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 ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Технологии хранения 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).

Дисциплина посвящена изучению технической защиты информации. Целями освоения учебной дисциплины «Технологии хранения данных» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих задач.

Основными задачами дисциплины являются:

- изучение архитектур и классификации систем хранения данных (СХД) — Формирование знаний об основных типах систем хранения данных (DAS, NAS, SAN, объектные СХД, гиперконвергентные системы), их архитектурных особенностях, достоинствах, недостатках и областях применения;

- освоение методов организации отказоустойчивости и обеспечения целостности данных — Изучение принципов работы избыточных массивов независимых дисков (RAID) различных уровней (0, 1, 5, 6, 10, 50, 60), механизмов резервного копирования, репликации и снапшотов (мгновенных копий) для обеспечения высокой доступности и сохранности данных;

- изучение протоколов и интерфейсов доступа к системам хранения — Освоение протоколов взаимодействия с СХД (SCSI, iSCSI, FC, FCoE, NVMe, NVMe-oF, NFS, SMB/CIFS), а также интерфейсов подключения накопителей (SATA, SAS, NVMe, U.2, M.2);

- приобретение навыков администрирования и мониторинга систем хранения данных — Формирование практических умений по настройке, управлению и мониторингу СХД (выделение томов (LUN), управление квотами, контроль производительности — IOPS, пропускная способность, задержки), а также диагностике и устранению неисправностей;

- оценка производительности и выбор оптимальной конфигурации СХД — Изучение методик расчета производительности систем хранения (IOPS, латентность, пропускная способность), анализа профилей нагрузки (OLTP, OLAP, потоковое видео, резервное копирование) и обоснованного выбора типа и конфигурации СХД в зависимости от требований бизнес-задач;

- изучение методов защиты данных в системах хранения

— Освоение технологий шифрования данных на дисках (SED), на уровне томов и на уровне СХД, механизмов контроля доступа (RBAC), аудита операций с данными, а также методов защиты от утечек и несанкционированного доступа к хранимой информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

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

Знать:

- концепцию инженерно-технической защиты информации;
- нормативно-правовые документы обеспечения информационной безопасности;
- технические каналы утечки информации;
- физические принципы утечки информации по техническим каналам;
- методы обнаружения и защиты информации в технических каналах от ее утечки.

Уметь:

- применять методы инженерно-технической защиты информации;
- анализировать возможные уязвимые места технической защиты информации;
- проводить предварительный сбор данных о технических уязвимостях;
- проектировать системы защиты и проводить анализ рисков утечки информации по техническим каналам.

Владеть:

- навыками работы с программным обеспечением по оценки рисков утечки информации по техническим каналам и программно-аппаратными комплексами по выявлению каналов утечки информации.
- навыками инструментального мониторинга защищенности информации АС и анализа ее функционального состояния;
- навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений;
- основными методами исследования, использующими теории квантовой информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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 №6
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	16	16

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 40 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	Введение в технологии хранения данных. Классификация систем хранения Содержание учебного материала: - Определение системы хранения данных (СХД). Роль и место СХД в современной ИТ-инфраструктуре - Основные тенденции развития технологий хранения: рост объемов данных, требования к производительности, облачные и гибридные решения - Классификация СХД по архитектуре: DAS (Direct Attached Storage), NAS (Network Attached

№ п/п	Тематика лекционных занятий / краткое содержание
	Storage), SAN (Storage Area Network) - Классификация по типу носителей: HDD, SSD, гибридные массивы, ленточные библиотеки - Классификация по уровню корпоративного применения: начальный уровень, средний уровень, enterprise-класс - Классификация по способу организации: традиционные, гиперконвергентные (HCI), программно-определяемые (SDS) - Основные производители СХД: Dell EMC, NetApp, Hitachi, IBM, Huawei, отечественные решения (YADRO, Аэродиск)
2	Физические основы хранения данных. Накопители и интерфейсы Содержание учебного материала: - Накопители на жестких магнитных дисках (HDD): принцип работы, конструкция (пластины, головки, шпиндель), основные характеристики (скорость вращения 5400/7200/10000/15000 об/мин, объем, MTBF) - Твердотельные накопители (SSD): принцип работы (NAND-память: SLC, MLC, TLC, QLC), контроллер, интерфейсы (SATA, SAS, NVMe, U.2, M.2) - Сравнение HDD и SSD: производительность (IOPS, задержки), надежность, стоимость, энергопотребление, ресурс перезаписи (TBW) - Гибридные накопители (SSHD): принцип работы, области применения - Ленточные накопители (LTO): принцип работы, поколения LTO (LTO-7, LTO-8, LTO-9), емкость, скорость доступа, применение для долгосрочного архивирования - Интерфейсы подключения накопителей: SATA, SAS, NVMe, Fibre Channel - сравнение пропускной способности и областей применения
3	Организация массивов дисков. Технология RAID Содержание учебного материала: - Проблема надежности одиночных дисков. Принцип избыточности - Определение RAID (Redundant Array of Independent Disks). Базовые уровни RAID: - RAID 0 (Striping): принцип, производительность, отказоустойчивость (отсутствует) - RAID 1 (Mirroring): принцип, зеркалирование, надежность, эффективность использования емкости - RAID 5 (Striping с четностью): принцип, распределенная четность, минимальное количество дисков, отказоустойчивость (1 диск) - RAID 6 (двойная четность): принцип, отказоустойчивость (2 диска) - Комбинированные уровни RAID: RAID 10 (1+0), RAID 50 (5+0), RAID 60 (6+0) - Аппаратный vs. программный RAID: достоинства, недостатки, производительность - Проблема деградации массива и восстановления (rebuild). Влияние на производительность - Современные технологии: RAID 2.0 (динамическое выделение блоков), Erasure Coding в распределенных системах
4	Архитектуры систем хранения: DAS, NAS, SAN Содержание учебного материала: - DAS (Direct Attached Storage): архитектура, протоколы подключения (SATA, SAS, SCSI), преимущества (низкая задержка, простота), недостатки (отсутствие разделения ресурсов, масштабируемость) - NAS (Network Attached Storage): архитектура (CIFS/SMB для Windows, NFS для Unix/Linux), компоненты (NAS-головка, дисковое шасси), преимущества (простота организации, доступ по сети), недостатки (зависимость от сети, латентность) - SAN (Storage Area Network): архитектура, выделенная сеть хранения (Fibre Channel, iSCSI, FCoE, NVMe-oF) - Сравнение DAS, NAS и SAN: критерии выбора (производительность, масштабируемость, стоимость, сложность администрирования)

№ п/п	Тематика лекционных занятий / краткое содержание
	- Примеры сценариев использования: DAS для серверов баз данных, NAS для файловых серверов и домашних систем, SAN для виртуализации и критических приложений
5	Протоколы доступа к системам хранения данных Содержание учебного материала: - Протокол SCSI (Small Computer System Interface): история, архитектура, команды SCSI, применение - Протокол iSCSI (Internet SCSI): инкапсуляция SCSI в TCP/IP, компоненты (Initiator, Target), преимущества (использование существующей IP-сети), настройка безопасности (CHAP-аутентификация, IPsec) - Протокол Fibre Channel (FC): физический уровень (оптоволокно, медь), топологии FC (Point-to-Point, Arbitrated Loop, Switched Fabric), адресация (WWN), зонирование (zoning) и маскирование (masking) для безопасности - Протокол FCoE (Fibre Channel over Ethernet): конвергенция FC и Ethernet, применение - Протокол NVMe (Non-Volatile Memory Express) и NVMe-oF (NVMe over Fabrics): архитектура, преимущества перед SCSI/SAS, низкая латентность, многопоточность, использование с RDMA (InfiniBand, RoCE) - Сравнение протоколов по задержке, пропускной способности и областям применения
6	Обеспечение отказоустойчивости и непрерывности хранения данных Содержание учебного материала: - Ключевые показатели доступности: MTBF (среднее время между отказами), MTTR (среднее время восстановления), уровень доступности (99,9%, 99,99%, 99,999% - «пять девяток») - Резервное копирование (Backup): виды резервного копирования (полное, дифференциальное, инкрементное), схемы ротации носителей (Grandfather-Father-Son, Tower of Hanoi) - Целевые показатели восстановления: RPO (Recovery Point Objective) и RTO (Recovery Time Objective). Баланс между RPO/RTO и стоимостью решений - Снапшоты (Snapshots): принцип работы (copy-on-write, redirect-on-write), применение для быстрого восстановления и создания тестовых копий - Репликация (Replication): синхронная и асинхронная репликация между СХД, конфигурации (активный-активный, активный-пассивный), проблема split-brain и механизмы кворума - Кластеризация СХД: отказоустойчивый кластер, распределенные СХД (Ceph, GlusterFS) - План непрерывности бизнеса (BCP) и план восстановления (DRP): процедуры, тестирование, документация
7	Защита информации в системах хранения данных Содержание учебного материала: - Угрозы безопасности для систем хранения данных: несанкционированный доступ, утечка данных при хищении диска, атаки на протоколы доступа, вредоносное ПО (шифровальщики) - Шифрование данных: на уровне диска (SED - Self-Encrypting Drive), на уровне тома (BitLocker, LUKS), на уровне СХД (аппаратное шифрование AES-256) - Управление ключами шифрования: централизованное управление (KMIP, HSM), ротация ключей, резервное копирование ключей - Контроль доступа к СХД: ролевая модель (RBAC), интеграция с Active Directory/LDAP, двухфакторная аутентификация, аудит действий администраторов - Защита от атак на протоколы: аутентификация и шифрование в iSCSI (CHAP, IPsec), зонирование и маскирование в Fibre Channel - Защита от вымогательского ПО: immutable snapshots (неизменяемые снапшоты), WORM-носители (Write Once Read Many), air-gap резервные копии
8	Современные тенденции в технологиях хранения данных

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - Программно-определяемые системы хранения (SDS - Software-Defined Storage): принципы (абстракция ресурсов, управление через API), примеры (Ceph, VMware vSAN, StarWind) - Гиперконвергентные инфраструктуры (HCI - Hyper-Converged Infrastructure): объединение вычислений, хранения и сети в одном узле, примеры (Nutanix, VMware vSAN, Dell VxRail) - Объектное хранение (Object Storage): архитектура (плоское пространство идентификаторов, метаданные), протокол S3 (Amazon Simple Storage Service), применение для облачных и архивных решений - NVMe over Fabrics (NVMe-oF): принципы, использование RDMA (InfiniBand, RoCE), снижение латентности, примеры реализации - Искусственный интеллект в управлении СХД (AIOps): прогнозирование отказов (Predictive Failure Analysis), автоматическая оптимизация производительности, обнаружение аномалий - Системы хранения на основе энергонезависимой памяти (NVDIMM, Optane): принципы, производительность, применение - Облачное хранение: модели (IaaS, PaaS, SaaS), гибридные решения (cloud bursting, tiering в облако), обзор решений (AWS S3, Azure Blob, Google Cloud Storage, отечественные: S3 VK Cloud, MTS Cloud)

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Исследование физических характеристик накопителей (HDD, SSD) В результате выполнения работы студент изучит физические принципы работы жестких магнитных дисков (HDD) и твердотельных накопителей (SSD), выполнит измерение и сравнение производительности различных типов накопителей с использованием специализированного программного обеспечения (CrystalDiskMark, fio) по показателям последовательного и случайного чтения/записи, IOPS и латентности, проанализирует влияние интерфейса подключения (SATA, SAS, NVMe) на пропускную способность, а также подготовит отчет с выводами о применимости каждого типа накопителя для различных сценариев использования (OLTP, OLAP, файловый сервер, архив).
2	Исследование уровней RAID (0, 1, 5, 6, 10) на программном или аппаратном контроллере В результате выполнения работы студент изучит процессы создания массивов RAID различных уровней (0, 1, 5, 6, 10) с использованием программных средств ОС (mdadm в Linux) или эмулятора RAID-контроллера, выполнит измерение производительности (чтение/запись, IOPS) и оценку отказоустойчивости (моделирование выхода одного или двух дисков из строя, процедура восстановления - rebuild), проанализирует эффективность использования дискового пространства для каждого уровня, а также подготовит отчет с рекомендациями по выбору уровня RAID в зависимости от требований к производительности, надежности и емкости.
3	Настройка и исследование NAS-сервера (на базе FreeNAS / TrueNAS / OpenMediaVault) В результате выполнения работы студент изучит процессы развертывания и настройки NAS-сервера на базе FreeNAS/TrueNAS или OpenMediaVault, выполнит создание ZFS-пула и файловых ресурсов, настройку сетевых протоколов (SMB/CIFS для Windows, NFS для Unix/Linux), организацию доступа пользователей с разграничением прав, измерение производительности доступа по сети (задержки,

№ п/п	Тематика практических занятий/краткое содержание
	пропускная способность), а также подготовит отчет с выводами о применении NAS в малых и средних предприятиях.
4	Исследование подключения и настройки целевого устройства iSCSI (iSCSI Target) В результате выполнения работы студент изучит процессы развертывания iSCSI-целевого устройства (target) на сервере Linux (tgt, LIO) или Windows, выполнения подключения с клиента (iSCSI initiator), форматирования подключенного тома, выполнения тестов производительности и отказоустойчивости (переподключение при обрыве связи), настройки аутентификации (CHAP) и шифрования (IPsec) для защиты канала, а также подготовит отчет с выводами о применении iSCSI для организации SAN в условиях существующей IP-инфраструктуры.
5	Резервное копирование и восстановление данных. Реализация схемы «дедушка-отец-сын» В результате выполнения работы студент изучит процессы настройки системы резервного копирования (например, Bacula, Veeam или rsync с ротацией), реализации схемы ротации носителей GFS (Grandfather-Father-Son) с полным, дифференциальным и инкрементным бэкапами, выполнения ручного и автоматического восстановления данных из резервной копии, расчета целевых показателей RPO и RTO для заданного сценария, а также подготовит отчет с анализом эффективности выбранной схемы резервного копирования.
6	Исследование снапшотов (мгновенных копий) и репликации данных В результате выполнения работы студент изучит процессы создания снапшотов (мгновенных копий) на ZFS-пуле (например, в TrueNAS) или LVM, выполнения восстановления данных из снапшота после их удаления или модификации, настройки асинхронной или синхронной репликации между двумя системами хранения (например, ZFS send/receive), анализа времени создания снапшота, потребления дискового пространства и времени восстановления, а также подготовит отчет с выводами о применении снапшотов и репликации для обеспечения непрерывности бизнеса.
7	Шифрование данных в системах хранения (BitLocker, LUKS, SED) В результате выполнения работы студент изучит процессы настройки шифрования дисков с использованием средств ОС (BitLocker в Windows, LUKS/dm-crypt в Linux) и аппаратного шифрования на SED-дисках (Self-Encrypting Drive), выполнит включение шифрования, монтирование зашифрованных томов с паролем или ключом-файлом, проведет попытку восстановления данных с зашифрованного диска в обход шифрования (внешнее подключение без ключа), настройку централизованного управления ключами (при наличии HSM или KMIP), а также подготовит отчет с выводами о необходимости шифрования для защиты от утечек при физическом хищении носителя.
8	Исследование объектного хранилища (на примере MinIO или Ceph RGW) В результате выполнения работы студент изучит процессы развертывания объектного хранилища, совместимого с Amazon S3 (например, MinIO в Docker или Ceph RGW), выполнения операций с объектами (создание бакетов, загрузка/скачивание/удаление объектов) с использованием клиента AWS CLI или S3-совместимых SDK, настройки политик доступа (IAM), версионирования объектов и жизненного цикла данных, измерения производительности операций с объектами разного размера, а также подготовит отчет с выводами о преимуществах объектного хранения для облачных и архивных решений по сравнению с файловыми (NAS) и блочными (SAN) системами.

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

№ п/п	Библиографическое описание	Место доступа
1	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. (в пер.)	URL: 03-42764.pdf (miit.ru). (дата обращения 10.06.2026) Текст : непосредственный.004 Г60
2	Голдовский Я.М. ,Желенков Б.В., Цыганова Н.А. Маршрутизация в компьютерных сетях : [Электронный ресурс] : учеб. пособие по дисц. "Сети и телекоммуникации" для студ. напр. "Информатика и вычислительная техника" ; МИИТ. Каф. "Вычислительные системы и сети". - М. : РУТ(МИИТ), 2017. - 114 с.	- URL: DC-407.pdf (miit.ru).(дата обращения 10.06.2026)) Текст : непосредственный.004 Г60
3	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с. : ил. - Библиогр.: с. 26.	URL: 04-46051.pdf (miit.ru). (дата обращения 10.06.2026) Текст : непосредственный.004 К 72
4	Желенков Борис Владимирович. Канальный уровень модели OSI : метод. указ. к лаб. раб. по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", напр. "Информатика и вычислительная техника" / Б.В. Желенков ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2011. - 50 с. : ил. с. 49. - Текст : непосредственный	URL: 03-41547.pdf (miit.ru).(дата обращения 10.06.2026).Полочный шифр 004-Ж51

5	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	URL: 04-35015.pdf (miit.ru). (дата обращения 10.06.2026)) Текст : непосредственный.681.3

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).

Для проведения занятий по дисциплине необходимо наличие ПО Microsoft Office

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 практических занятий:

- компьютерный класс; кондиционер;
- компьютеры с минимальными требованиями.

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 6 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