Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 20.10.2023 14:20:53
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

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

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Разработка и эксплуатация автоматизированных систем в защищенном исполнении»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
Должность, звание /_____/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность» /А.Ю. Гневшев/

Руководитель образовательной программы /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 4
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 5
3.3 Содержание дисциплины 5
3.4 Тематика семинарских/практических и лабораторных занятий 6
3.5 Тематика курсовых проектов (курсовых работ) 6
4 Учебно-методическое и информационное обеспечение 6
4.1 Нормативные документы и ГОСТы 6
4.2 Основная литература 7
4.3 Дополнительная литература 7
4.4 Электронные образовательные ресурсы 8
4.5 Лицензионное и свободно распространяемое программное обеспечение 8
4.6 Современные профессиональные базы данных и информационные справочные системы 8
5 Материально-техническое обеспечение 9
6 Методические рекомендации 9
6.1 Методические рекомендации для преподавателя по организации обучения 9
6.2 Методические указания для обучающихся по освоению дисциплины 9
7 Фонд оценочных средств 10
7.1 Методы контроля и оценивания результатов обучения 10
7.2 Шкала и критерии оценивания результатов обучения 10
7.3 Оценочные средства 12

1. Цели, задачи и планируемые результаты обучения по дисциплине

Учебная дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» обеспечивает формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации.

К **основным задачам** освоения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» следует отнести:

приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем;

- формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.
- определение места системы защиты информации в корпоративной информационной системе;
- определение и классификация методов защиты информации в распределенной вычислительной сети предприятия;
- раскрытие принципов, методов и технологии проектирования систем защиты информации для корпоративных информационных систем;
- изучение научных, прикладных и методологических аспектов организации технологии защиты автоматизированных систем;
- изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы;
- закрепление полученных знаний с целью их применения на практике после окончания учебы;
- управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного доступа к ее информационным, программным и аппаратным ресурсам;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;
- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

Обучение по дисциплине «Введение в аналитику информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ИОПК-14.1. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных

	системах. ИОПК-14.2. Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИОПК-14.3. Владеет методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и 26 подсистем безопасности автоматизированных систем; - методами и средствами технической защиты информации
ПК-1 Способность создавать и исследовать модели автоматизированных систем	ИПК-1.1. Знает: - модели шифров и математические методы их исследования; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; - требования к шифрам и основные характеристики 29 шифров; модели шифров и математические методы их исследования. ИПК -1.2. Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - исследовать эффективность создаваемых средств автоматизации, проводить технико - экономическое обоснование проектных решений. ИПК -1.3. Владеет: - навыками математического моделирования в криптографии; - методами и технологиями проектирования, моделирования, исследования 30 автоматизированных систем и подсистем безопасности автоматизированных систем; - навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-3 Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	ИПК-3.1. Знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.

	ИПК-3.2.Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности
ПК-5. Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	ИПК-5.1. Знает: - требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, электронную базу современных компьютеров, вычислительных и телекоммуникационны х систем; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основные информационные технологии, используемые в автоматизированных системах; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные комбинаторные и теоретико - графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК -5.2. Умеет: - анализировать программные, архитектурно - технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. ИПК -5.3. Владеет: - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - методами формирования требований по защите информации; - методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; - профессиональной терминологией в области информационной безопасности; - навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.
ПК-6. Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	ИПК-6.1. Знает: - средства обеспечения безопасности данных; - основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; - показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки ПО; - принципы организации документирования разработки, процесса сопровождения программного обеспечения; - основные структуры данных и способы их реализации на языке программирования - основные комбинаторные и теоретико -графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК_6.2. Умеет: - формировать требования и разрабатывать внешние спецификации для

	разрабатываемого программного обеспечения; - планировать разработку сложного программного обеспечения; - проводить комплексное тестирование и отладку программных систем; - проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; - проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения; - оценивать информационные риски в автоматизированных системах. ИПК -6.3. Владеет: - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - навыками проектирования программного обеспечения с использованием средств автоматизации; - навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов
ПК-7. Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	ИПК-7.1. Знает: - принципы построения и функционирования, примеры реализаций современных систем управления базами данных; - архитектуру систем баз данных; - основные модели данных; - физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных. ИПК-7.2. Умеет: - разрабатывать и администрировать базы данных; - выделять сущности и связи предметной области; - отображать предметную область на конкретную модель данных; - нормализовать отношения при проектировании реляционной базы данных; - применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации. ИПК-7.3. Владеет: - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.
ПК-16. Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	ИПК-16.1. Знает: - основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; - основные методы управления информационной безопасностью. ИПК-16.2. Умеет: - восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК -

	16.3. Владеет: - навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; - навыками использования программно - аппаратных средств обеспечения информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б.1) основной образовательной программы (Б1.1.44).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Безопасность операционных сетей ЭВМ», «Основы сетевых технологий», «Основы ИКТ», «Системы управления базами данных».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 288 часов (лабораторные занятия – 144 часа, самостоятельная работа - 144 часов, форма контроля – экзамен, курсовой проект) в 8 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**	**144**	8	1-19
	В том числе:			
1.1	Лекции	-		1-19
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	**144**	8	1-19
2	**Самостоятельная работа**	**144**	8	1-19
3	**Промежуточная аттестация**			
	Экзамен, курсовой проект			По расписанию
	Итого	**288**		

3.2. Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Защищенные АС. Основные понятия и классификация	57	-	-	28	-	29
2	Тема 2. Основы организации разработки защищенных АС	58	-	-	29	-	29
3	Тема 3. Общие принципы проектирования защищенных АС	58	-	-	29	-	29
4	Тема 4. Основы эксплуатации защищенных АС	58	-	-	29	-	29
5	Тема 5. Диагностика программных и аппаратных средств АС	57	-	-	29	-	28
Итого		**288**			**144**		**144**

3.3. Содержание дисциплины

Тема 1. Защищенные АС. Основные понятия и классификация

1.1. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. 1.2. Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.

Тема 2. Основы организации разработки защищенных АС

2.1. Последовательность и содержание этапов разработки АС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. 2.2. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС.

Тема 3. Общие принципы проектирования защищенных АС

3.1. Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. 3.2. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Технологии создания отказоустойчивых систем.

Тема 4. Основы эксплуатации защищенных АС

4.1. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Порядок обеспечения защиты информации при эксплуатации АС. 4.2. Технические и программные средства защиты АС от несанкционированного доступа. Организация технического обслуживания защищенных АС. Содержание и порядок ведения эксплуатационной документации. Методы проверки защищенных АС. Содержание и порядок ведения

эксплуатационной документации.
Тема 5. Диагностика программных и аппаратных средств АС
5.1. Средства диагностирования защищенных АС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АС. Технологическое оборудование для ремонта аппаратных средств АС. 5.2. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования. Аппаратно-программные средства диагностики АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков. Диагностика программных и аппаратных
средств АС

3.4. Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены программой.

3.4.2 Лабораторные занятия

1. Анализ рисков информационной безопасности
2. Построение концепции информационной безопасности предприятия.
3. Процедура аутентификации пользователя на основе пароля
4. Тестирование защищенности транспортного уровня.
5. Механизмы контроля целостности данных
6.Тестирование защищенности механизма управления доступом.
7.Тестирование защищенности механизма управления сессиями
8.Тестирование на устойчивость к атакам отказа в обслуживании

3.5. Тематика курсовых проектов (курсовых работ)

1. Виды, структура и безопасность автоматизированных систем.
2. Объекты защиты в автоматизированных (компьютерных) системах.
3. Общая характеристика стандартов по безопасности компьютерных систем.
4. Жизненный цикл защищенных автоматизированных систем – создание, эксплуатация и развитие, вывод из эксплуатации.
5. Эксплуатация изделий, комплексов и средств деятельности. Организационные и технические мероприятия по эксплуатации защищенных автоматизированных систем.
6. Понятие, содержание и виды технического обслуживания (регламентных работ).
7. Составляющие эксплуатации защищенных автоматизированных систем.
8. Особенности эксплуатации защищенных автоматизированных систем.
9. Угрозы безопасности на стадии эксплуатации и сопровождения АС.
10. Органы системы управления эксплуатацией защищенных автоматизированных систем функции и компетенции инженерно-технических, информационно-технологических и обеспечивающих подразделений, подразделений по защите информации.
11. Планирование эксплуатации защищенных автоматизированных систем.

12. Аудит безопасности в защищенных автоматизированных системах
13. Конструкторские эксплуатационные документы (эксплуатационные, организационно-распорядительные, учетно-отчетные) по вопросам эксплуатации.

4. Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 5 декабря 2016 г. № 646.
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N
6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // «Собрание законодательства РФ»,
14.04.2014, N 15, ст. 1691.
3. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности".
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. ГОСТ Р ИСО/МЭК 7498-1-99 Взаимосвязь открытых систем базовая эталонная модель Часть 1 Базовая модель
9. ГОСТ 24.104-85 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Автоматизированные системы управления. Общие требования
10. ГОСТ 24.202-80. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документа «Технико-экономическое обоснование»
11. ГОСТ 24.205-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по информационному обеспечению
12. ГОСТ 24.206-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по техническому обеспечению
13. ГОСТ 24.207-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по программному обеспечению
14. ГОСТ 24.208-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов стадии «Ввод в эксплуатацию»
15. ГОСТ 24.209-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по организационному обеспечению

6. ГОСТ 24.210-82 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по функциональной части
17. ГОСТ Р ИСО/МЭК 15408-2-2002 Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий Часть 2 Функциональные требования
безопасности
18. ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности».
19. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
20. ГОСТ Р ИСО/МЭК ТО 19791-2008. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Госстандарт
России
21. ГОСТ Р ИСО/МЭК 27005-2009 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», Госстандарт
России
22. ГОСТ 29339-92. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования».
23. ГОСТ Р 50739-95. «СВТ. Защита от несанкционированного доступа к информации. Общие технические требования».
24. ГОСТ Р 50752-95. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний».
25. ГОСТ Р 50922-96. «ЗИ. Основные термины и определения»
26. Руководящий документ. «АС. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1998 г.
27. Руководящий документ. «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998 г.
28. Приказ ФСТЭК России от 31 августа 2010 г. N 489 — устанавливает требования к защите информации, обрабатываемой в ИС общего пользования;
29. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 — содержит требования об обработке и защите информации, не являющейся гостайной, в ГИС;
30. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 — регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание;
31. Приказ ФСТЭК России от 14 марта 2014 г. N 31 — регламентирует работу по защите информации в АС, управляющими опасными производственными и технологическими процессами на важных и потенциально опасных объектах.

4.2. Основная литература

1. Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 293 с. — (Высшее образование). — ISBN 978-5-534-15923-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510287
2. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГРТУ, 2021. — 96 с. —

Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/220418

3. Чесалин, А. Н. Основы искусственного интеллекта с приложениями в информационной безопасности : учебное пособие / А. Н. Чесалин. — Москва : РТУ МИРЭА, 2021. — 155 с. — ISBN 978-5-7339-1589-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182429

4. Аудит безопасности информационных систем / Николай Скрабцов. – Санкт-Петербург : Питер,, 2017. – 272 с. – ISBN 978-5-4461-0662-2. 2. Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://lib.biblioclub.ru/index.php?page=book&id=93245

4.3. Дополнительная литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 28.08.2019). – ISBN 978-5-7422-4331-1. – Текст : электронный.

2. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 28.08.2019). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 28.08.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

4. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 28.08.2019). – Библиогр. в кн. – Текст : электронный.

4.4. Электронные образовательные ресурсы

Электронный образовательный ресурс разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Компьютер с операционной системой Microsoft Windows.

2. Microsoft Office.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

4. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.

5. Сайт Федеральной службы безопасности России (ФСБ России). - http://www.fsb.ru.

6. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.

7. Портал технического комитета по стандартизации «Защита информации». − http://tk.gost.ru/wps/portal/tk362

8. Информационно-аналитический Интернет-портал ISO27000.ru. − http://www.iso27000.ru/.

5. Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах.

6.2 Методические указания для обучающихся по освоению дисциплины

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, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы 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 установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Лабораторные работы проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально. Защита курсовых проектов осуществляется на последней неделе обучения в семестре.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

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

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен;
- защита курсовых проектов.

7.2 Шкала и критерии оценивания результатов обучения

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

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений				
ИОПК-14.1. Знает основные угрозы безопасности информации и модели	Обучающийся демонстрирует полное отсутствие или	Обучающийся демонстрирует неполное соответствие	Обучающийся демонстрирует частичное соответствие	Обучающийся демонстрирует полное соответствие

нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. ИОПК-14.2. Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности	недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

автоматизированных систем. ИОПК-14.3. Владеет методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и 26 подсистем безопасности автоматизированных систем; - методами и средствами технической защиты информации				
ПК-1 Способность создавать и исследовать модели автоматизированных систем				
ИПК-1.1. Знает: - модели шифров и математические методы их исследования; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; - требования к шифрам и основные характеристики 29 шифров; модели шифров и математические методы их исследования. ИПК -1.2. Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

безопасности автоматизированных систем; - исследовать эффективность создаваемых средств автоматизации, проводить технико - экономическое обоснование проектных решений. ИПК -1.3. Владеет: - навыками математического моделирования в криптографии; - методами и технологиями проектирования, моделирования, исследования 30 автоматизированных систем и подсистем безопасности автоматизированных систем; - навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - навыками анализа основных характеристик и возможностей телекоммуникационн ых систем по передаче информации; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем				
ПК-3 Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы				
ИПК-3.1. Знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).

системах (организационные, правовые, программно-аппаратные, криптографические, технические); - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационнх системах. ИПК-3.2.Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности	индикаторах компетенций дисциплины «Знать» (см. п. 3).	«Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	«Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Свободно оперирует приобретенными знаниями.
ПК-5. Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности				
ИПК-5.1. Знает: - требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, электронную базу современных компьютеров, вычислительных и телекоммуникационнх х систем; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основные информационные технологии, используемые в автоматизированных системах; - основные	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные комбинаторные и теоретико -графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК -5.2. Умеет: - анализировать программные, архитектурно - технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. ИПК -5.3. Владеет: - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - методами формирования требований по защите информации; - методиками оценки показателей качества и эффективности				

ЭВМ и вычислительных систем; - профессиональной терминологией в области информационной безопасности; - навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.				
ПК-6. Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем				
ИПК-6.1. Знает: - средства обеспечения безопасности данных; - основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; - показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки ПО; - принципы организации документирования разработки, процесса сопровождения программного обеспечения; - основные структуры данных и способы их реализации на языке программирования - основные комбинаторные и теоретико-графовые	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК_6.2. Умеет: - формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; - планировать разработку сложного программного обеспечения; - проводить комплексное тестирование и отладку программных систем; - проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; - проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения; - оценивать информационные риски в автоматизированных системах. ИПК -6.3. Владеет: - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - навыками проектирования программного обеспечения с				

использованием средств автоматизации; - навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов				
ПК-7. Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности				
ИПК-7.1. Знает: - принципы построения и функционирования, примеры реализаций современных систем управления базами данных; - архитектуру систем баз данных; - основные модели данных; - физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных. ИПК-7.2. Умеет: - разрабатывать и администрировать базы данных; - выделять сущности и связи предметной области; - отображать предметную область на конкретную модель данных; - нормализовать отношения при проектировании реляционной базы данных; - применять требования Единой системы конструкторской документации и	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

Единой системы программной документации при разработке технической документации. ИПК-7.3. Владеет: - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.				
ПК-16. Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности				
ИПК-16.1. Знает: - основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; - основные методы управления информационной безопасностью. ИПК-16.2. Умеет: - восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК -16.3.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

Владеет: - навыками эксплуатации и администрирования баз данных с учетом				

Форма промежуточной аттестации: дифференцированный зачет.

По итогам промежуточной аттестации по дисциплине (модулю) 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.

7.3 Оценочные средства

7.3. **Список вопросов для экзамена по дисциплине**

1. Виды автоматизированных систем (АС).

2. Общая характеристика систем автоматизации управленческой деятельности.

3. Структура автоматизированных систем по видам обеспечения.

4. Безопасность информации в автоматизированных системах.

5. Классификационные схемы объектов защиты в автоматизированных (компьютерных) системах.

6. Объекты защиты в защищенных автоматизированных системах.

7. Общая характеристика стандартов безопасности компьютерных систем.

8. Жизненный цикл защищенных автоматизированных систем – создание, эксплуатация и развитие, вывод из эксплуатации.

9. Общие положения по эксплуатации изделий, комплексов, средств деятельности. Понятие эксплуатации и системы эксплуатации изделий.

10. Организационные мероприятия по эксплуатации, их содержание и общая характеристика.

11. Технические мероприятия по эксплуатации защищенных автоматизированных систем - применение по назначению, техническое обслуживание, ремонт, хранение, сбережение, транспортирование, консервация.

12. Понятие, содержание и виды технического обслуживания (регламентных работ).

13. Составляющие эксплуатации защищенных автоматизированных систем.

14. Особенности эксплуатации защищенных автоматизированных систем.

15. Угрозы безопасности на стадии эксплуатации и сопровождения АС.

16. Органы системы управления эксплуатацией защищенных автоматизированных систем, функции и компетенции инженерно-технических, информационно-технологических и обеспечивающих подразделений, подразделений по защите информации.

17. Планирование эксплуатации защищенных автоматизированных систем.

18. Мониторинг, контроль, аудит безопасности в защищенных автоматизированных системах.

19. Конструкторские эксплуатационные документы.

20. Организационно-распорядительная документация и учетно-отчетная документации по вопросам эксплуатации.