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 направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Вычислительные системы и сети

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Защита информации» является 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:

• Ознакомление с методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

• Изучение методов проектирования систем, комплексов средств и технологий обработки и защиты информации и разработки технологической и эксплуатационной документации;

• Изучение методов установки, настройки, эксплуатации и поддержания в работоспособном состоянии компонентов системы обеспечения технической защиты информации с учетом установленных требований;

• Изучение методов проведения проектных расчетов элементов систем обеспечения технической защиты информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-4 - Способен решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и технологий искусственного интеллекта, а также с учетом основных требований информационной безопасности.

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 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 №5
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
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 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	Введение в защиту информации Содержание учебного материала: - Введение. - Информация. и защита данных. - Конфиденциальность информации. - Целостность информации. - Доступность информации. - Служебная информация. - Личные данные. - Государственные структуры, отвечающие за защиту данных. - Определение служебной тайны. - Законодательство РФ в области информационной безопасности. - Информационная безопасность коммерческой структуры. -Типовой набор должностей, связанных с защитой данных на предприятии. - Международные стандартизирующие организации. - Стандарты РФ в области информационной безопасности.
2	Криптографическая защита. Основы и классификация Содержание учебного материала: — Классификация криптографических алгоритмов — Основные определения (шифрование, ключ, криптостойкость) — Назначение шифрования: конфиденциальность и целостность — Принципы криптографического закрытия информации (замещение, переста-новка, гаммирование) — Простые методы шифрования (Цезарь, Атбаш) — Таблица Вижинера (алгоритм, примеры, вскрытие) — Шифрование с открытым и закрытым ключами: концептуальная разница — Основные виды атак на криптоалгоритмы (атака по шифротексту, по откры-тому тексту, «человек посередине»)
3	Симметричные криптоалгоритмы. DES и 3DES Содержание учебного материала:

№ п/п	Тематика лекционных занятий / краткое содержание
	— Принципы симметричного шифрования (общий ключ) — Алгоритм DES: структура (сеть Фейстеля), S-блоки, размер ключа и блока — Уязвимости DES: малый ключ, атака грубой силы — Алгоритм 3DES (тройной DES): режимы EDE, эффективная стойкость — Вопросы стойкости: время перебора, различимые атаки — Проблема распределения ключей в симметричной криптографии
4	Симметричная криптография. AES и современные алгоритмы Содержание учебного материала: — Алгоритм AES (Rijndael): этапы (SubBytes, ShiftRows, MixColumns, AddRoundKey) — Размеры ключа (128/192/256 бит) и стойкость — Режимы шифрования (ECB, CBC, CFB, OFB, GCM, CTR) — Вопросы стойкости: линейный и дифференциальный криптоанализ AES — Достоинства и недостатки симметричного шифрования (скорость vs. пробле-ма ключей) — Область применения симметричных алгоритмов (шифрование дисков, VPN, хранение данных)
5	Асимметричные криптоалгоритмы. Математические основы Содержание учебного материала: — Математические основы асимметричной криптографии (теория чисел, про-стые числа, модульная арифметика) — Алгоритм Диффи-Хэллмана: выработка общего ключа через открытый канал — Алгоритм RSA: генерация ключей (p, q, e, d), шифрование/дешифрование — Достоинства и недостатки асимметричного шифрования (безопасность без предварительного обмена ключами, но низкая скорость) — Область применения: шифрование небольших объёмов данных, транспорт ключей
6	Электронно-цифровая подпись (ЭЦП) и хэш-функции Содержание учебного материала: — Принципы ЭЦП: подпись приватным ключом, проверка публичным — Алгоритмы ЭЦП: RSA-PSS, DSA, ECDSA — Криптографические хэш-функции: требования (однонаправленность, устой-чивость к коллизиям) — Основные хэш-алгоритмы: MD5 (скомпрометирован), SHA-1, SHA-256, SHA-3 — Применение хэшей: контроль целостности, хранение паролей, связка с ЭЦП
7	Протоколы аутентификации и управления ключами Содержание учебного материала: — Протоколы аутентификации (простой пароль, challenge-response, одноразовые пароли) — Протокол Kerberos: билеты, KDC, временные метки — PKI (Public Key Infrastructure): удостоверяющие центры (CA), сертификаты X.509 — Отзыв сертификатов (CRL, OCSP) — Распределение ключей в сетях (IKE в IPsec)
8	Атаки на криптосистемы и их моделирование Содержание учебного материала: — Классификация атак: пассивные (прослушивание) и активные (подмена, повтор) — Атака «человек посередине» на Diffie-Hellman и RSA без аутентификации — Атака с использованием подобранного открытого текста (CPA) и шифротекста (CCA) — Атаки по побочным каналам (время, питание, электромагнитное излучение) — Атаки на протоколы SSL/TLS (POODLE, Heartbleed, BEAST)
9	Инфраструктура открытых ключей (PKI) и сертификаты Содержание учебного материала: — Компоненты PKI: CA, RA, хранилище сертификатов — Структура сертификата X.509 (поля: subject, issuer, public key, срок действия) — Цепочки доверия (корневой, промежуточный, конечный сертификат) — Регистрация и аннулирование сертификатов — Применение PKI: TLS/HTTPS, S/MIME, кодовая подпись

№ п/п	Тематика лекционных занятий / краткое содержание
10	Криптографическая защита в сетях. Протокол TLS/SSL Содержание учебного материала: — Архитектура TLS: Record Protocol, Handshake Protocol — Рукопожатие TLS: согласование шифров, аутентификация сервера (иногда клиента), выработка сессионного ключа — Используемые криптоалгоритмы в TLS (RSA, ECDHE, AES-GCM, ChaCha20) — Уязвимости версий SSL 2.0/3.0 и TLS 1.0/1.1 — Современные требования: TLS 1.2/1.3, отключение слабых шифров
11	Криптографическая защита виртуальных частных сетей (IPsec, OpenVPN) Содержание учебного материала: — Архитектура IPsec: ESP (шифрование и аутентификация), AH (аутентифика-ция) — Режимы IPsec: транспортный и туннельный — Управление ключами в IPsec: IKEv1/IKEv2 — OpenVPN: крипто-конфигурация (статический ключ, TLS-аутентификация) — Сравнение IPsec и OpenVPN: производительность, совместимость
12	Криптографическая защита дисков и файлов (BitLocker, LUKS, VeraCrypt) Содержание учебного материала: — Модели шифрования на диске: полное шифрование диска (FDE), шифрование файлов (EFS) — BitLocker (Windows): TPM, PIN, ключ восстановления — LUKS (Linux): заголовок LUKS, ключи, режим шифрования — VeraCrypt: скрытые тома, шифрование «на лету» — Атаки на шифрование дисков (холодная перезагрузка, перехват ключа из RAM)
13	Криптографические хэш-функции и аутентификация сообщений (HMAC) Содержание учебного материала: — Свойства хэш-функций (детерминизм, лавинный эффект) — Конструкция Меркла-Дамгора (MD5, SHA-1/2) и её уязвимости (длинная ата-ка) — Криптоанализ хэш-функций: атака «дней рождения», коллизии для MD5 — HMAC (Hash-based Message Authentication Code): конструкция, преимущества перед обычным хэшем с ключом — Применение HMAC в протоколах (TLS, IPsec, API-аутентификация)
14	Криптография в платежных системах и банковских картах (PCI DSS, EMV) Содержание учебного материала: — Стандарт PCI DSS: требования к хранению и передаче данных карт — Шифрование PAN в базах данных — EMV (чиповые карты): динамические данные, криптограмма (ARQC, ARPC) — Токенизация (замена PAN токеном) и её криптографические аспекты — Атаки на банковские карты (skim-устройства, реплей атаки)
15	Постквантовая криптография Содержание учебного материала: — Угрозы квантовых компьютеров (алгоритм Шора против RSA и ECC, Грове-ра против AES) — Постквантовые алгоритмы: на основе решёток (Kyber, Dilithium), хэш-функций (SPHINCS+) — Сравнение стойкости классической и постквантовой криптографии — Переход на постквантовые стандарты NIST — Проблемы совместимости и производительности
16	Криптографическая защита баз данных Содержание учебного материала: — Проблемы: шифрование колонок vs. индексирование, поиск по зашифрован-ным данным — Шифрование на уровне приложения, БД (TDE) и файловой системы — Deterministic шифрование для поиска (уязвимость к частотному анализу) — Homomorphic шифрование (теоретический обзор, выполнение операций над зашифрованными

№ п/п	Тематика лекционных занятий / краткое содержание
	данными) — Аудит доступа к зашифрованным БД
17	Целостность и аутентификация данных. Коды аутентичности (MAC, GMAC) Содержание учебного материала: — Отличие MAC от цифровой подписи (симметричный vs. асимметричный ключ) — Алгоритмы: CMAC, HMAC, Poly1305 — GMAC (на основе AES-GCM): принцип работы, производительность — Комбинированные режимы шифрования с аутентификацией (AEAD): GCM, CCM, ChaCha20-Poly1305 — Примеры использования в сетевых протоколах
18	Стеганография и криптография: сокрытие факта передачи информации Содержание учебного материала: — Определение стеганографии, отличие от криптографии — Классические методы: LSB (младший бит) в изображениях и аудио — Стеганография в сетевых протоколах (TCP-опции, поля IP ID) — Методы обнаружения стеганографии (стегоанализ) — Комбинация стеганографии и шифрования
19	Криптографическая защита беспроводных сетей (Wi-Fi, Bluetooth) Содержание учебного материала: — Протокол WEP: уязвимости (атака Флюрера, Мантейна, CRC-32) — WPA/WPA2: TKIP vs CCMP (AES), 4-way handshake — Атака KRACK на WPA2 — WPA3: Simultaneous Authentication of Equals (SAE), защита от офлайн-перебора — Безопасность Bluetooth (парный ключ, шифрование E0/LE)
20	Криптографические механизмы в операционных системах Содержание учебного материала: — Шифрование своп-раздела и подкачки (Windows, Linux) — Защита памяти ASLR, PIE, NX, KASLR (криптографические аспекты) — Хранение хэшей паролей: /etc/shadow, NTLM, пассивная защита — Криптографические API: CryptoAPI (Windows), Keychain (macOS), Kernel keyring (Linux) — Аппаратная поддержка: TPM (Trusted Platform Module), инструкции AES-NI
21	Правовое регулирование криптографии. Экспортный контроль Содержание учебного материала: — Законодательство РФ: ФЗ «Об информации», ФЗ «О связи», приказы ФСБ — Экспортный контроль криптографических средств (Вассенаарские соглашения) — Лицензирование деятельности по распространению шифровальных средств — Ответственность за нелегальное использование криптографии — Зарубежные регуляторы: ITAR (США), GDPR и шифрование
22	Криптографические протоколы электронного голосования Содержание учебного материала: — Требования к криптопротоколам голосования (анонимность, корректность, устойчивость к повторам) — Протоколы на основе слепой подписи (схема Фудзиока — Окамото — Оты) — Homomorphic шифрование (схема Эль-Гамаля для голосования) — Голосование с использованием блокчейна (анализ) — Реальные системы: Helios Voting, Voatz (криптоанализ)
23	Управление жизненным циклом ключей Содержание учебного материала: — Генерация ключей (энтропия, TRNG, PRNG) — Распределение ключей (KDC, протоколы, предварительное распределение)

№ п/п	Тематика лекционных занятий / краткое содержание
	— Хранение ключей (HSM, аппаратные токены, смарт-карты) — Ротация, отзыв и уничтожение ключей — Резервное копирование ключей (key escrow)
24	Атаки на реализацию криптоалгоритмов (side-channel attacks) Содержание учебного материала: — Атаки по времени (Timing attacks) на сравнение строк и RSA — Анализ питания (Simple / Differential Power Analysis) на AES — Акустический криптоанализ (звук конденсаторов и катушек) — Атаки по ошибкам (Fault injection), сброс напряжения — Контрмеры: маскировка, постоянное время выполнения

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Введение в информационную безопасность. Стандарты и организации, работающие в области информационной безопасности В результате выполнения лабораторной работы студент получит практические навыки поиска нормативной информации в глобальной сети, работы с нормативными актами в сфере ИБ, навыки выяв-ления и учета информационных активов защищаемой организации.
2	Угрозы информационной безопасности В результате выполнения лабораторной работы студент получит навыки создания списка информационных активов, определения актуальных угроз информационной безопасности, классификации источников угроз и защищаемой информации в соответствии с существующей нормативной базой.
3	Политика безопасности. Разработка политики безопасности В результате выполнения лабораторной работы студент получит практические навыки разработки политики информационной безопасности предприятия.
4	Криптографическая защита. Шифрование и расшифрование данных В результате выполнения лабораторной работы студент приобретает навыки работы с базовыми криптографическими алгоритмами и совершенствует свои навыки программирования на языках высокого уровня.
5	Изучение оборудования стенда «Системы контроля и управления доступом» В результате выполнения лабораторной работы студент изучает состав лабораторного оборудования, технику безопасности при работе с ним и готовится к выполнению последующих лабораторных работ.
6	Изучение интерфейса связи Dallas Touch Memory (iButton) В результате выполнения лабораторной работы студент приобретает навыки работы с норматив-ной и технической документацией и подготовке к работе интерфейса связи iButton.
7	Контроль доступа с помощью считывателя iButton и контролера СКУД в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение с помощью считывателя iButton, включая программирование ключей и ведение базы данных пользователей.
8	Изучение интерфейса связи Wiegand В результате выполнения лабораторной работы студент приобретает навыки работы с нормативной и технической документацией и подготовке к работе интерфейса связи Wiegand.

№ п/п	Наименование лабораторных работ / краткое содержание
9	Изучение RFID-технологии и стандартов карт доступа В результате выполнения лабораторной работы студент приобретает навыки использования нормативной документации - стандартов на карты доступа и выполняет подготовку к работе с RFID-оборудованием.
10	Контроль доступа с помощью RFID-считывателя и контролера СКУД в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение с помощью считывателя карт доступа по RFID-технологии, включая программирование карт и ведение базы данных пользователей.
11	Контроль доступа с помощью контролера СКУД в сетевом режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение в сетевом режиме работы контроллера СКУД.
12	Изучение технологии считывания биометрических данных В результате выполнения лабораторной работы студент приобретает навыки с технической документацией, изучает состав оборудования считывания биометрических данных и готовится к его использованию.
13	Конфигурирование биометрического считывателя в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение или к рабочему месту с помощью анализа его биометрических данных – отпечатков пальца.
14	Установка устройства контроля доступа к компьютеру «Соболь» В результате выполнения лабораторной работы студент изучает устройство «Соболь», технику безопасности при работе с ним и устанавливает его на компьютер.
15	Защита от несанкционированного доступа В результате выполнения лабораторной работы студент получит базовые навыки защиты информации от НСД: обеспечение безопасности персонального компьютера средствами операционной системы и с помощью USB-ключей.
16	Защита информации в глобальной сети В результате выполнения лабораторной работы студент получит навыки безопасного использования сети Internet.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Защита информации в глобальной сети
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. Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей.

2. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

3. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

4. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

5. Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ.

6. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.

7. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации.

8. Технические средства контроля эффективности защиты информации на примере вербального объекта информатизации.

9. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации.

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 03.05.2026) 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 03.05.2026) 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 03.05.2026) 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 03.05.2026).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 без-опасность 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 03.05.2026) Текст : непосредственный.681.3

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

- Научная электронная библиотека (http://elibrary.ru)
- Материалы по информационным технологиям (www.citforum.ru)
- Официальный сайт РУТ (МИИТ) http://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).

- Интернет-браузер (Yandex и др.)
- Microsoft Windows.
- Microsoft Office

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ, курсового проектирования (выполнения курсовых работ):

- компьютер преподавателя, мультимедийное оборудование, рабочие станции студентов, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

Курсовая работа в 5 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