятием. ИПК-13.2. Умеет: анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. ИПК-13.3. Владеет: навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и систем процессов в целом

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части блока Б1 «Дисциплины (модули)».

Дисциплина «Управление информационной безопасностью» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Защищенные информационные системы».
Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» и подготовку выпускной квалификационной работы.

3. **3. Структура и содержание дисциплины**

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	**Вид учебной работы**	**Количество часов**	**Семестры**
			2
1	**Аудиторные занятия**	**72**	2
	В том числе:		
1.1	Лекции	18	2
1.2	Семинарские/практические занятия		2
1.3	Лабораторные занятия	54	2
2	**Самостоятельная работа**	**72**	**2**
3	**Промежуточная аттестация**		**2**
	Экзамен		2
	Итого:	**144**	

Защищенные информационные системы

1. Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины:

Изучение технологий, методов и средств создания защищенных информационных систем для успешной профессиональной деятельности.

Задачи дисциплины:

1. Формирование профессиональной культуры обеспечения информационной безопасности (ИБ) в ИС.
2. Изучение принципов построения защищенных ИС.
3. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС.
4. Изучение подходов и методов обеспечения ИБ ИС.

Планируемые результаты обучения

Обучение по дисциплине «Защищенные информационные системы» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Умеет: разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.
ПК-2. Способен разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	ИПК-2.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности; ИПК-2.2. Умеет применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности; ИПК-2.3. Владеет навыками разработки систем, комплексов, средств и технологий обеспечения информационной безопасности
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ИПК-3.1. Знает: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных.

	ИПК-3.2. Умеет: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. ИПК-3.3. Владеет: навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности. ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)».

Во время освоения дисциплины «Защищенные информационные системы» студентам понадобятся знания, приобретенные ранее в ходе обучения по следующим дисциплинам:

- Методы и средства криптографической защиты информации;
- Стандартизация и сертификация в информационной безопасности;
- Защита информации в автоматизированных системах управления технологическими процессами;
- Защита информации от утечки по техническим каналам;
- Проектирование организационно-распорядительных документов по обеспечению информационной безопасности;
- Программно-аппаратные средства защиты информации.

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

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

«Построение и совершенствование систем управления информационной безопасностью»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Построение и совершенствование систем управления информационной безопасностью» следует отнести:

- обучение навыкам экономического, организационного и психологического анализа управленческих отношений, основам деловой этики и культуры управленческого труда.
- получение студентами специальных знаний и навыков в области управления различными объектами информатизации, подлежащими защите
- изучение методов проектирования, моделирования и оптимизации отдельных частей системы управления и построение комплексной системы управления.
- формирование практических навыков воздействия на социально-психологический климат, разрешение конфликтных ситуаций, разработки и принятия управленческих решений.
- приобретение студентами базовых теоретических знаний и практических навыков по экономическому обоснованию затрат на создание и эксплуатацию технических, организационных и программно-аппаратных средств системы за-щиты объектов информатизации.
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистратуры по направлению, в том числе формирование у них умений по выявлению недостатков и оценки эффективности внедрения про-грессивных технологий и средств информационной безопасности.

К **основным задачам** освоения дисциплины «Построение и совершенствование систем управления информационной безопасностью» следует отнести:

- Приобретение знаний о человеческом факторе в управлении, поведении людей в организации, их взаимодействии. Знакомство с психологической характеристикой трудовой группы и процессом её развития.
- Овладение знаниями об организации, её формах и законах, внутренней и внешней среде организации.
- Приобретение знаний об управленческих структурах и полномочиях, путях совершенствования организации управления.
- Приобретение навыков выработки рационального управленческого решения и его реализации.
- овладение принципами проведения качественного аутсорсинга и аутстаффинга в ИТ-сфере и в сфере безопасности
- Освоение методологии анализа и стоимостной оценки ущерба, наносимого владельцу информации, в результате противоправного ее использования, мето-дики оценки затрат на эксплуатацию системы информационной безопасности, технико-экономического обоснования целесообразности инвестиций в комплексные системы защиты информации предприятия..

В результате освоения дисциплины «Построение и совершенствование систем управления информационной безопасностью» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	**знать:** • требования к системе обеспечения информационной безопасности; **уметь:** • разрабатывать проект технического задания на создание системы обеспечения информационной безопасности; **владеть:** • инструментарием формирования требований к системе обеспечения информационной безопасности
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты"	**знать:** • направления развития информационных (телекоммуникационных) технологий; **уметь:** • прогнозировать эффективность функционирования объектов защиты; **владеть:** • методами оценки затрат и рисков, формирования политик безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	**знать:** • принципы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности; **уметь:** • использовать программы и методики испытаний средств и систем обеспечения информационной безопасности; **владеть:** • принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности
ПК-13. Способен организовать управление информационной безопасностью	**знать:** • способы организации управления информационной безопасностью; **уметь:** • организовать управление информационной безопасностью; **владеть:** • принципами организации управления информационной безопасностью

2 Место дисциплины в структуре образовательной программы

Дисциплина «Построение и совершенствование систем управления информационной безопасностью» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы магистра (Б1.2.1).

Дисциплина «Построение и совершенствование систем управления информационной безопасностью» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Управление информационной безопасностью» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 0 часов, лабораторные занятия – 72 часов, самостоятельная работа студентов – 72 часа, курсовой проект, форма контроля – экзамен) в 1 семестре.

Структура и содержание дисциплины «Построение и совершенствование систем управления информационной безопасностью» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**72**	1	1-18
	В том числе:			
1.1	Лекции	-	-	-
1.2	Семинарские/практические занятия			-
1.3	Лабораторные занятия		1	1-18
2	**Самостоятельная работа**	**72**	1	1-18
3	**Промежуточная аттестация**		1	6-17
	Зачет/диф. зачет/экзамен	экзамен	1	По расписанию
	Курсовой проект	диф. зачет	1	По расписанию
	Итого	**144**		

«Методология и методы научных исследования в области защиты информации»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Методология и методы научных исследования в области защиты информации» следует отнести:

- обучение навыкам обработки и анализа научно-технической информации по теме исследования в области защиты информации;
- получение студентами знаний об этапах научных исследований;
- изучение методов научного познания и овладение приемами применения их в научной деятельности;
- формирование практических навыков в области организации научных исследований;
- приобретение студентами базовых теоретических знаний и практических навыков по оценке практических и теоретических результатов научной деятельности;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистратуры по направлению, в том числе формирование у них умений по оформлению научно-технических отчетов, обзоров, научных докладов и статей.

К **основным задачам** освоения дисциплины «Методология и методы научных исследования в области защиты информации» следует отнести:

- Приобретение знаний о методах научных исследований, методологии научного поиска, принципов выбора научной проблематики в области защиты информации.
- Овладение знаниями о синтезе математических моделей систем.
- Приобретение знаний о базовых методах, применяемых в системном анализе.
- Приобретение навыков обобщения, оценивания и анализа результатов, в ходе исследований в области защиты информации.
- Овладение принципами выбора и модификации необходимых методов исходя из задач конкретного исследования.
- Освоение методологии интерпретации результатов научных исследований.

В результате освоения дисциплины «Методология и методы научных исследования в области защиты информации» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	**знать:** • требования к формулированию научных гипотез; **уметь:** • проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно—технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи; **владеть:** • навыком теоретического форсайта;

ПК-5. Способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	**знать:** • фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; **уметь:** • анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; **владеть:** • навыками анализа фундаментальных и прикладных проблемы информационной безопасности;
ПК-8. Способен обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	**знать:** • методы экспериментальных исследований; **уметь:** • применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; **владеть:** • навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;
ПК-11. Способен проводить занятия по предметной области данного направления и разрабатывать методические материалы	**знать:** • структуру и состав методических материалов, используемые в образовательной деятельности; **уметь:** • проводить экспериментально-исследовательские работы при аттестации объектов информатизации с учетом нормативных документов по защите информации; **владеть:** • навыками разработки методических материалы, используемых в образовательной деятельности;

2 Место дисциплины в структуре образовательной программы

Дисциплина «Методология и методы научных исследования в области защиты информации» относится к числу профессиональных учебных дисциплин части, формируемой участниками образовательных отношений, цикла (Б1.2) основной образовательной программы магистра (Б1.2.2).

Дисциплина «Методология и методы научных исследования в области защиты информации» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности».

Дисциплина обеспечивает изучение дисциплин «Научно-исследовательская и проектная деятельность» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 18 часов, лабораторные занятия – 54 часа, самостоятельная работа студентов – 72 часа, форма контроля – дифференцированный зачет) во 2 семестре.

Структура и содержание дисциплины «Методология и методы научных исследования в области защиты информации» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**72**	2	1-18
	В том числе:			
1.1	Лекции	18	2	1-18
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	54	2	1-18
2	**Самостоятельная работа**	**72**		
2.1	СРС		2	1-18
3	**Промежуточная аттестация**		2	6,17
	Зачет/диф. зачет/экзамен		2	По расписанию
	Курсовой проект		-	
	Итого	**144**		

«Аудит систем управления информационной безопасностью»

1. Цели, задачи и планируемые результаты обучения по дисциплине

Основной **целью** дисциплины «Аудит систем управления информационной безопасностью» является формирование у студентов знаний в области организации аудита информационной безопасности для решения задач профессиональной деятельности организационно-управленческого типа.

К **основным задачам** дисциплины «Аудит систем управления информационной безопасности» относится:

- изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации и обеспечения безопасности критической информационной инфраструктуры;
- анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите;
- выявление степени участия персонала в обработке защищаемой информации.

Обучение по дисциплине «Аудит систем управления информационной безопасностью» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации.
ПК-9. Способен проводить аудит информационной безопасности информационных систем и объектов информатизации	ИПК-9.1. Знает: каналы утечки информации. ИПК-9.2. Умеет проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. ИПК-9.3. Владеет: методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов информатизации.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений (Б1.2), частью основной образовательной программы (Б1.2.3).

Дисциплина является базовой по своим компетенциям.

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов).

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			2
1	**Аудиторные занятия**	**72**	**2**
	В том числе:		
1.1	Лекции	18	2
1.2	Семинарские/практические занятия		2
1.3	Лабораторные занятия	54	2
2	**Самостоятельная работа**	**72**	**2**
3	**Промежуточная аттестация**		**2**
	Экзамен		2
	Итого:	**144**	

Стратегии управления информационной безопасностью

1. Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого, проектного и научно-исследовательского типов в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся с российскими нормативными правовыми документами, международными и отечественными стандартами в области обеспечения информационной безопасности;

- дать представление об угрозах, рисках и уязвимостях информационной безопасности;

- сформировать умение проводить анализ проблем информационной безопасности;

- сформировать навыки разработки концепции и политики информационной безопасности; -сформировать умение разрабатывать стратегию построения и внедрения системы

управления информационной безопасностью;

-сформировать практические навыки разработки технического задания на создание системы обеспечения информационной безопасности;

- научить выполнять оценку экономической эффективности системы обеспечения информационной безопасности предприятия.

Планируемые результаты обучения

В результате освоения дисциплины «Стратегии управления информационной безопасностью» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Разрабатывает концепцию управления проектом на всех этапах его жизненного цикла в рамках обозначенной проблемы: формулирует цель и пути

	достижения, задачи и способы их решения, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения. ИУК-2.2. Разрабатывает план реализации проекта в соответствии с существующими условиями, необходимыми ресурсами, возможными рисками и распределением зон ответственности участников проекта. ИУК-2.3. Осуществляет мониторинг реализации проекта на всех этапах его жизненного цикла, вносит необходимые изменения в план реализации проекта с учетом количественных и качественных параметров достигнутых промежуточных результатов
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Демонстрирует управленческую компетентность, необходимую для формирования команды и руководства ее работой на основе разработанной стратегии сотрудничества. ИУК-3.2. Планирует, организует, мотивирует, оценивает и корректирует совместную деятельность по достижению поставленной цели с учетом интересов, особенностей поведения и мнений ее членов. ИУК-3.3. Применяет способы, методы и стратегии оптимизации социально-психологического климата в коллективе, предупреждения и разрешения конфликтов, технологии обучения и развития профессиональной и коммуникативной компетентности членов команды
УК-6. Способен определять реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. ИУК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. ИУК-6.3. Выстраивает собственную профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда

ПК-12. Способен организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ИПК-12.1. Знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно- технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-12.2. Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; -администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-12.3. Владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные систем
ПК-13. Способен организовать управление информационной безопасностью	ИПК-13.1. Знает: современные подходы к управлению ИБ и направлениям их развития; основные стандарты, регламентирующие управление ИБ; принципы построения СУИБ; принципы разработки процессов управления ИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; подходы к интеграции СУИБ в общую систему управления предприятием. ИПК-13.2.

	Умеет: анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. ИПК-13.3. Владеет: навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и систем процессов в целом

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Защита информации в системах обработки данных».

Дисциплина обеспечивает изучение дисциплин «Защита информации в автоматизированных системах управления технологическими процессами», «Защита информации от утечки по техническим каналам» и подготовку выпускной квалификационной работы.

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	**Аудиторные занятия**	**72**	3
	В том числе:		
1.1	Лекции	18	3
1.2	Семинарские/практические занятия		3
1.3	Лабораторные занятия	54	3
2	**Самостоятельная работа**	**72**	**3**
3	**Промежуточная аттестация**		**3**
	Экзамен		3
	Итого:	**144**	

«Научно-исследовательская и проектная деятельность»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Научно-исследовательская и проектная деятельность» следует отнести:

- обучение навыкам обработки и анализа научно-технической информации по теме исследования в области защиты информации;
- получение студентами знаний об этапах научно-исследовательской и проектной деятельности;
- изучение методов научно-исследовательской деятельности;
- формирование практических навыков в области проектной деятельности;
- приобретение студентами знаний в области анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистратуры по направлению, в том числе формирование у них умений по оформлению научно-технических отчетов, обзоров, научных докладов и статей.

К **основным задачам** освоения дисциплины «Научно-исследовательская и проектная деятельность» следует отнести:

- Приобретение знаний о методах научных исследований, методологии научного поиска, принципов выбора научной проблематики в области защиты информации.
- Овладение знаниями о составе этапов проектной деятельности.
- Приобретение знаний о базовых методах, применяемых в системном анализе.
- Приобретение навыков обобщения, оценивания и анализа результатов, в ходе исследований в области защиты информации.
- Овладение принципами выбора и модификации необходимых методов исходя из задач конкретного исследования.
- Освоение методологии интерпретации результатов научных исследований.

В результате освоения дисциплины «Научно-исследовательская и проектная деятельность» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.	**знать:** • функциональные особенности современных коммуникативных технологий; **уметь:** • осуществлять выбор необходимых средств для эффективной коммуникации; **владеть:** • техническими средствами поддержки коммуникативных технологий;
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и	**знать:** • государственные стандарты, этапы НИОКР; **уметь:**

программы проведения научных исследований и технических разработок;	• осуществлять сбор, обработку и анализ научно— технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок **владеть:** навыками разработки планов и программ проведения научных исследований;
ПК-6. Способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	**знать:** • методы и средства сбора, обработки, анализа и систематизации научно-технической информации по теме исследования для решения задач; **уметь:** • осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок; **владеть:** • методами и средствами сбора, обработки, анализа и систематизации научно-технической информации по теме исследования для решения задач, планами и программами проведения научных исследований и технических разработок
ПК-8. Способен обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	**знать:** • методы экспериментальных исследований; **уметь:** • применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; **владеть:** • навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;

2 Место дисциплины в структуре образовательной программы

Дисциплина «Научно-исследовательская и проектная деятельность» относится к числу профессиональных учебных дисциплин части, формируемой участниками образовательных отношений, цикла (Б1.2) основной образовательной программы магистра (Б1.2.5).

Дисциплина «Научно-исследовательская и проектная деятельность» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Методология и методы научных исследований в области защиты информации».

Дисциплина обеспечивает подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 11 зачетных единицы, т.е. **396** академических часа (лекции – не предусмотрены, лабораторные занятия – 198 часа, курсовой проект 4 семестр, самостоятельная работа студентов – 192 часа, форма контроля – дифференцированный зачет в 3 семестре, экзамен в 4 семестре).

Структура и содержание дисциплины «Научно-исследовательская и проектная деятельность» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			3	4
1	**Аудиторные занятия**	**396**	138	258
	В том числе:			
1.1	Лекции	-	-	-
1.2	Семинарские/практические занятия	-	-	
1.3	Лабораторные занятия	198	72	126
2	**Самостоятельная работа**	**198**	66	132
2.1	СРС		2	
3	**Промежуточная аттестация**		2	
	Зачет/диф. зачет/экзамен		диф. зачет	экзамен
	Курсовой проект		-	Курсовой проект
	Итого	**396**		

«Программно-аппаратные средства защиты информации»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- ознакомление студентов с современными программно-аппаратными средствами защиты информации в компьютерных системах;
- овладение методами решения задач программно-аппаратной защиты информации.

К основным задачам освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- обучение студентов современным методам программно-аппаратной защиты информации;
- приобретение профессиональной компетентности в программно-аппаратных средствах защиты информации;
- умение ориентироваться в продуктах и тенденциях развития средств программно-аппаратной защиты информационных технологий.

В результате освоения дисциплины «Программно-аппаратные средства защиты информации» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

ПК - 7. Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента ;

знать:

- возможные действия противника, направленные на нарушение политики безопасности информации;
- наиболее уязвимые для атак противника элементы компьютерных систем;

механизмы решения типовых задач программно-аппаратной защиты информации;

уметь:

-анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач;

-применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач;

-квалифицированно оценивать область применения конкретных механизмов программно-аппаратной защиты информации;

-использовать аппаратные и программные средства защиты информации при решении практических задач.

- организовать его внедрение и последующее сопровождение;
- выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации;

владеть:

- навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

ПК-15 Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

уметь:

- администрировать подсистемы информационной безопасности объекта защиты;

владеть:

- навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

Обучение по дисциплине ««Программно-аппаратные средства защиты информации» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
ПК – 7 Способен проводить экспериментальные Исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ИПК-7.1. Знает: методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. ИПК-7.2. Умеет: проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. ИПК-7.3. Владеет: навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.
ПК-15 Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к числу профессиональных учебных дисциплин обязательная части цикла (Б1.2) основной образовательной программы.

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 144 академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) во 2 семестре.

Структура и содержание дисциплины «Программно-аппаратные средства защиты информации» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	2	1-19
	В том числе:			
1.1	Лекции	-	-	-
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	72	2	3-19
2	**Самостоятельная работа**	**72**		
	В том числе:			
2.1	СРС	72	2	1-19
3	**Промежуточная аттестация**	**-**	2	6-19
	Зачет/диф.зачет/экзамен		2	По расписанию
	Итого	**144**		

«Методы и средства криптографической защиты информации»

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Методы и средства криптографической защиты информации» следует отнести:

- изучение современных методов и средств криптографической защиты информации для решения проблем защиты информации.

К **основным задачам** освоения дисциплины «Методы и средства криптографической защиты информации» следует отнести:

- овладение основными криптографическими инструментами, необходимыми для построения защищенных информационных систем.

Обучение по дисциплине «Методы и средства криптографической защиты информации» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Умеет: разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

2 Цели, задачи и планируемые результаты обучения по дисциплине

Дисциплина «Методы и средства криптографической защиты информации» относится к числу учебных дисциплин блока 1 обязательной части (Б1.1) основной образовательной программы (Б1.1.22).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Математический анализ», «Линейная алгебра», «Теория вероятностей и математическая статистика», «Основы информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

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

«Защита информации от утечки по техническим каналам»

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации от утечки по техническим каналам» следует отнести:

- теоретическую и практическую подготовленность магистра к формированию требований по защите информации от утечки по техническим каналам в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

К **основным задачам** освоения дисциплины следует отнести:

- изучение и усвоение директивных и нормативно-методических документов Федеральной службы технического и экспортного контроля (ФСТЭК) по направлению защиты информации от утечки по техническим каналам;
- практическое ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, автоматизированными системами и с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации от утечки по техническим каналам;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации защиты информации от утечки по техническим каналам на объектах информатизации.

Обучение по дисциплине направлено на формирование у обучающихся следующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-3	**Способен** проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**Знать**: - отечественные и международные стандарты информационной безопасности; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные методы и средства, в отношении которых отсутствует необходимость присвоения им категорий значимости категорий значимости обеспечения безопасности операционных систем; - основные методы и средства обеспечения сетевой безопасности; основные методы и

		средства обеспечения безопасности в системах управления базами данных. **Уметь**: - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. **Владеть**: - навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; - навыками настройки подсистем защиты основных операционных систем
ПК-7	**Способен** проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	**Знать:** - методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. **Уметь:** - проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. **Владеть**: - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» относится к числу профессиональных учебных элективных дисциплин №2 (Б1.2.ЭД.2.2) основной образовательной программы магистратуры.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП специалитета по направлению подготовки 10.05.03

(Информационная безопасность автоматизированных систем): «Математический анализ», «Теория вероятностей», «Электроника и схемотехника», «Физические основы информационной безопасности», «Основы информационной безопасности».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетных единиц, т.е. **144** академических часов (лабораторные занятия – 72 часа, самостоятельная работа – 72 часа), форма контроля – **экзамен** в 3 семестре.

3.1. Виды учебной работы и трудоемкость (по формам обучения)

Очная форма обучения

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

«Защита информации в автоматизированных системах управления технологическим процессом»

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** дисциплины «Защита информации в автоматизированных системах управления технологическим процессом» следует отнести:

- формирование у студентов теоретических знаний о необходимом комплексе мер ИБ, организационной структуре АСУ ТП, вероятных угрозах и внешних воздействиях на такие системы;
- развитие у студентов практических навыков и умений по организации и поддержании выполнения комплекса мер ИБ, управления процессом их реализации с учетом решаемых задач и организационной структуры АСУ ТП, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации; проведения анализа ИБ объектов и систем на соответствие требованиям стандартов в области защиты информации.

К **основным задачам** дисциплины «Защита информации в автоматизированных системах управления технологическим процессом» относится:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- изучение способов и средств защиты информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

Обучение по дисциплине «Защита информации в автоматизированных системах управления технологическим процессом» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.	ИПК-3.1. Знает: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных. ИПК-3.2. Умеет: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; осуществлять выбор функциональной

	структуры системы обеспечения информационной безопасности. ИПК-3.3. Владеет: навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности. ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к числу элективных дисциплин (Б1.2) основной образовательной программы (Б1.2.ЭД.2.1).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности», «Стандартизация и сертификация в информационной безопасности», «Защищенные информационные системы», «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов).

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	**Аудиторные занятия**	**72**	**3**
	В том числе:		
1.1	Лекции	-	3
1.2	Семинарские/практические занятия	-	3
1.3	Лабораторные занятия	72	3
2	**Самостоятельная работа**	**72**	**3**

3	**Промежуточная аттестация**		**3**
	Экзамен		3
	Итого:	**144**	