

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ

И.о. зав. кафедрой
«Информационная
безопасность»



Сафиуллина Л.Х.

«20» марта 2026 г.

Программа вступительных испытаний в магистратуру

Направление 10.04.01 «Информационная безопасность»
Программа подготовки «Комплексное обеспечение безопасности
автоматизированных систем»

Институт ИУАИТ

Кафедра-разработчик программы:
«Информационная безопасность»

Казань, 2026

1. Вопросы программы вступительного экзамена в магистратуру по направлению

10.04.01 «Информационная безопасность» Программа подготовки «Комплексное обеспечение безопасности автоматизированных систем».

1. Информация и данные: понятие информации, отличие данных от информации. Меры количества информации (синтаксическая, семантическая, прагматическая). Сравнение формул Хартли и Шеннона.
2. Сигналы и их преобразование: аналоговый, дискретный и цифровой сигналы; дискретизация и квантование. Преобразование аналоговых сигналов в цифровые (АЦП). Понятие модуляции/демодуляции.
3. Кодирование информации. Цели кодирования. Сжимающее (архивация) и помехоустойчивое кодирование. Обнаружение и исправление ошибок.
4. Передача данных. Канал и линия связи. Характеристики каналов (пропускная способность, помехозащищенность). Виды физических линий связи (проводные, оптоволоконные, беспроводные).
5. Сетевые технологии: корпоративная сеть передачи данных: характеристики, уровни (модель OSI/стек TCP/IP), топология. Маршрутизация потоков: статические и динамические протоколы, таблицы маршрутизации.
6. Сетевые протоколы и адресация: базовые протоколы стека TCP/IP (IP, TCP, UDP, HTTP, DNS, DHCP). Принципы IP-адресации (IPv4, IPv6). NAT.
7. Модели угроз в сетях: основные виды сетевых атак (перехват, DDoS, ARP-спуфинг, DNS-спуфинг). Понятие Cyber Kill Chain. Матрица MITRE ATT&CK. Межсетевое экранирование, ACL.
8. Основы информационной безопасности: определение информации как объекта права. Классификация информации по категориям доступа (общедоступная, ограниченного доступа). Свойства информации как объекта безопасности (конфиденциальность, целостность, доступность). Модель угроз.
9. Государственная политика: понятие безопасности и информационной безопасности. Основные положения Доктрины информационной безопасности Российской Федерации.
10. Законодательство РФ в области ИБ (общие законы): основные положения Федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите информации».
11. Законодательство РФ в области ИБ (персональные данные): основные положения Федерального закона №152-ФЗ «О персональных данных». Государственное регулирование работы с ПДн.

12. Законодательство РФ в области ИБ (гос. и коммерческой тайны): основные положения Федеральных законов «О государственной тайне» №5485-1 и «О коммерческой тайне» №98-ФЗ.
13. Регуляторы в сфере ИБ в РФ: ФСТЭК, ФСБ, Роскомнадзор, Банк России. Их функционал и сфера деятельности.
14. Защита критической информационной инфраструктуры (КИИ): понятие КИИ, субъекты и объекты КИИ. Основные положения Федерального закона №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Требования к созданию систем безопасности КИИ (ГосСОПКА).
15. Управление информационной безопасностью: цели и задачи управления ИБ. Понятие рисков ИБ. Основные принципы управления рисками.
16. Стандартизация в области ИБ: международные и национальные стандарты (семейство ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001). Основные принципы и подходы СУИБ.
17. Политика информационной безопасности (ПИБ): структура ПИБ, этапы разработки, внедрения и совершенствования. Распределение обязанностей, связанных с ИБ, в организации.
18. Аудит и структура подразделений ИБ: цели и основные этапы аудита информационной безопасности. Структура, задачи и функции департамента (отдела) информационной безопасности на предприятии.
19. Основы криптографии: симметричное и асимметричное шифрование. Хэш-функции и их применение (ЭЦП, имитовставка). Управление ключами.
20. Криптографические протоколы: протоколы аутентификации и обеспечения конфиденциальности (TLS/SSL, IPsec, SSH). Инфраструктура открытых ключей (PKI), цифровые сертификаты.
21. Основы криптографии: симметричное и асимметричное шифрование. Хэш-функции и их применение (ЭП, имитовставка). Управление ключами.
22. Криптографические протоколы: протоколы аутентификации и обеспечения конфиденциальности (TLS/SSL, IPsec, SSH). Инфраструктура открытых ключей (PKI), цифровые сертификаты.
23. Инженерно-техническая защита информации (ИТЗИ): технические каналы утечки информации (акустические, визуально-оптические, электромагнитные). Методы и средства защиты от утечек по техническим каналам.
24. Физическая защита и контроль доступа: системы контроля и управления доступом (СКУД), системы охранной сигнализации и видеонаблюдения. Организация пропускного режима на объекте.

25. Безопасность автоматизированных систем (АС): особенности защиты АСУ ТП и промышленного интернета вещей (IIoT). Отличия от защиты классических ИТ-систем. Понятие SDLC (безопасная разработка).

2. Учебно-методическое и информационное обеспечение программы вступительного экзамена в магистратуру по направлению 10.04.01 «Информационная безопасность»
Программа подготовки «Комплексное обеспечение безопасности автоматизированных систем»

а) основная литература:

Нормативно-правовая литература:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/.
2. Российская Федерация. Законы. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/.
3. Российская Федерация. Законы. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_220885/.
4. Российская Федерация. Указы Президента. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: <https://login.consultant.ru/link/?req=doc&base=LAW&n=208191>.

Учебники и учебные пособия:

Основы теории информации и сигналов:

5. Осокин, А. Н. Теория информации : учебник для вузов / А. Н. Осокин, А. Н. Мальчуков. — Москва : Издательство Юрайт, 2025. — 208 с.
6. Лидовский В.В. Основы теории информации и криптографии / В.В. Лидовский. - Москва : Национальный Открытый Университет ИНТУИТ, 2024. - 141 с.,
7. Сафиуллина Л. Х., Алексеева А. А., Сабирова Д. И. Аппаратные средства вычислительной техники / КНИТУ. 2024 – 108 с.
8. Сафиуллина Л.Х., Алексеева А.А., Садыков А.М. Основы информационной безопасности / МеДДок. 2025 – 156 с.

Сети и телекоммуникации:

9. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 423 с.
10. Таненбаум Э. Компьютерные сети. 6-е изд. / Э. Таненбаум, Н. Фимстер, Д. Уэзеролл. — 6-е изд. — СПб.: Питер, 2023. — 960 с.

Организационно-правовое обеспечение и управление ИБ:

11. Аверченков, В. И. Организационная защита информации / В. И. Аверченков, М. Ю. Рытов. — 3-е изд. — Москва : ФЛИНТА, 2011. — 184 с.
12. Москвитин, Г. И., Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с.
13. Алексеева А.А., Сафиуллина Л.Х., Садыков А.М., Основы вычислительных систем / КНИТУ. 2025. — 160 с.

Инженерно-техническая защита информации (ИТЗИ):

14. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с.
15. Рогозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю.Н. Рогозин. — Санкт-Петербург : ИЦ Интермедия, 2019. — 216 с.
16. Мельников, В. П. Защита информации : учебник / В.П. Мельников. Под ред., Мельников В.П., Куприянов А.И. — Москва : Академия, 2021. — 267 с.

Физическая защита и системы охраны:

17. Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения : учебное пособие / Р. Г. Магауенов. — 2-е изд. — Москва : Горячая линия–Телеком, 2022. — 494 с.
18. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. — Москва : Горячая линия–Телеком, 2025. — 272 с.

б) дополнительная литература:

По разделу «Теория информации»:

1. Данелян, Т. Я. Общая теория информации (ОТИ) : учебно-методическое пособие / Т. Я. Данелян, М. Н. Епихин. — Москва : Русайнс, 2024. — 116 с.

По разделу «Сети»:

2. Никулин, А. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / А. В. Никулин, В. В. Артюшенко. – Новосибирск : НГТУ, 2019. – 72 с.
3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – СПб : Питер, 2024. – 1008 с.
4. Сафиуллина Л.Х., Ишкинин И.Ф., Касимова А.Р., Уязвимость и безопасность вычислительных сетей. Часть 1,2,3 / Мэйл Текнолоджи. 2021 – 216 с.
5. Касимова А.Р., Сабирова Д.И., Угрозы и защита корпоративных сетей: моделирование на киберполигоне / МеДДок. 2025 – 100 с.

По разделу «Комплексная защита и управление ИБ»:

6. Жук, А. П. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. – 400 с.
7. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 с.
8. Астахов, А. М. Искусство управления информационными рисками / А. М. Астахов. – Москва : ДМК Пресс, 2018. – 314 с.

По разделу «ИТЗИ и физическая защита» (Фундаментальные труды):

9. Торокин, А. А. Инженерно-техническая защита информации : учеб. пособие для студентов, обучающихся по специальностям в обл. / А. А. Торокин. – 2-е изд. – М. : Гелиос АРВ, 2005 – 960 с.
10. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил.

в) программное обеспечение и Интернет-ресурсы

Официальные ресурсы (нормативная база):

1. Официальный сайт ФСТЭК России: <http://fstec.ru/> (разделы «Техническая защита информации», «Документы»).
2. Официальный сайт ФСБ России: <http://www.fsb.ru/> (разделы по лицензированию и сертификации).
3. Официальный сайт Совета Безопасности РФ: <http://www.scrf.gov.ru/>

4. Справочно-правовая система «КонсультантПлюс»: <http://www.consultant.ru/>
5. Справочно-правовая система «Гарант»: <http://www.garant.ru/>

Электронно-библиотечные системы (ЭБС) и базы данных:

1. Электронный каталог УНИЦ КНИТУ: <http://ruslan.kstu.ru/>
2. ЭБС «Лань»: <https://e.lanbook.com>
3. Образовательная платформа «Юрайт»: <https://urait.ru/>
4. ЭБС «Znaniy.com»: <http://znaniy.com/>
5. ЭБС «Университетская библиотека онлайн»: <http://biblioclub.ru/>
6. ЭБС IPRbooks: <http://www.iprbookshop.ru/>
7. ЭБС BOOK.ru: <https://www.book.ru/>
8. Научная электронная библиотека (eLibrary): <https://elibrary.ru/>

Профессиональные журналы и порталы (рекомендуется для самостоятельного изучения):

1. Журнал «Вопросы защиты информации» (eLibrary).
2. Журнал «Защита информации. Инсайд».
3. Интернет-портал «SecurityLab»: <https://www.securitylab.ru/>
4. Интернет-портал Anti-Malware: <https://www.anti-malware.ru/> (аналитика и новости ИБ).