Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
_____ 2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И БАЗ ДАННЫХ»

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования: специалитет
Квалификация (степень) выпускника: экономист
Форма обучения очная, заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: к.т.н., доцент Вихров А.П., Рабочая программа дисциплины: «Информационная безопасность операционных систем и баз данных». – Королев МО: ФГБОУ ВО «Технологический университет», 2023.

Рецензент: к.в.н., доцент Воронов А.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Семиков В.М., к.в.н., доцент				
Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023 г.				

Рабочая программа согласована:
Руководитель ОПОП _____ Коба Е.Е., к.э.н., доцент

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023 г.				

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ОПК-6 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;

ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-4 - Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками.

Основными задачами дисциплины являются:

1. Определение общей методологии защиты информации в информационных системах;
2. Освоение методических подходов в выборе способов и средств защиты информации;
3. Установление основных тенденций развития, направлений совершенствования информационных систем (ИС) и технологических операций, используемых при обработке данных;
4. Приобретение знаний по основам проектирования автоматизированных информационных систем (АИС), базирующимся на применении современных технических и программных средств с учётом требований безопасности;
5. Оценка степени защищённости информационных систем и алгоритмов их безопасного функционирования;
6. приобретение навыков в решении задач сбора, хранения и обработки защищаемой информации, а также овладении приёмами работы с современными пакетами прикладных программ;
7. Определение основных угроз информационной безопасности информационных систем и факторов, влияющих на требуемый уровень их защищённости;
8. Определение путей совершенствования информационных систем с учётом требований по защите информации;
9. Определение методологических подходов к оценке эффективности информационных систем.

Показатели освоения компетенции отражают следующие индикаторы:

Трудовые действия	**Необходимые умения**	**Необходимые знания**
ОПК-6. И-1 Использует современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач	ОПК-6. И-1. У-1 Умеет использовать современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач (СПС Консультант+, Гарант, TrueConf Server, Zoom, Яндекс.Телемост и др.)	ОПК-6. И-1. З-1 Знает методы работы с современными специализированными программными средствами коммуникации и справочными системами для решения профессиональных задач
ОПК-6. И-2. Использует современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач	ОПК-6. И-2. У-1 Умеет использовать современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач (один из общих или специализированных пакетов прикладных программ: PowerPoint, Word, Excel, Access и др. СУБД, системы ЭДО, CRM и ERP системы, программные продукты "1С", Альт-Финансы", " Audit Expert", IT-audit", АФСП, Project Expert, STATISTICA и т.д.); ОПК-6. И-2. У-2 Умеет работать с источниками информации, цифровыми инструментами и средами с целью поиска и обработки информации, необходимой для реализации отдельных задач стратегического планирования; ОПК-6. И-2. У-3 Умеет использовать методы коллективной работы в цифровой среде, в том числе, с интеллектуальными устройствами, для сбора, обработки и анализа данных при решении отдельных задач стратегического планирования; использовать методы визуализации данных и результатов их анализа с учетом особенностей этапов стратегического планирования; ОПК-6. И-2. У-4 Умеет интерпретировать данные и результаты их обработки с учетом особенностей этапов	ОПК-6. И-2. З-1 Знает современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач (один из общих или специализированных пакетов прикладных программ: PowerPoint, Word, Excel, Access и др. СУБД, системы ЭДО, CRM и ERP системы, программные продукты "1С", Альт-Финансы", " Audit Expert", IT-audit", АФСП, Project Expert, STATISTICA и т.д.); ОПК-6. И-2. З-2 **Знает** методы и программные инструменты поиска, сбора, обработки и анализа информации об экономических процессах и явлениях.

	стратегического планирования.	
ОПК-6. И-3. Использует электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики	ОПК-6. И-3. У-1 Умеет использовать электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики (Электронно-библиотечные системы Znanium, Ланнь, Руконт, электронная библиотека РГБ, российская научная электронная библиотека eLibrary.Ru, ProQuest и др.)	ОПК-6. И-3. З-1 Знает электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики (Электронно-библиотечные системы Znanium, Ланнь, Руконт, электронная библиотека РГБ, российская научная электронная библиотека eLibrary.Ru, ProQuest и др.)
ОПК-7. И-1 Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач	ОПК-7. И-1. У-1 Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий	ОПК-7. И-1. З-1 Знает принципы работы современных информационных технологий в экономике и программных средств
ОПК-7. И-2 Ставит задачу для решения экономических задач, понимая специфику применения информационных технологий	ОПК-7. И-2. У-1 Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных	ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных
ОПК-7- И-1 Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных	ОПК-7- И-1. У-1 Умеет составлять запрос и проанализировать извлеченные данные	ОПК-7- И-1. З-1 Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.
ПК-4. И-1 Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности	ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности	ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации, ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы	ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному обеспечению системы	ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками;

стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками	стратегического управления рисками; ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками	ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками
ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией, ПК-4.И-3. У-2 Умеет применять принципы и методы управления проектами, ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией ПК-4.И-3. З-2 Знает принципы и методы управления проектами ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя	ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками; ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.	ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных)
ПК-4. И-6 Решает поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов,	ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в	ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации; ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота; ПК-4. И-6. З-3

методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность операционных систем и баз данных» относится к дисциплинам специальной подготовки базовой части Блока 1 модуля «Информационные технологии и экономическая безопасность» основной профессиональной образовательной программы подготовки специалистов по направлению 38.05.01 «Экономическая безопасность». Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученной дисциплине: «Информационные системы в экономике», «Основы информационной безопасности», «Безопасность электронного документооборота» и компетенциях УК-1; ОПК-6; ОПК-7; ПК-4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Безопасность банковских и платежных ИС», «Информационно-аналитическая деятельность по обеспечению комплексной информационной безопасности» и выполнении выпускной квалификационной работы.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов составляет 2 зачетных единиц, 108часов.

Таблица 1-Объем дисциплины и виды учебной работы

Виды занятий	Всего часов	Семестр 7	Семестр 9	Семестр	Семестр
Общая трудоемкость	**108**				
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**32**	**32**			
Лекции (Л)	**16**	**16**			
Практические занятия (ПЗ)	**16**	**16**			
Лабораторные работы (ЛР)	**-**	**-**			
Самостоятельная работа	**76**	**76**			
Практическая подготовка	**-**	**-**			
Курсовые работы (проекты)	**-**	**-**			
Расчетно-графические работы	**-**	**-**			
Контрольная работа, домашнее задание	**+ -**	**+ -**			
Текущий контроль знаний	**тесты**	**тесты**			

Вид итогового контроля	**зачет**	**зачет**			
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**16**		**16**		
Лекции (Л)	**8**		**8**		
Практические занятия (ПЗ)	**8**		**8**		
Лабораторные работы (ЛР)	-		-		
Самостоятельная работа	**92**		**92**		
Практическая подготовка	-		-		
Курсовые, расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+ -		+ -		
Вид итогового контроля	**зачет**		**зачет**		

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2-Темы дисциплины и виды занятий

Наименование тем	Лекции, час.	Практические занятия, час	Занятия в интерактивной форме, час	Код компетенций
Тема 1: Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации	1/1	0,5/0,5	-	ОПК-6, ОПК-7, ПК-4
Тема 2: Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем	1/1	0,5/0,5	-	ОПК-6, ОПК-7, ПК-4
Тема 3: Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий	2/1	2/1	-	ОПК-6 ОПК-7 ПК-4
Тема 4: Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий	2/1	2/1	4/0,5	ОПК-6 ОПК-7 ПК-4
Тема5: Структура и содержание информационного обеспечения. Технология применения электронного документооборота	2/1	2/1	4/0,5	ОПК-6 ОПК-7 ПК-4
Тема6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации	2/1	2/1	4/1	ОПК-6 ОПК-7 ПК-4
Тема 7:Экспертные информационные системы. Проблемы безопасности	2/1	2/1	4/1	ОПК-6 ОПК-7

Наименование тем	Лекции, час.	Практические занятия, час	Занятия в интерактивной форме, час	Код компетенций
информационных систем				ПК-4
Тема 8:Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем	2/1	1/0,5	4/0,5	ОПК-6 ОПК-7 ПК-4
Тема 9:Методы и средства обеспечения информационной безопасности информационных систем	-	1/0,5	2/0,5	ОПК-6 ОПК-7 ПК-4
Итого:	**16/4**	**16/8**	**22/4**	

4.2. Содержание тем дисциплины

Тема 1. Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний.

Анализ нормативных источников, научной и учебной литературы.

Знания и умения студентов, которые должны быть получены в результате изучения курса.

Становление и развитие понятия "информационные процессы". Современные подходы к определению понятия «информатизация».

Две стороны задачи восприятия. Цель измерительного преобразования. Угловая и временная формы представления параметров передаваемой информации. Операционная схема процедуры восприятия. Первичное восприятие и измерение информации.

Тема 2. Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем

Задачи обнаружения и распознавания информации. Характеристика пространства признаков и его разбиение. Вероятностный подход при рассмотрении зависимости реализаций от состояний. Характерные случаи расположения условных распределений. Качество распознавания и его параметры.

Структура информационных ресурсов. Основные свойства информационных систем. Структурированность информационных систем. Принципы построения информационных систем. Многоуровневость и

распределенность информационных систем. Особенности применения информационных систем в различных областях. Интегрированные информационные системы.

Тема 3. Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий

Определение автоматизированных информационных технологий (АИТ). Основные компоненты АИТ. Виды классификаций АИТ. Основные тенденции развития АИТ в современных условиях. Интегрированные информационные системы обработки данных и способы защиты информации. Многоуровневые и распределённые информационные системы организационного управления.

Система управления и её роль в процессе получения информации и её обработки с помощью заданных алгоритмов. Технологические процессы при обработке данных. Основные задачи автоматизированных информационных систем (АИС). Структура и составные элементы АИС и АИТ. Функции АИТ. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ

Тема 4. Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий

Цель и задачи проектирования АИТ и АИС. Основополагающие принципы создания АИС. Принцип системности – важнейший принцип при создании, функционировании и развитии АИС. Стадии жизненного цикла АИС и АИТ. Модели жизненного цикла АИС и АИТ. Особенности разработки АИС и АИТ.

Особенности создания АИТ. Основные требования к АИТ с учётом информационной безопасности. Аппаратно-программные комплексы, используемые при создании АИТ. Классы пользователей АИТ.

Тема 5. Структура и содержание информационного обеспечения. Технология применения электронного документооборота

Определение информационного обеспечения. Организация информационного обеспечения. Классификаторы, коды и технология их применения. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.

Последовательность прохождения документов. Автоматизация движения информационных потоков. Система поиска. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

Тема 6. Информационные базы и банки данных. Базы знаний.

Цели и задачи технологического обеспечения. Режимы обработки информации

Технология информационных баз и банков данных. Требования, предъявляемые к информационным базам данных. Распределённая система информационных баз и банков данных. Этапы создания информационных баз и банков данных. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.

Техническое обеспечение. Средства обработки информации. Распределённая система обработки информации. Условия разработки и выбора программного обеспечения. Классификация программного обеспечения. Диалоговый режим обработки информации. Сетевой режим обработки информации.

Тема 7. Экспертные информационные системы. Проблемы безопасности информационных систем

Определение экспертной системы. Технология применения экспертных систем. Разработка экспертных систем. Преимущества использования экспертных систем. Отличительные особенности экспертных систем. Области применения экспертных систем. Уязвимость экспертных систем.

Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз. Мероприятия по предотвращению угроз безопасности информационных систем. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.

Тема 8. Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

Глобальные информационные сети и системы, их свойства. Правовые аспекты информационного обмена в глобальных сетях. Особенности отношений субъектов информационного обмена в сетях. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости. Роль стандартов информационной безопасности при создании информационных систем.

Основные стадии жизненного цикла системы защиты информации. Общая методология в выборе средств и способов защиты информации в информационных системах. Модель построения системы защиты информации. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

Тема 9. Методы и средства обеспечения информационной безопасности информационных систем

Методы и средства защиты информации в информационных

системах. Два подхода к проблеме обеспечения информационной безопасности информационных систем. Пути решения проблем защиты информации в информационных системах. Задачи управления средствами информационной безопасности. Политики безопасности. Протоколы безопасной передачи данных.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность операционных систем и баз данных» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 04.10.2022). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

2. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. URL: https://urait.ru/bcode/451231

3. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов / В.Г. Проскурин. – Москва : Горячая линия – Телеком, 2014. – 192 с. : ил. – URL: https://biblioclub.ru/index.php?page=book&id=275128

Дополнительная литература:

1.Балдин, К. В. Информационные системы в экономике : учебник / К. В. Балдин, В. Б. Уткин. – 9-е изд., стер. – Москва : Дашков и К°, 2021. – 395 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=684194 (дата обращения:

04.10.2022). – Библиогр. в кн. – ISBN 978-5-394-04038-2. – Текст : электронный.

2. Информатика и математика : учебник и практикум для вузов / Т. М. Беляева [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 402 с. — URL: https://urait.ru/bcode/451169

Рекомендуемая литература:

1. Васильков А.В. Информационные системы и их безопасность. Учебное пособие, М.: «Форум», 2010.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М.: «Форум»-Инфра-М. 2008.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp –** научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды «МГОТУ».
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационная безопасность операционных систем и баз данных»
3. Информационно – справочные (правовые) системы:
   – «Гарант»;
   – «Кодекс»;
   – «Консультант +».

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows-10; офисные программы MSOffice;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И БАЗ ДАННЫХ»

(Приложение 1 к рабочей программе)

Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Квалификация (степень) выпускника: экономист
Форма обучения: очная, заочная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Трудовые действия	**Необходимые умения**	**Необходимые знания**
1	ОПК-6	способен использовать современные информационные технологии и программные средства при решении профессиональных задач	Темы 1-9	ОПК-6. И-1 Использует современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач	ОПК-6. И-1. У-1 Умеет использовать современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач (СПС Консультант+, Гарант, TrueConf Server, Zoom, Яндекс.Телемост и др.)	ОПК-6. И-1. З-1 Знает методы работы с современными специализированными программными средствами коммуникации и справочными системами для решения профессиональных задач
				ОПК-6. И-2. Использует современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач	ОПК-6. И-2. У-1 Умеет использовать современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач (один из общих или специализированных пакетов прикладных программ: PowerPoint, Word, Excel, Access и др. СУБД, системы ЭДО, CRM и ERP системы, программные продукты "1С", Альт-Финансы", " Audit Expert", IT-audit", АФСП, Project Expert, STATISTICA и т.д.); ОПК-6. И-2. У-2 Умеет работать с источниками информации, цифровыми инструментами и средами с целью	ОПК-6. И-2. З-1 Знает современные информационные технологии в экономике и программные средства для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач (один из общих или специализированных пакетов прикладных программ: PowerPoint, Word, Excel, Access и др. СУБД, системы ЭДО, CRM и ERP системы, программные продукты "1С", Альт-Финансы", " Audit Expert", IT-audit", АФСП, Project Expert, STATISTICA и т.д.); ОПК-6. И-2. З-2 **Знает** методы и программные инструменты поиска, сбора, обработки и анализа информации об экономических процессах и

					поиска и обработки информации, необходимой для реализации отдельных задач стратегического планирования; ОПК-6. И-2. У-3 Умеет использовать методы коллективной работы в цифровой среде, в том числе, с интеллектуальными устройствами, для сбора, обработки и анализа данных при решении отдельных задач стратегического планирования; использовать методы визуализации данных и результатов их анализа с учетом особенностей этапов стратегического планирования; ОПК-6. И-2. У-4 Умеет интерпретировать данные и результаты их обработки с учетом особенностей этапов стратегического планирования.	явлениях.
				ОПК-6.И-3. Использует электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики	ОПК-6.И-3. У-1 Умеет использовать электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики (Электронно-библиотечные системы Znanium, Ланнь, Руконт, электронная библиотека РГБ, российская научная электронная библиотека eLibrary.Ru, ProQuest и др.)	ОПК-6.И-3. З-1 Знает электронные библиотечные системы для поиска необходимой научной литературы и социально-экономической статистики (Электронно-библиотечные системы Znanium, Ланнь, Руконт, электронная библиотека РГБ, российская научная электронная библиотека eLibrary.Ru, ProQuest и др.)

2	ОПК-7	способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Темы 1-9	ОПК-7. И-1 Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач	ОПК-7. И-1. У-1 Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий	ОПК-7. И-1. З-1 Знает принципы работы современных информационных технологий в экономике и программных средств
				ОПК-7. И-2 Ставит задачу для решения экономических задач, понимая специфику применения информационных технологий	ОПК-7. И-2. У-1 Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных	ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных
				ОПК-7- И-1 Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных	ОПК-7- И-1. У-1 Умеет составлять запрос и проанализировать извлеченные данные	ОПК-7- И-1. З-1 Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.

3	ПК-4:	способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками.	Темы 1-9	ПК-4. И-1 Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности	ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности	ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации, ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
				ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками	ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному обеспечению системы стратегического управления рисками; ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения	ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками; ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками

	системы управления рисками	
ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией, ПК-4.И-3. У-2 Умеет применять принципы и методы управления проектами, ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией ПК-4.И-3. З-2 Знает принципы и методы управления проектами ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя	ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками; ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.	ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных)

				ПК-4. И-6 Решает поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации; ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота; ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-6	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Оформляется письменно, защита осуществляется с использованием мультимедийных систем, а также с использованием технических средств
ОПК-7	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Оформляется письменно, защита осуществляется с использованием мультимедийных систем, а также с использованием технических средств
ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Задание 1

Какие требования надо выполнить в установках (настройках) Подсистемы управления доступом защищенной операционной системы для обеспечения класса защиты АС от НСД 1Д. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы управления доступом защищенной ОС для обеспечения класса защиты АС от НСД 1Д необходимо выполнить следующие требования:

должна осуществляться идентификация (1-й элемент) и проверка подлинности субъектов доступа при входе в систему (2-й элемент) по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов (3-й элемент).

Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации«Автоматизированные системы. Защита от несанкционированного доступа к информацииКлассификация автоматизированных систем и требования по защите информации», утвержденым решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. (4-й элемент).

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает четыре названных выше элемента, но содержит негрубые ошибки.	100%
Ответ включает три-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает один-два из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 2

Какие требования надо выполнить в установках (настройках) Подсистемы регистрации и учета защищенной операционной системы для обеспечения класса защиты АС от НСД 1Д. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы регистрации и учета защищенной ОС для обеспечения класса защиты АС от НСД 1Д необходимо выполнить следующие требования:

1. - должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

2. - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;

3. - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

4. - должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);

5. - учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

6. - требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. (4-й элемент).

Время, отводимое на выполнение задания: 10 минут.
Критерии оценивания:

Ответ включает пять названных выше элемента, но содержит негрубые ошибки.	100%
Ответ включает три-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает два из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 3

Какие требования надо выполнить в установках (настройках) Подсистемы обеспечения целостности защищенной операционной системы для обеспечения класса защиты АС от НСД 1Д. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы обеспечения целостности защищенной ОС для обеспечения класса защиты АС от НСД 1Д необходимо выполнить следующие требования:

1. - должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

2. - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

3. - должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

4. - должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

5. - должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

6. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает все названные выше элементы, но содержит негрубые ошибки.	100%
Ответ включает четыре из названных выше элементов, и не содержит ошибок или Ответ включает четыре названных выше элемента, но содержит негрубые ошибки.	66,67%
Ответ включает два из названных выше элементов и не содержит ошибок. или Ответ содержит три из названных выше элементов, но содержит негрубые ошибки	33,33%
Ответ неправильный	0%

Задание 4

Какие требования надо выполнить в установках (настройках) Подсистемы управления доступом защищенной операционной системы для обеспечения класса защиты АС от НСД 1В. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы управления доступом защищенной ОС для обеспечения класса защиты АС от НСД 1В необходимо выполнить следующие требования:

1. - должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
2. - должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам;
3. - должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
4. - должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
5. - должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.
6. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает пять названных выше элемента, но содержит негрубые ошибки.	100%
Ответ включает три-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает два из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 5

Какие требования надо выполнить в установках (настройках) Подсистемы регистрации и учета защищенной операционной системы для обеспечения класса защиты АС от НСД 1В. В каком документе это определено.

Ключ:
В параметрах настройки Подсистемы регистрации и учета защищенной ОС для обеспечения класса защиты АС от НСД 1В необходимо выполнить следующие требования:

1. - должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

2. - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;

3. - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

4. - код или пароль, предъявленный при неуспешной попытке;

5. - должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

6. - дата и время выдачи (обращение к подсистеме вывода);

7. - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

8. - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

9. - идентификатор субъекта доступа, запросившего документ;

10. - объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

11. - должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

12. - дата и время запуска;

13. - имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);

14. - результат запуска (успешный, неуспешный - несанкционированный);

15. - должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

16. - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

17. - идентификатор субъекта доступа;

18. - спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;

19. - вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

20. - должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

21. - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

22. - идентификатор субъекта доступа;

23. - спецификация защищаемого объекта [логическое имя (номер)];

24. - имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

25. - должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

26. - дата и время изменения полномочий;

27. - идентификатор субъекта доступа (администратора), осуществившего изменения;

28. - должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

29. - должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);

30. - учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

31. - должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

32. - должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

33. - должна осуществляться сигнализация попыток нарушения защиты.

34. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.
Критерии оценивания:

Ответ включает десять названных выше элемента, но содержит негрубые ошибки.	100%
Ответ включает шесть-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает четыре из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 6

Какие требования надо выполнить в установках (настройках) Подсистемы управления доступом: защищенной операционной системы для обеспечения класса защиты АС от НСД 2Б. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы управления доступом защищенной ОС для обеспечения класса защиты АС от НСД 2Б необходимо выполнить следующие требования:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) (1-й элемент) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов (2-й элемент).

Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. (3-й элемент).

Время, отводимое на выполнение задания: 10 минут.
Критерии оценивания:

Ответ включает три названных выше элемента, но содержит негрубые ошибки.	100%

Ответ включает два-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает один из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 7

Какие требования надо выполнить в установках (настройках) Подсистемы регистрации и учета защищенной операционной системы для обеспечения класса защиты АС от НСД 2Б. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы регистрации и учета защищенной ОС для обеспечения класса защиты АС от НСД 2Б необходимо выполнить следующие требования:

1. должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

2. - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);

3. - должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

4. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает четыре названных выше элемента, но содержит негрубые ошибки.	100%
Ответ включает три-из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает два из названных выше элементов и не содержит ошибок.	33,33%
Ответ неправильный	0%

Задание 8

Какие требования надо выполнить в установках (настройках) Подсистемы обеспечения целостности защищенной операционной системы для обеспечения класса защиты АС от НСД 2Б. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы обеспечения целостности защищенной ОС для обеспечения класса защиты АС от НСД 2Б необходимо выполнить следующие требования:

1. должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

2. - целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

3. - целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

4. - должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

5. - должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

6. - должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД, их периодическое обновление и контроль работоспособности.

7. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает шесть названных выше элементов и не содержит ошибок	100%
Ответ включает три-четыре из названных выше элементов, и не содержит ошибок	66,67%

или Ответ включает четыре названных выше элемента, но содержит негрубые ошибки.	
Ответ включает один-два из названных выше элементов и не содержит ошибок. или Ответ содержит два-три из названных выше элементов, но содержит негрубые ошибки	33,33%
Ответ неправильный	0%

Задание 9

Какие требования надо выполнить в установках (настройках) Подсистемы управления доступом защищенной операционной системы для обеспечения класса защиты АС от НСД 2А. В каком документе это определено.

Ключ: В параметрах настройки Подсистемы управления доступом ОС для обеспечения класса защиты АС от НСД 2А необходимо выполнить следующие требования:

1. - должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
2. - должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);
3. - должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
4. - должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.
5. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.

Критерии оценивания:

Ответ включает четыре названных выше элементов и не содержит ошибок	100%
Ответ включает три-четыре из названных выше элементов, и не содержит ошибок или	66,67%

Ответ включает четыре названных выше элемента, но содержит негрубые ошибки.	
Ответ включает один-два из названных выше элементов и не содержит ошибок. или Ответ содержит два-три из названных выше элементов, но содержит негрубые ошибки	33,33%
Ответ неправильный	0%

Задание 10

Какие требования надо выполнить в установках (настройках) Подсистемы регистрации и учета защищенной операционной системы для обеспечения класса защиты АС от НСД 2А. В каком документе это определено.

Ключ:

В параметрах настройки Подсистемы регистрации и учета ОС для обеспечения класса защиты АС от НСД 2А необходимо выполнить следующие требования:

1. - должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

2. - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);

3. - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

4. - должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц).

В параметрах регистрации указываются:

5. - дата и время выдачи (обращения к подсистеме вывода);

6. - спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

7. - идентификатор субъекта доступа, запросившего документ;

8. - должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

9. - дата и время запуска;

10. - имя (идентификатор) программы (процесса, задания);

11. - идентификатор субъекта доступа, запросившего программу (процесс, задание);

12. - результат запуска (успешный, неуспешный - несанкционированный);

13. - должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

14. - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная,

15. - идентификатор субъекта доступа;

16. - спецификация защищаемого файла;

17. - должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

18. - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

19. - идентификатор субъекта доступа;

20. - спецификация защищаемого объекта [логическое имя (номер)];

21. - должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

22. - должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

23. - учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

24. - должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

25. Требования изложены в РД Государственной технической комиссии при Президенте Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Время, отводимое на выполнение задания: 10 минут.
Критерии оценивания:

Ответ включает десять названных выше элементов и не содержит ошибок	100%
Ответ включает семь из названных выше элементов, и не содержит ошибок	66,67%
Ответ включает четыре из названных выше элементов и не содержит ошибок	33,33%
Ответ неправильный	0%

Темы рефератов (докладов)

1. Виды атак на сетевые информационные системы и методы борьбы с ними.
2. Скорость передачи информации дискретных каналов с помехами.
3. Современные системы электронного документооборота и показатели их защищённости.
4. Информационная безопасность электронного бизнеса.
5. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах.
6. Методы оценки эффективности функционирования современных информационных систем.
7. Перспективные информационные системы, технологии управления и обеспечение их безопасности.
8. Методы разграничения доступа в информационных системах.
9. Интегрированные и корпоративные информационные системы, проблемы их защищённости.
10. Статистические критерии обнаружения и распознавания информации.

Примерная тематика заданий на контрольную работу:

1. Задача стандартизации при разработке систем защиты информации.
2. Правовая основа защиты информации на объектах информатизации.
3. Криптографические методы защиты информации в современных информационных системах.
4. Компьютерные вирусы и проблемы антивирусной защиты.
5. Организация защиты при обмене данными в информационных системах.
6. Протоколы, применяемые для защиты информации в сетевых информационных системах.
7. Проблемы обеспечения информационной безопасности беспроводных информационных систем.

8. Общая методология выбора средств и способов защиты информации в информационных системах.

9. Организация парольной защиты в информационных системах.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Информационная безопасность операционных систем и баз данных» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-6, ОПК-7, ПК-4	20-40 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-6, ОПК-7, ПК-4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Зачет	ОПК-6, ОПК-7, ПК-4	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** – знание основных понятий предмета; – умение использовать и применять полученные знания на практике; – работа на семинарских

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						занятиях; – знание основных научных теорий, изучаемых предметов; – ответ на вопросы билета. **«Не зачтено»:** – демонстрирует частичные знания по темам дисциплин; – незнание основных понятий предмета; – неумение использовать и применять полученные знания на практике; – не работал на семинарских занятиях; – не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

Первый тест для текущего контроля

1. Какую модель используют для построения системы управления информационной безопасностью на предприятии:

*модель PDCA (Plan-Do-Chek-Act)

семи-рубежную модель защиты информации

семи-уровневую эталонную модель взаимодействия открытых систем

шести-рубежную модель защиты информации

Время отводимое на выполнение задания (теста) - 2 минуты.

Критерии оценивания: верный ответ соответствует 100 %.

2. Сколько установлено классов защищенности АС от НСД к информации:
3 класса
5 классов
6 классов
*9 классов

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

3. Что входит в функции систем мониторинга:
выявление состояния систем
установка отношений между объектами
установка соответствия правил и обязанностей
*все варианты верны

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

4. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
*анализа рисков информационной безопасности организации
мониторинга функционирования средств защиты информации

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

5. Без непосредственного участия службы безопасности (режимно-секретного подразделения) совещания могут проводиться:
с фирмами партнерами
встречи, совещания с гарантированным заключением сделок
совещания с представителями конкурирующих организаций
*внутренние совещания

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

6. Независимо от степени конфиденциальности рассматриваемых на совещании вопросов участникам совещания не разрешается:
информировать о факте, месте, времени проведения совещания, повестке дня, рассматриваемых вопросах и ходе их обсуждения любых лиц, не принимающих участия в совещании и не имеющих к нему непосредственного отношения

в ходе совещания производить выписки из документов и иных носителей конфиденциальной информации, используемых при обсуждении, на неучтенные в установленном порядке носители (отдельные листы бумаги и т.п.)
обсуждать вопросы, вынесенные на совещание, в местах общего пользования во время перерывов в совещании и после его завершения
в ходе проведения совещания расширять объем конфиденциальной информации, используемой в выступлениях, а также при обмене мнениями и обсуждении рассматриваемых вопросов
*все выше перечисленное

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

7. Основной функцией аналитического подразделения не является:
обеспечение своевременного поступления достоверных и всесторонних сведений по проблемам защиты информации
учет, обобщение и постоянный анализ материалов о состоянии дел в системе защиты информации предприятия (его филиалов и представительств)
* изменение кода ПО для устранения уязвимости

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

8. В аналитической работе можно выделить следующие основные этапы:
*формулирование целей аналитической работы, разработка программы исследований, формулирование предварительных гипотез (результатов аналитической работы)
*отбор и анализ источников информации, сбор и обобщение информации
проверка на актуальность существующей документации
*полноценный анализ имеющейся информации и подготовка выводов

Наиболее НЕтипичные задачи аналитического исследования:
получение данных о состоянии системы защиты информации на предприятии (его конкретных объектах, в филиалах, представительствах)
*выявление возможных вариантов утраты/блокировки информации подлежащей защите
выявление возможных каналов утечки информации, подлежащей защите
определение обстоятельств, причин и факторов, способствующих возникновению каналов утечки и созданию предпосылок для утечки информации

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

9. В аналитической работе при проведении оценки указанных элементов, как правило, НЕ используется следующий критерий:
* оценка актуальности
оценка источника
оценка полученной информации
оценка получения информации источником

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

10. В основные направления аналитической работы на предприятии входит:
анализ объекта защиты
анализ внутренних и внешних угроз информационной безопасности предприятия
анализ возможных каналов несанкционированного доступа к информации
* моделирование потенциальных атак

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

11. Система КОНДОР (программный продукт КОНДОР, разработанный российской компанией DigitalSecurity, предназначен для проверки соответствия политики информационной безопасности компании)предназначена для проверки стандарта:
ГОСТ Р 50922-96
ГОСТ Р 51275-99
ISO 9001
*ISO 17799
Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

12. Какой программный продукт относится к сетевым сканерам:
*MaxPatrol 8
PT ISIM
HP ArcSight
SearchInform Контурбезопасности

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

13. Работу по планированию мероприятий в области защиты информации, проводимых в ходе совещания с участием представителей сторонних организаций, возглавляют:

*на руководителя предприятия совместно с его заместителями
на независимое стороннее лицо
на представителя вышестоящей организации или ведомства
на руководителей организаций-партнеров участников совещания

Время отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

14. Наиболее актуальными и значимыми совещаниями с точки зрения проведения подготовительных мероприятий по защите информации являются:

совещания совета директоров
совещания отдела безопасности предприятия
совещания отдела кадров предприятия
*совещания предприятия с участием представителей сторонних организаций

Время, отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

15. Мероприятия по обеспечению защиты информации на организуемых на предприятии совещаниях проводятся:

*при подготовке, а также в ходе проведения и по окончанию совещания
перед началом совещания
непосредственно во время совещания
во время начала а также окончания совещания

Время, отводимое на выполнение задания (теста) - 2 минуты.
Критерии оценивания: верный ответ соответствует 100 %.

Вопросы, выносимые на зачет

1. Понятие "информационный процесс". Восприятие информации.
2. Операционная схема процедуры восприятия информации.
3. Две стороны задачи восприятия. Цель измерительного преобразования.
4. Угловая и временная формы представления параметров передаваемой информации.
5. Первичное восприятие и измерение информации.
6. Задачи обнаружения и распознавания информации.
7. Характеристика пространства признаков и его разбиение.
8. Качество распознавания и его параметры.
9. Свойства информационных систем. Структурированность информационных систем.

10. Принципы построения защищённых информационных систем.
11. Интегрированные информационные системы и их защищённость.
12. Основные тенденции развития АИТ в современных условиях.
13. Интегрированные информационные системы обработки данных и способы защиты информации.
14. Многоуровневые и распределённые информационные системы организационного управления.
15. Структура и составные элементы АИС и АИТ. Функции АИТ.
16. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ.
17. Определение информационного обеспечения. Организация информационного обеспечения.
18. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.
19. Автоматизация движения информационных потоков. Система поиска.
20. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.
21. Требования, предъявляемые к информационным базам данных.
22. Распределённая система информационных баз и банков данных.
23. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.
24. Техническое обеспечение. Средства обработки информации.
25. Распределённая система обработки информации.
26. Диалоговый режим обработки информации.
27. Сетевой режим обработки информации.
28. Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз.
29. Мероприятия по предотвращению угроз безопасности информационных систем.
30. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.
31. Глобальные информационные сети и системы, их свойства.
32. Правовые аспекты информационного обмена в глобальных сетях.
33. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости.
34. Роль стандартов информационной безопасности при создании информационных систем.
35. Основные стадии жизненного цикла системы защиты информации.
36. Общая методология в выборе средств и способов защиты информации в информационных системах.
37. Модель построения системы защиты информации.
38. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

39. Методы и средства защиты информации в информационных системах.

40. Два подхода к проблеме обеспечения информационной безопасности информационных систем.

41. Пути решения проблем защиты информации в информационных системах.

42. Задачи управления средствами информационной безопасности. Политики безопасности.

43. Протоколы безопасной передачи данных.

44. Свойства и параметры сложных информационных систем.

45. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И БАЗ ДАННЫХ»

(Приложение 2 к рабочей программе)

Специальность:38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

1. Общие положения

Цели изучения дисциплины:

- формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества;

- закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.

- В процессе обучения студент приобретает и совершенствует следующую компетенцию:

ОПК-6 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;

ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-4 - Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками.

получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Основными задачами дисциплины являются:

1. Ознакомление студентов с информационными процессами на предприятии с точки зрения информационной безопасности;
2. Формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
3. Формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

2. Указания по проведению практических занятий

Практическое занятие 1.Идентификация пользователей КС - субъектов доступа к данным.

Образовательные технологии: технология активного метода обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Понятие идентификации пользователя.
2. Задача идентификации пользователя.

3. Понятие протокола идентификации.

4. Локальная и удаленная идентификация.

5. Идентифицирующая информация. Понятие идентифицирующей информации.

Способы хранения идентифицирующей информации, связь с ключевыми системами.

Практическое занятие 2. Предмет и задачи программно-аппаратной защиты информации.

Образовательные технологии: технология формирования ключевых компетентностей.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Компьютерная система (КС). Структура и компоненты КС. Классы и типы КС. Сети ЭВМ.

2. Основные понятия программно-аппаратной защиты информации: электронный документ (ЭД) и их типы; виды информации в КС; информационные потоки в КС; понятие исполняемого модуля.

3. Уязвимость компьютерных систем: понятие доступа, субъект и объект доступа; понятие несанкционированного доступа (НСД); классы и виды НСД; несанкционированное копирование программ как особый вид НСД; понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

.

Практическое занятие 3. Программно-аппаратные средства шифрования

Образовательные технологии: технология развивающего обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Построение программно-аппаратных комплексов шифрования: аппаратные и программно-аппаратные средства криптозащиты данных; построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.

2. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.

3. Необходимые и достаточные функции аппаратного средства криптозащиты, проектирование модулей криптопреобразований на основе сигнальных процессоров.

Плата Криптон-3 (Криптон-4): архитектура платы; организация интерфейса с приложениями. 5. Другие программно-аппаратные СКЗД.

Практическое занятие 4. Средства и методы ограничения доступа к файлам.

Образовательные технологии: технология проблемного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Основные подходы к защите данных от НСД: шифрование; контроль доступа; разграничения доступа; файл как объект доступа; оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости.

2. Организация доступа к файлам: иерархический доступ к файлам; понятие атрибутов доступа; организация доступа к файлам в различных ОС; защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, NovellNetWare и т. д.

3. Фиксация доступа к файлам: способы фиксации фактов доступа; журналы доступа; критерии информативности журналов доступа; выявление следов несанкционированного доступа к файлам; метод инициированного НСД.

4. Доступ к данным со стороны процесса: понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя; понятие и примеры скрытого доступа; надежность систем ограничения доступа.

5. Особенности защиты данных от изменения: зашита массивов информации от изменения (имитозащита); криптографическая постановка защиты от изменения данных; подходы к решению задачи защиты данных от изменения; подход на основе формирования имитовставки (MAC), способы построения MAC; подход на основе формирования хэш-функции, требования к построению и способы реализации; формирование электронной цифровой подписи (ЭЦП); особенности защиты ЭД и исполняемых файлов; проблема самоконтроля исполняемых модулей.

Практическое занятие 5. Защита программ от изучения

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Изучение и обратное проектирование ПО: понятие изучения и обратного проектирования ПО; цели и задачи изучения работы ПО; способы изучения ПО: статическое и динамическое изучение; роль программной и аппаратной среды; временная надежность (невозможность обеспечения гарантированной надежности).

2. Задачи защиты от изучения и способы их решения: защита от отладки; динамическое преобразование кода; итеративный программный замок А. Долгина; принцип ловушек и избыточного кода; защита от дизассемблирования; принцип внешней загрузки файлов; динамическая модификация программы; защита от трассировки по прерываниям.

3. Аспекты проблемы защиты от исследования: способы ассоциирования защиты и программного обеспечения; оценка надежности защиты от отладки.

4. Вирусы: защита от разрушающих программных воздействий; вирусы как особый класс разрушающих программных воздействий; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

Практическое занятие 6. Защита программ от несанкционированного копирования

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Несанкционированное копирование программ: несанкционированное копирование программ как тип НСД; юридические аспекты несанкционированного копирования программ; общее понятие защиты от копирования. Разновидности задач защиты от копирования.

Подходы к задаче защиты от копирования: привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО; привязка программ к гибким магнитным дискам (ГМД); структура данных на ГМД; управление контроллером ГМД; способы создания некопируемых меток; точное измерение характеристик форматирования дорожки; технология «слабых битов»; физические метки и технология работы с ними; привязка программ к жестким магнитным дискам (ЖМД); особенности привязки к ЖМД; виды меток на ЖМД; привязка к прочим компонентам штатного оборудования ПЭВМ; привязка к внешним (добавляемым) элементам ПЭВМ; привязка к портовым ключам; использование дополнительных плат расширения; методы «водяных знаков» и методы «отпечатков пальцев».

Практическое занятие 7. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения.

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trustedcomputingbase-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Практическое занятие 8. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации

3. Указания по проведению лабораторного практикума

Не предусмотрен учебным планом.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области защиты информационных процессов;

2) привить навыки самостоятельного решения задач в области создания безопасной среды функционирования предприятия.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	Очная форма обучения/заочная форма обучения
	Всего академических часов
Всего часов на самостоятельную работу	**76/92**
Вопросы, выносимые на самостоятельное изучение	30/32
Подготовка к практическим занятиям	18/24
Подготовка докладов	18/24
Выполнение практических заданий	10/12

Вопросы, выносимые на самостоятельное изучение:

1. Задача стандартизации при разработке систем защиты информации.
2. Правовая основа защиты информации на объектах информатизации.
3. Криптографические методы защиты информации в современных информационных системах.
4. Компьютерные вирусы и проблемы антивирусной защиты.
5. Организация защиты при обмене данными в информационных системах.
6. Протоколы, применяемые для защиты информации в сетевых информационных системах.
7. Проблемы обеспечения информационной безопасности беспроводных информационных систем.
8. Общая методология выбора средств и способов защиты информации в информационных системах.
9. Организация парольной защиты в информационных системах.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	30/32	Изучение открытых источников
2.	Подготовка к практическим занятиям	12/12	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Тематика докладов	10/10	1. Виды атак на сетевые информационные системы и методы борьбы с ними. 2. Скорость передачи информации дискретных каналов с помехами. 3. Современные системы электронного документооборота и показатели их защищённости. 4. Информационная безопасность электронного бизнеса.
4.	Выполнение практических заданий	8/8	1. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых

			информационных системах. 2. Методы оценки эффективности функционирования современных информационных систем. 3. Перспективные информационные системы, технологии управления и обеспечение их безопасности. 4. Методы разграничения доступа в информационных системах.

Примерные темы докладов

1. Виды атак на сетевые информационные системы и методы борьбы с ними.
2. Скорость передачи информации дискретных каналов с помехами.
3. Современные системы электронного документооборота и показатели их защищённости.
4. Информационная безопасность электронного бизнеса.
5. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах.
6. Методы оценки эффективности функционирования современных информационных систем.
7. Перспективные информационные системы, технологии управления и обеспечение их безопасности.
8. Методы разграничения доступа в информационных системах.
9. Интегрированные и корпоративные информационные системы, проблемы их защищённости.
10. Статистические критерии обнаружения и распознавания информации.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс анализа заданной электрической цепи и должна содержать промежуточные и окончательные результаты расчетов, а также соответствующие временные или частотные диаграммы, поясняющие работу электрической цепи.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт TimesNewRoman,кегль 14).

6. Указания по проведению курсовых работ

Курсовая работа по дисциплине не предусмотрена.

7. Перечень основной и дополнительной учебной литературы

Основная литература:

4. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 04.10.2022). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

5. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. URL: https://urait.ru/bcode/451231

6. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов / В.Г. Проскурин. – Москва : Горячая линия – Телеком, 2014. – 192 с. : ил. – URL: https://biblioclub.ru/index.php?page=book&id=275128

Дополнительная литература:

1.Балдин, К. В. Информационные системы в экономике : учебник / К. В. Балдин, В. Б. Уткин. – 9-е изд., стер. – Москва : Дашков и К°, 2021. – 395 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=684194 (дата обращения: 04.10.2022). – Библиогр. в кн. – ISBN 978-5-394-04038-2. – Текст : электронный.

2. Информатика и математика : учебник и практикум для вузов / Т. М. Беляева [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 402 с. — URL: https://urait.ru/bcode/451169

Рекомендуемая литература:

1. Васильков А.В. Информационные системы и их безопасность. Учебное пособие, М.: «Форум», 2010.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М.: «Форум»-Инфра-М. 2008.

Электронные книги:

1. Иванов М.А., Чугунов И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.
http://biblioclub.ru/index.php?page=book_view&book_id=231673
2. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие.М.: ИНТУИТ,2006
http://www.intuit.ru/goods_store/ebooks/8172
3. Д.С. Кулябов Защита информации в сетях. Уч. пос.ч.1.2004.
http://telesys.pfu.edu.ru/sites/telesys.pfu.edu.ru/files/imported/studies/book/net-sec-p1.pdf
4. Международные стандарты по оценке безопасности информационных технологий. Гармонизированные критерии Европейских стран ITSEC.
http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/
5. Андрианов В.В. Обеспечение информационной безопасности бизнеса. 2-е издание, переработанное и дополненное. 2011
http://fanread.ru/book/8496757/?page=1
6. Блинов А.М. Информационная безопасность: Учебное пособие. Часть1.-СПб.:Изд-во СПГУЭФ,2010.
http://elibrary.unecon.ru/materials_files/341423666.pdf
7. Скотт Бармен. Разработка правил информационной безопасности. Учебное пособие: Изд-во: Вильямс. 2002
http://bookimir.ru/loads/kompyuteryiinternet/aznoe37/501266-razrabotka-pravil-informacionnoy-bezopasnosti-skott-barmen.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp –** научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации

8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Перечень информационных технологий

Перечень программного обеспечения: MSOffice.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды «МГОТУ».
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационная безопасность операционных систем и баз данных».
3. Информационно – справочные (правовые) системы: «Гарант»; «Кодекс»; «Консультант +».