

**Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

Утверждаю:

Проректор по учебной работе



В.В. Смирнов

« 47 » *сентября* 2025 г.

ПРОГРАММА

**Вступительного испытания
для поступающих на программу магистратуры 10.04.01 «Безопасность
киберфизических систем»**

Основы защиты информации в киберфизических системах

Иркутск 2025 г.

Программа вступительных испытаний для поступления на программу магистратуры «Безопасность киберфизических систем (защита информации в компьютерных системах и сетях)» по направлению 10.04.01 «Информационная безопасность» разработана на основании федеральных государственных образовательных стандартов высшего образования – входящих в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ АБИТУРИЕНТА

Абитуриент должен иметь представление:

- о роли проблем защиты информации в общей совокупности информационных проблем современного общества;
- о способах представления различных видов информации на компьютерных носителях, а также защиты данной информации;
- о регулировании и противодействиях правонарушениям в сфере экономической безопасности;
- о сферах науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Абитуриент должен знать:

- принципы построения аналитико-имитационных моделей информационных процессов, основные классы моделей и методы моделирования, методы формализации, алгоритмизации и реализации моделей на вычислительных системах;
- способы записи алгоритмов и конструирования программ с использованием различных алгоритмических языков процедурного и объектно-ориентированного программирования;
- основные принципы организации и функционирования компьютерных систем, комплексов и сетей;
- характеристики, возможности и области применения наиболее распространенных классов и типов вычислительных систем в информационных системах;
- формы представления, хранения, передачи и преобразования информации в вычислительных системах;
- архитектуру, основные устройства, системное программное обеспечение персонального компьютера и компьютерных сетей;
- методы разработки алгоритмов и программ, основные информационные и управляющие структуры алгоритмов;
- средства описания данных и действий в языках программирования высокого уровня, основные алгоритмы решения типовых задач и способы их реализации; виды программного

обеспечения, для решения математических и инженерно-технических задач.

Абитуриент должен уметь использовать:

- специальные знания по применению современных технологий информационной безопасности, в том числе в структуре региона;
- осуществлять информационную безопасность различных информационных объектов и структур;
- современные системные программные средства защиты информации;
- сетевые программные и технические средства защиты информации.

Абитуриент должен иметь опыт:

- применения математических методов и алгоритмов вычислительной математики при решении профессиональных задач и анализе прикладных проблем в профессиональной области;
- практический опыт использования математически сложных алгоритмов в современных программных комплексах (ТЗИ), включая реализацию в них собственных методов и моделей по защите информации;
- работы с объектами информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере.

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема 1. Основные понятия информационной безопасности и защиты информации.

1.1 Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.

1.2 Основные понятия информатики. Сообщения, данные, сигнал, показатели качества информации, формы представления информации. Системы передачи информации. Меры и единицы количества и объема информации. Понятие и защита данных.

1.3 Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.

1.4 Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.

1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.

1.6 Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.

Тема 2. Организационное и правовое обеспечение информационной безопасности.

2.1 Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации.

2.2 Системы сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации. Справочно-правовые системы с нормативными и правовыми документами по информационной безопасности.

2.3 Основные положения Доктрины информационной безопасности Российской Федерации.

2.4 Стратегия национальной безопасности Российской Федерации. Государственная система защиты информации и ее структура.

2.5 Лицензирование, сертификация и аттестация в области защиты информации.

2.6 Основные положения закона РФ «Об информации, информационных технологиях и о защите информации», закона РФ «О персональных данных». Основные положения Федеральных Законов РФ «О государственной тайне», «О коммерческой тайне».

2.7 Преступления в области защиты информации (Уголовный кодекс РФ, Гражданский кодекс РФ, Кодекс об административных правонарушениях РФ).

Тема 3. Защита информации в автоматизированных (информационных) системах.

3.1 Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.

3.2 Программные и программно-аппаратные средства защиты информации.

3.3 Инженерная защита и техническая охрана объектов информатизации.

3.4 Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно-распорядительной системы.

Тема 4. Локальные и глобальные компьютерные сети (защита информации в сетях).

4.1 Классификация компьютерных сетей. Топологии, методы доступа к физической среде. Понятие, классификация и виды компьютерных сетей. Аппаратные

компоненты вычислительных сетей. Сервисы Интернета. Социальная сеть и социальные сервисы. Угрозы безопасности информации в сети, их виды.

4.2 Защита информации от несанкционированного доступа в сети, IP-адресация, служба DHCP. Защита информации в локальных и глобальных компьютерных сетях.

4.3 Оборудование для связи компьютеров. Стеки протоколов и модель OSI. Механизмы перемещения данных в сети. Протоколы передачи информации. Защита службы трансляции имен Интернета. Защита облачных вычислений.

4.4 Классификация сетевых атак. Анализ трафика. Создание ложного потока. Повторное использование (replay-атака). Модификация потока данных. Отказ в обслуживании (DoS-атака). Шифрование (алгоритмы симметричного шифрования; алгоритмы шифрования с открытым ключом), Malicious software – вредоносное программное обеспечение.

Тема 5. Технологии программирования, алгоритмы и структуры данных.

5.1 Жизненный цикл программного обеспечения. Тестирование программ. Параллельные методы программирования.

5.2 Основные алгоритмы поиска данных, их временная сложность. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных.

5.3 Временная сложность алгоритмов. Оценка времени выполнения программ. Основные абстрактные типы данных: списки, стеки, очереди, деревья, ориентированные и неориентированные графы.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ, 2019.
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2018.
3. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – 2-е изд., стер. – М. : КНОРУС, 2017.
4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2018. <http://biblioclub.ru/index.php?page=book&id=571750>.
5. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования // Национальные стандарты. – Режим доступа: <http://protect.gost.ru/document.aspx?control=7&id=139177> (дата обращения: 15.01.2025).
6. Диогенес Ю., Озкая Э. Кибербезопасность: стратегии атак и обороны /пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с
7. Дергачева, Л. М. Решение типовых экзаменационных задач по информатике: учеб. пособие / Л. М. Дергачева. – М. : БИНОМ. Лаборатория знаний, 2013. – 360 с.
8. Зиангирова, Л. Технологии облачных вычислений // НОУ «ИНТУИТ». – Режим доступа: <http://www.intuit.ru/studies/courses/3508/750/lecture/27409> (дата обращения: 15.01.2025).
9. Колисниченко, Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание / Д. Н. Колисниченко. – СПб. : Наука и техника, 2004. – 400 с.
10. Островский Г. М., Волин Ю. М. Технические системы в условиях неопределенности: анализ гибкости и оптимизация: учебное пособие / Островский Г. М., Волин Ю. М. – М.: Лаборатория знаний, 2020. – 322 с.
11. Куроуз, Дж. Компьютерные сети / Дж. Куроуз, К. Росс. – СПб. : Питер, 2004. – 765 с.
12. К. Дж. Дейт Введение в системы баз данных. – Вильямс, 2018 г.
13. Лапониная, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапониная. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608 с.
14. Русанов Г.А. Противодействие легализации (отмыванию) преступных доходов: учеб. пособие для бакалавриата и магистратуры. – М.: Издательство Юрайт, 2017. – 157 с.

15. Хизер Адкинс, Бетси Бейер, Пол Бланкиншип, Петр Левандовски, Ана Опреа, Адам Стаблфилд Безопасные и надежные системы: Лучшие практики проектирования, внедрения и обслуживания как в Google. – СПб.: Питер, 2025. – 592 с.
16. Хоффман Эндрю Безопасность веб-приложений. Разведка, защита, нападение. 2-е изд. – Астана: «Спринт Бук», 2025. – 432 с.

КРИТЕРИИ ОЦЕНКИ

В ходе экзамена абитуриент проходит компьютерное тестирование с ограничением времени по темам программы вступительного экзамена, утвержденной проректором по учебной работе Иркутского национального исследовательского технического университета.

Абитуриенту предлагается суммарно 50 вопросов из обязательных разделов 1-3 и разделов 4-5 по выбору. В тесте присутствуют задания открытого типа, открытого типа с развёрнутым ответом и закрытого типа. Задания открытого типа предполагают, что на каждый вопрос испытуемый должен предложить свой ответ: дописать слово, словосочетание, предложение, знак, формулу. В заданиях открытого типа с развёрнутым ответом нужно подробно объяснить свою мысль, привести аргументы, сделать выводы или описать процесс решения (например, написать эссе или решить задачу с полным объяснением хода решения). Задания закрытого типа предусматривают различные варианты ответа на поставленный вопрос: из ряда предлагаемых выбираются один или несколько правильных ответов.

По результатам тестирования выставляется итоговая оценка путем суммирования количества правильных ответов.

Правила оценки всего теста. Общая сумма баллов за все правильные ответы составляет «наивысший балл», например 95 баллов. В спецификации указывается общий наивысший балл по тесту. Также устанавливается диапазон баллов, которые необходимо набрать для того, чтобы получить отличную, хорошую, удовлетворительную или неудовлетворительную оценки.

В процентном соотношении оценки (по пятибалльной системе) рекомендуется выставлять в следующих диапазонах:

Процентное соотношение	Оценка
менее 50%	Неудовлетворительно- «2»
50%-64%	Удовлетворительно – «3»
65%-84%	Хорошо – «4»
85%-100%	Отлично – «5»