МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защищенные центры обработки данных

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины «Защищенные центры обработки данных» является приобретение учащимися навыков и знаний в области аппаратных средств хранения и обработки данных; концепций архитектуры серверной системы; методов локального хранения данных; структуры сетей и систем хранения данных; структуры и обеспечения защиты информации в центрах обработки данных (ЦОД).

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

- Сбор и анализ исходных данных для расчета и проектирования баз данных и систем управления базами данных;

- Разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам;

- контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

Организационно-управленческая деятельность

- Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;

- Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;

- Организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.

Проектная деятельность:

- Составление инструкций по эксплуатации систем управления базами данных и средств обеспечения их информационной безопасности;

- Обеспечение эффективного функционирования систем управления базами данных и средств обеспечения их информационной безопасности;

- Администрирование подсистем информационной безопасности компьютерных систем.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-7 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

-особенности аппаратных средств хранения и обработки данных;

-архитектурные концепции серверной системы;

-основные методы локального хранения данных;

-структуру сетей и систем хранения данных;

-структуру и методы обеспечения защиты информации в центрах обработки данных (ЦОД).

Владеть:

-методами проектирования предметной области в модели «сущность-связь» и структуры базы данных в реляционной СУБД;

- технологией разработки приложений на языке высокого уровня, использующих для хранения информации базу данных.

Уметь:

-организовывать работы по созданию и совершенствованию структуры ЦОД;

-применять современные методы локального хранения данных;

-применять эффективные методы обеспечения целостности и доступности данных в СХД;

-применять эффективные методы обеспечения целостности и доступности данных в СХД.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №10
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 100 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Архитектура современных ЦОД. Основные элементы и зоны Содержание учебного материала: — Классификация ЦОД по надежности (Tier I—IV) — Основные подсистемы: ИТ-оборудование, электропитание, охлаждение, СКС — Зонирование ЦОД: серверная, сетевая, хранения данных, резервного копирования — Понятие DMZ (демилитаризованная зона) в ЦОД — Принципы построения защищенного периметра ЦОД
2	Модели угроз и нарушителя для защищенного ЦОД Содержание учебного материала: — Типы нарушителей: внутренний (администратор, инженер, уборщик), внешний (хакер, конкурент) — Основные угрозы: несанкционированный доступ, утечка данных, отказ оборудования, атаки на инфраструктуру — Анализ рисков для ЦОД: методологии (FMEA, CORAS) — Примеры реальных инцидентов в ЦОД — Разработка частной модели угроз для конкретного ЦОД

№ п/п	Тематика лекционных занятий / краткое содержание
3	Физическая защита периметра ЦОД Содержание учебного материала: — Проектирование внешнего периметра: ограждения, КПП, системы контроля доступа на территорию — Противопожарные разрывы и зоны эвакуации — Защита от транспортных средств (болларды, противотаранные устройства) — Системы охранного освещения и видеонаблюдения (CCTV) на периметре — Интеграция физической защиты с системами управления ЦОД (DCIM)
4	Системы контроля доступа (СКУД) в ЦОД Содержание учебного материала: — Идентификация и аутентификация персонала (пропуска, биометрия) — Двухфакторная аутентификация для доступа в серверные залы — Управление зонами доступа: гранулярность прав (помещение, стойка, сервер) — Электронные замки, турникеты, тамбуры-шлюзы (мантрапы) — Журналирование и аудит событий доступа
5	Системы видеонаблюдения и охранной сигнализации Содержание учебного материала: — Типы камер: IP, аналоговые, тепловизионные, панорамные — Требования к разрешению и углам обзора для критических зон — Хранение видеозаписей: сроки, защита от удаления, централизованное хранилище — Детекция движения и аналитика (распознавание лиц, обнаружение оставленных предметов) — Интеграция с СКУД и системой оповещения
6	Инженерная безопасность: электропитание и кондиционирование Содержание учебного материала: — Бесперебойное электропитание (ИБП): онлайн, линейно-интерактивный, резервный — Дизель-генераторные установки (ДГУ): запуск, время переключения, запас топлива — Системы распределения электроэнергии (PDU, rPDU) с мониторингом — Микроклимат: точное кондиционирование (CRAC/CRAH), холодные/горячие коридоры — Защита от перегрева, датчики температуры и влажности в стойках
7	Противопожарная защита ЦОД Содержание учебного материала: — Раннее обнаружение пожара: аспирационные дымовые извещатели (VESDA) — Типы пожаротушения: водяное, порошковое, аэрозольное, газовое (Novec 1230, Inergen) — Преимущества и недостатки газового пожаротушения для серверного оборудования — Зонирование систем пожаротушения в ЦОД — Процедуры эвакуации персонала и отключения вентиляции
8	Сетевая безопасность ЦОД: сегментация и микросегментация Содержание учебного материала: — Традиционная сегментация с использованием VLAN и ACL — Микросегментация на основе политик (VMware NSX, Cisco ACI, Calico) — Изоляция приложений и сервисов в пределах одного сервера — Межсетевые экраны нового поколения (NGFW) на границах сегментов — Сравнение подходов: физическая, виртуальная и программно-определяемая сегментация

№ п/п	Тематика лекционных занятий / краткое содержание
9	Защита от DDoS-атак на уровне ЦОД Содержание учебного материала: — Типы DDoS-атак: сетевой уровень (SYN flood, UDP flood), прикладной (HTTP slowloris) — Обнаружение аномалий трафика (NetFlow, sFlow, IPFIX) — Очистка трафика (scrubbing) on-premise и cloud-based (например, Cloudflare, Qrator) — Емкостное резервирование каналов связи ЦОД — Автоматическое реагирование: blackholing, rate limiting, капчи
10	Отказоустойчивость и резервирование в ЗЦОД Содержание учебного материала: — Концепции N, N+1, 2N, 2(N+1) для разных подсистем — Резервирование сетевых коммутаторов (stack, VPC, MLAG) — Резервирование каналов связи (BGP multihoming, Link Aggregation) — Кластеризация серверов и систем хранения данных — Планы непрерывности бизнеса (BCP) и восстановления после сбоев (DRP)
11	Географически распределенные ЦОД. Синхронизация и репликация Содержание учебного материала: — Активный-активный, активный-пассивный, активный-резервный режимы — Синхронная и асинхронная репликация данных — Split-brain проблема и механизмы её предотвращения (Quorum, Witness) — Защищенные каналы связи между ЦОД (MACsec, IPsec) — Оркестрация переключения трафика (GSLB, Anycast, DNS failover)
12	Защита систем хранения данных (СХД) в ЦОД Содержание учебного материала: — Шифрование на уровне диска, массива (SED) и на уровне СХД — Контроль доступа к LUN и томам (RBAC на СХД) — Аудит действий администраторов СХД — Защита от атак на протоколы: iSCSI (CHAP), FC (zoning, masking) — Обнаружение аномалий в работе СХД (аномальный доступ, утечки через snapshots)
13	Виртуализация как угроза и средство защиты в ЦОД Содержание учебного материала: — Риски гипервизора: VM escape, атаки на management plane (vCenter, Proxmox) — Изоляция виртуальных машин: VLAN, VXLAN, NSX, сегментация трафика VMs — Защита управляющей сети гипервизора — Шифрование виртуальных машин (в состоянии покоя и в памяти) — Обнаружение rootkit в гостевых ОС из домена гипервизора (встроенный антивирус)
14	Безопасность облачных и гибридных ЦОД Содержание учебного материала: — Модели ответственности (Shared Responsibility Model) для IaaS, PaaS, SaaS — Защита API управления облачным ЦОД — Перенос данных между on-premise и облаком: шифрование, VPN, Direct Connect — Управление идентификацией (IDaaS, федерация удостоверений) — Аудит конфигураций облачных ресурсов (CSPM)
15	SIEM и SOC для защищенного ЦОД

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: — Сбор и нормализация событий: логов серверов, сетевого оборудования, СКУД, видеонаблюдения — Правила корреляции для обнаружения аномалий в ЦОД — Использование UEBA для выявления внутренних нарушителей — Реагирование на инциденты (SOAR) в инфраструктуре ЦОД — Метрики эффективности SOC (MTTD, MTTR)
16	Защита от внутренних нарушителей в ЦОД Содержание учебного материала: — Модели угроз от администраторов, дата-центр инженеров, подрядчиков — Принцип наименьших привилегий (PoLP) для всех категорий персонала — Разделение административных ролей: сеть, СХД, гипервизор, СКУД — Двухглазое правило (два администратора для критических действий) — Мониторинг сессий администраторов (session recording, jump servers)

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Определение назначения ЦОД В результате выполнения лабораторной работы студент получит навыки классификации ЦОД по уровням надежности (Tier I—IV) и назначению (корпоративный, коммерческий, облачный, государственный), формирования технического задания на проектирование ЗЦОД с учетом требований заказчика и отраслевой специфики, а также навыки составления научно-технического отчета по результатам анализа.
2	Идентификация активов ЦОД и построение модели угроз. В результате выполнения лабораторной работы студент получит навыки инвентаризации информационных и физических активов защищенного ЦОД (серверы, СХД, сетевое оборудование, системы охлаждения, СКУД), идентификации угроз для каждого актива с использованием методологий (FMEA, STRIDE), построения модели нарушителя (внутренний, внешний, случайный), а также оформления раздела «Модель угроз» в проектной документации.
3	Разработка политики физической безопасности ЦОД. В результате выполнения лабораторной работы студент получит навыки проектирования периметральной защиты ЦОД (выбор типа ограждения, КПП, зон досмотра), определения уровней доступа в зоны (серверная, сетевая, административная, инженерная), составления политики контроля доступа персонала и посетителей, а также расчета необходимого количества постов охраны и точек видеонаблюдения.
4	Проектирование системы контроля доступа (СКУД) для серверной. В результате выполнения лабораторной работы студент получит навыки выбора типа идентификаторов (пропуски, PIN-код, биометрия) для разных категорий персонала ЦОД, настройки прав доступа на уровне дверей, стоек и отдельных серверов (IP-контроллеры, считыватели на стойках), проектирования мантрапа (тамбур-шлюза) для входа в серверный зал, а также настройки аудита событий доступа в реальном времени.

№ п/п	Наименование лабораторных работ / краткое содержание
5	Настройка системы видеонаблюдения (CCTV) для критических зон ЦОД. В результате выполнения лабораторной работы студент получит навыки размещения камер видеонаблюдения в серверной, зоне ввода кабелей, помещении с ИБП и административной зоне с учетом углов обзора и освещенности, выбора параметров записи (разрешение, частота кадров, срок хранения), настройки детекции движения и аналитики (распознавание лиц, обнаружение оставленных предметов), а также интеграции видеонаблюдения с СКУД для привязки событий доступа к видеоряду.
6	Расчет системы бесперебойного электропитания и резервирования. В результате выполнения лабораторной работы студент получит навыки расчета потребляемой мощности серверного оборудования (по паспортным данным или замерам), выбора ИБП с топологией онлайн (double conversion) для обеспечения защиты от провалов напряжения, проектирования резервного питания от ДГУ с учетом времени запуска и емкости топливного бака, расчета уровней резервирования (N+1, 2N, 2(N+1)) для разных категорий нагрузок, а также настройки мониторинга электропитания через rPDU.
7	Проектирование системы охлаждения и мониторинга микроклимата. В результате выполнения лабораторной работы студент получит навыки расчета тепловыделения серверного оборудования, выбора схемы охлаждения (холодные/горячие коридоры, контейнеризация), размещения датчиков температуры и влажности на уровне стоек, настройки системы прецизионного кондиционирования (CRAC/CRAH) с резервированием, а также настройки порогов срабатывания аварийной сигнализации при превышении температуры.
8	Настройка системы газового пожаротушения и аспирационного дымообнаружения. В результате выполнения лабораторной работы студент получит навыки выбора типа огнетушащего вещества (Novec 1230, Inergen, аргон) для серверной с дорогостоящим оборудованием, проектирования зон пожаротушения и расчета необходимого объема газа, настройки аспирационных дымовых извещателей (VESDA) с разными уровнями чувствительности (Alert, Action, Fire), составления процедуры эвакуации персонала и отключения вентиляции, а также проведения тестового запуска системы (моделирование без подачи газа).
9	Сегментация сети ЦОД с использованием VLAN и микросегментации. В результате выполнения лабораторной работы студент получит навыки проектирования сетевой топологии ЦОД с выделением DMZ, внутренней серверной сети, сети управления и сети резервного копирования, настройки VLAN на коммутаторах уровня распределения, создания политик микросегментации с помощью программно-определяемой сети (например, VMware NSX или Cisco ACI) для изоляции отдельных приложений, а также проверки проходимости трафика между сегментами с помощью сканера портов.
10	Настройка IDS/IPS для обнаружения атак внутри ЦОД. В результате выполнения лабораторной работы студент получит навыки размещения сенсоров IDS (например, Snort или Suricata) на зеркальных портах коммутаторов в ключевых точках ЦОД (на границе сегментов, перед СХД), написания сигнатур для обнаружения горизонтального перемещения (например, сканирование портов между виртуальными машинами), настройки автоматической изоляции скомпрометированного сервера (через API коммутатора), а также анализа ложных срабатываний в высоконагруженной среде.
11	Резервное копирование и восстановление в географически распределенном ЦОД. В результате выполнения лабораторной работы студент получит навыки выбора схемы резервного

№ п/п	Наименование лабораторных работ / краткое содержание
	копирования (полное, дифференциальное, инкрементное) для критических баз данных ЦОД, настройки синхронной и асинхронной репликации между основным и резервным ЦОД (например, через DRBD или NetApp SnapMirror), тестирования процедуры восстановления (failover/failback) без остановки бизнес-процессов, а также расчета целевых показателей RPO и RTO для разных классов данных.
12	Шифрование данных на дисках и в системах хранения (СХД) ЦОД В результате выполнения лабораторной работы студент получит навыки включения аппаратного шифрования на SSD с интерфейсом SED (Self-Encrypting Drive), настройки шифрования томов на уровне СХД (например, с использованием AES-256), развертывания сервера управления ключами (KMIP) для централизованной ротации ключей, проведения атаки на извлечение диска из работающей системы (моделирование кражи физического диска), а также аудита событий доступа к зашифрованным томам.
13	Настройка системы обнаружения внутренних нарушителей (UEBA) в ЦОД. В результате выполнения лабораторной работы студент получит навыки сбора поведенческих метрик администраторов ЦОД (время входа, типичные команды, объем выгруженных данных), настройки профилей нормального поведения для каждой роли (администратор СХД, сетевой инженер, инженер гипервизора), выявления аномалий (например, вход в 3 часа ночи или копирование конфигурации коммутатора), а также настройки автоматической блокировки сессии при превышении порога риска.
14	Аудит соответствия ЗЦОД требованиям PCI DSS (для обработки платежных данных) В результате выполнения лабораторной работы студент получит навыки проверки выполнения контрольных пунктов PCI DSS, относящихся к физической безопасности ЦОД (требования 9), защите сетевой инфраструктуры (требование 1), шифрованию данных карт (требование 3), мониторингу доступа (требование 10), составления отчета о несоответствиях с приоритизацией по критичности, а также разработки плана корректирующих мероприятий с указанием сроков.
15	Разработка плана непрерывности бизнеса (BCP) и восстановления (DRP) для ЦОД. В результате выполнения лабораторной работы студент получит навыки проведения анализа воздействия на бизнес (BIA) для определения критических сервисов ЦОД, составления процедур переключения на резервный ЦОД (ручное, полуавтоматическое, автоматическое), документирования ролей и ответственности в аварийной комиссии, проведения командно-штабного учения (таблиленое моделирование) по сценарию отказа электропитания, а также расчета финансовых потерь от простоя ЦОД.
16	Интеграция SIEM для централизованного мониторинга безопасности ЦОД. В результате выполнения лабораторной работы студент получит навыки подключения к SIEM-системе (например, ELK Stack, Splunk или MaxPatrol) источников событий: логов СКУД, видеорегистраторов (поиск событий в записях), ИБП, систем охлаждения, сетевого оборудования и гипервизора, написания правил корреляции (например, «открытие двери серверной + отсутствие карты доступа + движение в CCTV»), создания дашборда для мониторинга состояния защищенности ЦОД в реальном времени, а также настройки автоматического создания тикета в Service Desk при обнаружении инцидента.
17	Проектирование серверной комнаты и расчет энергоэффективности (PUE) Цель: Научиться рассчитывать потребности ЦОД в электроэнергии и охлаждении, а также

№ п/п	Наименование лабораторных работ / краткое содержание
	оптимизировать коэффициент PUE (Power Usage Effectiveness). Задание: Студентам выдается вводная по количеству серверов, их тепловыделению и типу стоек. Необходимо рассчитать требуемую мощность кондиционеров, спроектировать «холодные/горячие» коридоры и предложить меры по снижению PUE (например, использование фрикулинга или жидкостного охлаждения).
18	Построение сетевой архитектуры Data Center Fabric (Leaf-Spine) Цель: Понять разницу между классической трехуровневой сетью и современной архитектурой Leaf-Spine, используемой в ЦОД. Задание: Спроектировать сеть топологии Leaf-Spine. Настроить протоколы маршрутизации (BGP EVPN или OSPF/ECMP) для обеспечения равноценных путей (Multipath) и отсутствия петель. Проверить сходимость сети при обрыве линка между коммутаторами.
19	Автоматизация инфраструктуры ЦОД (Infrastructure as Code) Цель: Научиться управлять конфигурациями сотен серверов без ручного вмешательства. Задание: Написать плейбуки (playbooks) или скрипты для автоматического развертывания и настройки узлов ЦОД. Например, автоматическая установка гипервизора, настройка сетевых интерфейсов, подключение к домену и установка агентов мониторинга.
20	Развертывание и администрирование кластера Kubernetes Цель: Освоить современные подходы к оркестрации контейнеров, которые стали стандартом для современных ЦОД. Задание: Развернуть кластер Kubernetes (например, с помощью kubeadm или k3s). Настроить Ingress-контроллер, развернуть отказоустойчивое веб-приложение, состоящее из нескольких микросервисов, и настроить автомасштабирование (HPA) в зависимости от нагрузки.
21	Настройка комплексного мониторинга и DCIM-системы Цель: Научиться собирать телеметрию как с программного, так и с физического уровня оборудования. Задание: Развернуть стек мониторинга. Настроить сбор метрик с виртуальных машин (CPU, RAM, Disk I/O) и с физического оборудования по протоколу SNMP/IPMI (температура в стойках, энергопотребление, статус блоков питания). Создать дашборды и настроить алерты.
22	Организация резервного копирования и аварийного восстановления (DR) Цель: Изучить стратегии обеспечения непрерывности бизнеса (RTO и RPO). Задание: Настроить систему резервного копирования (например, Veeam Backup & Replication или Proxmox Backup Server). Создать задания для инкрементальных и полных бэкапов. Отработать сценарий Instant VM Recovery (мгновенного поднятия ВМ напрямую с бэкапа) и репликации ВМ на удаленную площадку.
23	Внедрение микросегментации сети для безопасности рабочих нагрузок Цель: Освоить принципы Zero Trust и защиты от lateral movement (перемещения злоумышленника внутри ЦОД). Задание: Настроить распределенный межсетевой экран (Distributed Firewall). Создать правила, которые запрещают прямой доступ между виртуальными машинами в разных контурах безопасности, даже если они находятся в одной физической стойке или на одном гипервизоре. Разрешить трафик только по принципу "необходимо и достаточно" (например, только порт 80/443 от балансировщика к веб-серверу).

№ п/п	Наименование лабораторных работ / краткое содержание
24	Программно-определяемые сети (SDN) и оверлейные сети (VXLAN) Цель: Изучить технологии абстрагирования сети от физической инфраструктуры. Задание: Спроектировать оверлейную сеть VXLAN, позволяющую растягивать L2-домены (VLAN) поверх L3-инфраструктуры ЦОД. Подключить виртуальные машины из разных физических локаций к одной логической подсети.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Проектирование отказоустойчивого ЦОД уровня Tier III для компании
2. Оптимизация энергоэффективности (Green DC): модернизация системы охлаждения для снижения PUE
3. Проектирование сети периферийных вычислений (Edge Computing) и микро-ЦОД для распределенной филиальной сети
4. Разработка архитектуры частного облака (IaaS) на базе гиперконвергентной инфраструктуры (HCI)
5. Проектирование высокопроизводительного вычислительного кластера (HPC/GPU) для задач машинного обучения и ИИ
6. Разработка корпоративной платформы контейнеризации (PaaS) на базе Kubernetes
7. Проектирование гибридного облака: интеграция локального ЦОД с публичными облачными провайдерами
8. Модернизация сетевой инфраструктуры ЦОД: переход на архитектуру Leaf-Spine с применением SDN
9. Проектирование высокопроизводительной сети хранения данных (SAN)
10. Проектирование системы резервного копирования и долговременного архивирования данных
11. Разработка архитектуры безопасности ЦОД на основе концепции Zero Trust и микросегментации

12. Внедрение системы управления инфраструктурой ЦОД (DCIM) для автоматизации мониторинга и управления ресурсами

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Голдовский, Яков Михайлович. Базы данных : метод. указ. к лаб. раб. для студ. спец. "Выч. машины, комплексы, системы и сети" / Я.М. Голдовский ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2006. - 35 с. : ил.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/04-35430.pdf. Текст : непосредственный. (дата обращения 10.06.2026)
2	Голдовский, Яков Михайлович. Введение в постреляционные базы данных : учеб. пособие для студ. спец. "Информатика и вычислительная техника" по дисц. "Постреляционные базы данных" / Я.М Голдовский ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2008. - 92 с. : ил. - Библиогр.: с. 92. -	Научно-техническая библиотека МИИТ(дата обращения 10.06.2026)полочный шифр 004-Г60. Текст : непосредственный.

	84.42 р. - Текст : непосредственный	
3	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 10.06.2026)Текст : непосредственный. 004 Г60
4	Давыдовский, Михаил Альбинович. Организация базы данных и язык запросов системы ИНЕС : метод. указания к учебно-исслед. работам по дисц. "Банки данных", "Теория вычислительных систем" для студ. спец. "Прикладная математика", "Автоматизир. системы	URL:http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/04-35820.pdf(дата обращения 10.06.2026)Текст : непосредственный. Полочный шифр 681.3 -Д13

	управления" / М.А. Давыдовский, В.Г. Чернов ; МИИТ. Каф. "Электронные вычислительные машины". - М. : МИИТ, 1983. - 37 с. : ил.. - Б. ц.	
5	Отладка программ в системе Турбо-Паскаль : метод. указания к практическим, лабораторным и учебно-исследовательским работам / МИИТ. Каф. "Математическое обеспечение автоматизированных систем управления" ; Сост.: М.А. Давыдовский, Ф.Б. Поволоцкий. - М. : МИИТ, 1990. - 32 с.- Б. ц. - Текст : непосредственный.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/01-51151.pdf. (дата обращения 10.06.2026) Полочный шифр 681.3 - Д13
6	Обучающиеся системы обработки информации и принятия решений: непараметрический подход : монография / А.В.Лапко, С.В.Ченцов, С.И.Крохов, Л.А.Фельдман ; Под ред. А.М.Федотова. - Новосибирск : Наука, Сибирск. изд. фирма РАН,	Научно-техническая библиотека МИИТ(дата обращения 10.06.2026)полочный шифр 519-О26. Текст : непосредственный.

	1996. - 296 с. - Библиогр.: 153 назв. - ISBN 5-02-030699-1 (в пер.) : 9000 р. - Текст : непосредственный.	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Современные профессиональные базы данных и информационные справочные системы не требуются.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Windows

Microsoft Office

Бесплатное использование (GNU LGPL FAR manager. Бесплатное использование (BSD)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуются:

• Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

• Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

• Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения лабораторных работ:

• компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

• В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 10 семестре.
Курсовая работа в 10 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова