МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защищенные центры обработки данных

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

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).

Основными задачами дисциплины являются:

- Разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам;
- Сбор и анализ исходных данных для расчета и проектирования баз данных и систем управления базами данных;
- Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- Составление инструкций по эксплуатации систем управления базами данных и средств обеспечения их информационной безопасности;
- Администрирование подсистем информационной безопасности компьютерных систем;
- Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

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).

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;

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.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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 №1
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 168 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 защищенного ЦОД. Классификация и принципы построения Содержание учебного материала: — Определение защищенного центра обработки данных (ЗЦОД), отличие от обычного ЦОД — Классификация ЦОД по уровням надежности (Tier I–IV) и требованиям безопасности — Основные функциональные зоны ЗЦОД: серверная, сетевая, хранения данных, резервного копирования, административная, инженерная, зона досмотра — Принципы построения защищенного периметра: многоуровневая физическая защита — Требования к расположению ЗЦОД (удаленность от промышленных объектов, транспортных магистралей, водных преград)
2	Модель угроз и нарушителя для защищенного ЦОД Содержание учебного материала: — Классификация угроз информационной безопасности для ЦОД (физические, технические, человеческие, природные) — Типы нарушителей: внешний (хакер, конкурент, террорист), внутренний (администратор, инженер, уборщик, охрана) — Моделирование сценариев атак на ЗЦОД (несанкционированный доступ, утечка данных, вывод оборудования из строя) — Анализ рисков: методы оценки вероятности и ущерба — Разработка частной модели угроз для конкретного ЗЦОД
3	Физическая защита периметра и системы контроля доступа (СКУД) Содержание учебного материала: — Проектирование внешнего периметра: ограждения, КПП, контрольно-пропускной режим, противотаранные устройства — Системы контроля доступа: типы идентификаторов (пропуска, PIN-код, биометрия), считыватели, контроллеры — Организация зон доступа: разграничение прав для разных категорий персонала — Тамбур-шлюзы (мантрапы) для входа в серверные залы: принцип работы, требования — Журналирование и аудит событий доступа, интеграция СКУД с системой видеонаблюдения
4	Системы видеонаблюдения, охранной сигнализации и обнаружения вторжений Содержание учебного материала: — Типы камер видеонаблюдения (IP, аналоговые, тепловизионные, панорамные) и требования к их размещению

№ п/п	Тематика лекционных занятий / краткое содержание
	— Хранение видеозаписей: сроки, защита от удаления, централизованное хранилище — Видеоаналитика: распознавание лиц, детекция движения, обнаружение оставленных предметов — Охранная сигнализация: датчики открытия дверей, разбития стекла, движения, вибрации — Интеграция систем видеонаблюдения и сигнализации с СКУД и системой оповещения
5	Инженерная безопасность ЗЦОД: электропитание, охлаждение, мониторинг среды Содержание учебного материала: — Системы бесперебойного электропитания (ИБП): топологии (offline, line-interactive, online double conversion), резервирование — Дизель-генераторные установки (ДГУ): запуск, время переключения, запас топлива, требования к размещению — Системы распределения электроэнергии (PDU, rPDU) с мониторингом потребления — Системы охлаждения: прецизионные кондиционеры (CRAC/CRAH), холодные и горячие коридоры, контейнеризация — Мониторинг микроклимата: датчики температуры, влажности, перепада давления на уровне стоек и залов
6	Противопожарная защита защищенного ЦОД Содержание учебного материала: — Раннее обнаружение пожара: аспирационные дымовые извещатели (VESDA), пороги чувствительности (Alert, Action, Fire) — Типы систем пожаротушения: водяное (спринклерное), порошковое, аэрозольное, газовое — Газовое пожаротушение: огнетушащие вещества (Novec 1230, Inergen, аргон, CO?), преимущества и недостатки для серверного оборудования — Зонирование системы пожаротушения в ЦОД, расчет объема газа — Процедуры эвакуации персонала, отключения вентиляции, автоматический и ручной пуск
7	Сетевая безопасность ЗЦОД: сегментация, микросегментация и защита от DDoS Содержание учебного материала: — Сетевая топология ЗЦОД: выделение зон (DMZ, внутренняя серверная, управления, резервного копирования, мониторинга) — Традиционная сегментация с использованием VLAN и ACL — Микросегментация на основе политик (VMware NSX, Cisco ACI, Calico): изоляция отдельных приложений и сервисов — Межсетевые экраны нового поколения (NGFW) на границах сегментов — Защита от DDoS-атак: обнаружение аномалий трафика (NetFlow, sFlow), очистка (scrubbing), blackholing, rate limiting
8	Безопасность систем хранения данных и резервное копирование в ЗЦОД Содержание учебного материала: — Классификация систем хранения данных (СХД): DAS, NAS, SAN, объектные СХД — Шифрование данных на дисках (SED), на уровне массивов и на уровне СХД — Контроль доступа к LUN и томам: RBAC на СХД, аудит действий администраторов — Защита протоколов доступа: iSCSI (CHAP), Fibre Channel (zoning, masking) — Резервное копирование и репликация: схемы (полное, дифференциальное, инкрементное), синхронная и асинхронная репликация между ЦОД — Планы непрерывности бизнеса (BCP) и восстановления после сбоев (DRP): RPO, RTO, процедуры переключения (failover/failback)

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Классификация ЦОД по уровням надежности (Tier) и формирование ТЗ на проектирование В результате выполнения лабораторной работы студент получит навыки анализа требований заказчика (доступность 99,741%, 99,982% и т.д.) и выбора соответствующего уровня Tier (I—IV), составления технического задания на проектирование ЗЦОД с указанием требований к электропитанию, охлаждению, резервированию каналов, а также оформления научно-технического отчета с обоснованием выбора Tier.
2	Идентификация активов ЗЦОД и построение модели угроз В результате выполнения лабораторной работы студент получит навыки инвентаризации физических и информационных активов ЦОД (серверы, СХД, сетевое оборудование, системы охлаждения, ИБП, СКУД), идентификации угроз для каждого актива с использованием методологии STRIDE, построения модели нарушителя (внешний, внутренний — администратор, инженер, уборщик), а также оформления раздела «Модель угроз» в проектной документации ЗЦОД.
3	Проектирование периметральной физической защиты ЗЦОД В результате выполнения лабораторной работы студент получит навыки разработки схемы внешнего периметра ЦОД (выбор типа ограждения, расположение КПП, противотаранных устройств, зон досмотра), определения количества постов охраны и маршрутов патрулирования, расчета необходимого количества камер видеонаблюдения на периметре (с учетом углов обзора и зон перекрытия), а также составления спецификации оборудования периметральной защиты.
4	Настройка системы контроля доступа (СКУД) для серверной зоны Настройка системы контроля доступа (СКУД) для серверной зоны В результате выполнения лабораторной работы студент получит навыки выбора типа идентификаторов (EM-Marine, Mifare, биометрия) для разных категорий персонала (администраторы, инженеры, подрядчики), настройки прав доступа на уровне дверей, стоек и отдельных серверов (IP-контроллеры, считыватели на стойках), проектирования мантрапа (тамбур-шлюза) с весовым контролем, а также настройки журналирования событий доступа в реальном времени.
5	Настройка системы видеонаблюдения (CCTV) для критических зон ЦОД В результате выполнения лабораторной работы студент получит навыки размещения IP-камер в серверной, зоне ввода кабелей, помещении с ИБП и административной зоне с учетом освещенности и углов обзора, выбора параметров записи (разрешение от 1080p, частота 25 fps, срок хранения от 30 суток), 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 (ИБП) и ДГУ для ЗЦОД В результате выполнения лабораторной работы студент получит навыки расчета суммарной потребляемой мощности серверного оборудования (по паспортным данным или с помощью ваттметра), выбора ИБП с топологией онлайн (double conversion) для обеспечения защиты от провалов и импульсных помех, проектирования резервного питания от дизель-генераторной установки (ДГУ) с учетом времени запуска (не более 15 секунд) и емкости топливного бака (на 24 часа), расчета уровней резервирования (N+1, 2N, 2(N+1)) для разных групп нагрузок, а также настройки мониторинга электропитания через rPDU.
7	Проектирование системы охлаждения и мониторинга микроклимата Проектирование системы охлаждения и мониторинга микроклимата

№ п/п	Наименование лабораторных работ / краткое содержание
	В результате выполнения лабораторной работы студент получит навыки расчета тепловыделения серверного оборудования (в кВт) на основе его паспортной мощности, выбора схемы организации воздушных потоков (холодные/горячие коридоры, контейнеризация), размещения датчиков температуры и влажности на уровне стоек (сверху, посередине, снизу), настройки системы прецизионного кондиционирования (CRAC/CRAH) с резервированием N+1, а также настройки порогов срабатывания аварийной сигнализации при превышении температуры (например, +25°C — предупреждение, +32°C — критическая авария).
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 (предпочтение газовым составам, не повреждающим электронику), проектирования зон пожаротушения и расчета необходимого объема газа (исходя из объема помещения и нормативной концентрации), настройки аспирационных дымовых извещателей (VESDA) с четырьмя уровнями чувствительности (Alert, Action, Fire), составления процедуры эвакуации персонала и отключения вентиляции, а также проведения тестового запуска системы в режиме моделирования (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 (для публичных сервисов), внутренней серверной сети (для приложений), сети управления (iLO, IPMI, контроллеры СХД) и сети резервного копирования, настройки VLAN на коммутаторах уровня распределения (например, в Cisco Packet Tracer), создания политик микросегментации с помощью программно-определяемой сети (например, VMware NSX или Cisco ACI) для изоляции отдельных приложений друг от друга, а также проверки проходимости трафика между сегментами с помощью сканера портов (nmap).
10	Настройка IDS/IPS для обнаружения атак внутри периметра ЦОД Настройка IDS/IPS для обнаружения атак внутри периметра ЦОД В результате выполнения лабораторной работы студент получит навыки размещения сенсоров IDS (Snort или Suricata) на зеркальных портах коммутаторов в ключевых точках ЦОД (на границе сегментов, перед СХД, в сети управления), написания сигнатур для обнаружения горизонтального перемещения (например, обнаружение сканирования портов между виртуальными машинами, идентификация попыток подключения к iLO/IPMI), настройки автоматической изоляции скомпрометированного сервера (через API коммутатора или интеграцию с SIEM), а также анализа ложных срабатываний в высоконагруженной среде.
11	Резервное копирование и репликация данных в географически распределенном ЦОД В результате выполнения лабораторной работы студент получит навыки выбора схемы резервного копирования (полное, дифференциальное, инкрементное) для критических баз данных ЦОД (например, PostgreSQL, Oracle), настройки синхронной и асинхронной репликации между основным и резервным ЦОД (например, через DRBD, ZFS send/receive или средства СХД NetApp SnapMirror), тестирования процедуры восстановления (failover/failback) без остановки бизнес-процессов или с минимальным простоем, 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) через настройку ATA Security, настройки шифрования томов на уровне СХД (например, для FreeNAS/ZFS включение шифрования zfs-томов с использованием AES-256-GCM), развертывания сервера управления ключами (KMIP) —

№ п/п	Наименование лабораторных работ / краткое содержание
	например, HashiCorp Vault или собственный KMIP-сервер — для централизованной ротации ключей, проведения атаки «извлечение диска из работающей системы» (моделирование кражи физического диска и попытки чтения без ключа), 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 и место входа в систему, типичные команды (bash history), IP-адреса, объемы выгруженных данных), настройки профилей нормального поведения для каждой роли (администратор СХД, сетевой инженер, инженер гипервизора), выявления аномалий (например, вход в систему в 3 часа ночи с нехарактерного IP, копирование конфигурации коммутатора, массовое чтение файлов резервных копий), а также настройки автоматической блокировки сессии (или отправки предупреждения в SOC) при превышении порога риска.
14	Аудит соответствия ЗЦОД требованиям PCI DSS (для обработки данных платежных карт) В результате выполнения лабораторной работы студент получит навыки проверки выполнения контрольных пунктов стандарта PCI DSS версии 3.2.1 или 4.0, относящихся к физической безопасности ЦОД (требование 9 — ограничение физического доступа, видеонаблюдение, реестр посетителей), защите сетевой инфраструктуры (требование 1 — установка межсетевых экранов между зонами), шифрованию данных карт при передаче и хранении (требование 3 и 4), мониторингу доступа (требование 10 — сбор и анализ логов), составления отчета о несоответствиях с приоритизацией по критичности (High, Medium, Low), а также разработки плана корректирующих мероприятий с указанием сроков устранения и ответственных.
15	Разработка плана непрерывности бизнеса (BCP) и восстановления (DRP) для ЦОД В результате выполнения лабораторной работы студент получит навыки проведения анализа воздействия на бизнес (Business Impact Analysis, BIA) для определения критических сервисов ЦОД и их максимально допустимого времени простоя (MTPD), составления процедур переключения на резервный ЦОД (ручное переключение, полуавтоматическое, полностью автоматическое), документирования ролей и ответственности в аварийной комиссии (RACI-матрица), проведения командно-штабного учения (таблиленое моделирование) по сценарию отказа электропитания основного ЦОД с заполнением чек-листов, а также расчета финансовых потерь от простоя ЦОД на основе заданной стоимости часа простоя.
16	Интеграция SIEM для централизованного мониторинга безопасности ЗЦОД В результате выполнения лабораторной работы студент получит навыки подключения к SIEM-системе (например, ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, MaxPatrol SIEM или Wazuh) следующих источников событий: логов СКУД (события входа/выхода, отказ доступа), видеорегистраторов (поиск событий в записях по временным меткам), ИБП и систем охлаждения (аварии, переход на батареи), сетевого оборудования (syslog коммутаторов и маршрутизаторов), гипервизора (логи создания/удаления ВМ, изменения ресурсов), написания правил корреляции (например, «открытие двери серверной + отсутствие карты доступа в СКУД за 5 секунд до открытия + детекция движения в CCTV в этой зоне»), создания дашборда для мониторинга состояния защищенности ЗЦОД в реальном времени (количество активных тревог, статус систем жизнеобеспечения, число неудачных попыток доступа), а также настройки автоматического создания тикета в Service Desk (или отправки e-mail/SMS) при обнаружении инцидента критического уровня.

4.3. Самостоятельная работа обучающихся.

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

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

№ п/п	Библиографическое описание	Место доступа
1	Защищенные беспроводные и мобильные коммуникации: Учеб. пособие для студ., обуч. по магистерской программе Безопасность и защита инф-ции напр. Информатика и выч. тех.; МИИТ. Центр компетентности Защита и безопасность информации / В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев. - М.: МИИТ, 2007. - 121 с. : ил. - Библиогр.: с. 120 (7 назв.).	URL: http://library.miit.ru/miitpublishing/04-35015.pdf (miit.ru). (дата обращения 03.04.2025) Текст : непосредственный. 681.3
2	Голдовский Яков Михайлович. Структуры и алгоритмы обработки данных : Метод. указ. к лаб. раб. по дисц. "Структуры и алгоритмы обработки данных" для студ., обуч. по напр. "Информатика и вычислительная техника" / Я. М. Голдовский ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2012. - 36 с. : ил. - 100 экз.	URL: http://library.miit.ru/bookscatalog/metod/03-42034.pdf Текст : непосредственный. Полочный шифр 004 Г60. (дата обращения 03.04.2025)
3	Списки в моделях реляционных баз данных: метод. указ. к курсовому проекту по дисц. Структуры и алгоритмы обработки данных для студ., обуч. по напр. Информатика и выч. техника, профиль Программное обеспечение выч. техники и автоматизированных систем , по напр. Программная инженерия / Г.А. Шейкина; МИИТ. Каф. Математическое обеспечение автоматизированных систем управления. - М.: МИИТ, 2011. - 26 с. - Библиогр.: с. 26.	URL: http://library.miit.ru/bookscatalog/metod/04-35586.pdf,Текст : непосредственный. Полочный шифр 681.3-Ш39. (дата обращения 03.04.2025)

4	Методы обработки структур в среде DELPHI: метод. указ. к лаб. раб. для студ. информационных спец. ИУИТа / В.П. Соловьев, Н.Н. Пуцко; МИИТ. Каф. Математическое обеспечение автоматизированных систем управления. - М.: МИИТ, 2008. - 36 с. : ил.	URL: http://library.miit.ru/bookscatalog/metod/04-35737.pdf.(дата обращения 03.04.2025) Текст : непосредственный 004 С60
5	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://library.miit.ru/bookscatalog/metod/04-35430.pdf. (дата обращения 03.04.2025) Текст : непосредственный. 681.3 Г-60

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

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

ОС Microsoft Windows.

Microsoft Office

Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций):

- компьютер преподавателя, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 1 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