МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«ХЕРСОНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
(ФГБОУ ВО «ХТУ»)

СОГЛАСОВАНО:
Начальник учебно-методического управления
_____ П.В. Молчанов
«__» 05 2025 г.

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «ХТУ»
_____ Г.А. Райко
«__» 05 2025 г.

# ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
# ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ
# 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Квалификация (степень)
Магистр

Форма обучения:
очная

Геническ, 2025

Программа содержит описание формы вступительных испытаний, перечень вопросов для вступительных испытаний и список литературы, рекомендуемой для подготовки.

Прием осуществляется на конкурсной основе по результатам вступительных испытаний.

## 1. ЦЕЛЬ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Вступительные испытания призваны определить степень готовности поступающего к освоению основной образовательной программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность.

## 2. ФОРМА ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Вступительные испытания проводятся в форме тестирования в соответствии с установленным приемной комиссией ХТУ расписанием.

Поступающему предлагается ответить письменно на 50 вопросов в виде тестов, охватывающих содержание разделов и тем программы соответствующих вступительных испытаний.

На ответы по вопросам и задачам билета отводится 120 минут. Результаты испытаний оцениваются по стобалльной шкале.

## 3. ОЦЕНКА РЕЗУЛЬТАТОВ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Тесты состоят из 50 заданий, примерно, одинаковых по сложности.

Закрытая форма теста применение материала по известным стандартным алгоритмам и образцам, то есть предоставляются задания с выбором одного ответа из нескольких вариантов ответов, один из которых правильный. Каждое задание оценивается в 2 балла.

Суммарно максимальное количество - 100 баллов.

Минимальное количество баллов – 60.

## 4. ПЕРЕЧЕНЬ ТЕМ ДЛЯ ПОДГОТОВКИ К ТЕСТИРОВАНИЮ ПО НАПРАВЛЕНИЮ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ":

**Тема 1. Основы компьютерной архитектуры и безопасности**: базовые компоненты компьютера (процессор, память, накопители), их функции и взаимодействие; уязвимости на программном уровне и методы их устранения.

**Тема 2. Принципы работы компьютерных сетей и сетевая безопасность**: основы сетевых протоколов, топологии сетей, модель OSI, типичные сетевые атаки и способы защиты от них.

**Тема 3. Операционные системы и их защита**: классификация и назначение операционных систем, механизмы безопасности в ОС, настройка прав доступа, обновления безопасности.

**Тема 4. Основы криптографии и шифрования данных**: симметричное и асимметричное шифрование, хеширование, цифровые подписи. Применение криптографии для защиты информации.

**Тема 5. Управление доступом и аутентификация пользователей**: методы аутентификации, авторизации и учета, политики паролей, многофакторная аутентификация, управление идентификацией.

**Тема 6. Защита персональных данных и конфиденциальность**: принципы обработки персональных данных, методы их защиты. Законодательные требования к обработке персональных данных.

**Тема 7. Угрозы информационной безопасности и методы защиты**: классификация киберугроз, вредоносное ПО, социальная инженерия. Комплексные методы защиты информации в организации.

**Тема 8. Правовые аспекты информационной безопасности**: основные законы и нормативные акты в сфере информационной безопасности, ответственность за киберпреступления, защита интеллектуальной собственности.

## 5. ПЕРЕЧЕНЬ ВОПРОСОВ ПО ПРЕДЛОЖЕННЫМ ТЕМАМ

**Основы компьютерной архитектуры и безопасности**

Какой компонент компьютера отвечает за выполнение арифметических и логических операций?

Как называется и какие функции выполняет быстрая память, расположенная между процессором и оперативной памятью?

Какие существуют типы типами оперативной памяти?

Что такое BIOS и UEFI, их назначение и отличие?

Какие существуют типы накопителей информации, в чем заключается отличие твердотельных накопителей от механических жестких дисков?

Что такое порт в контексте компьютерной архитектуры, сколько используется портов в современных операционных системах, назовите наиболее часто используемые порты в серверных операционных системах?

Что такое технология Secure Boot?

**Принципы работы компьютерных сетей и сетевая безопасность**

Что из себя представляет модель OSI?

Какой уровень модели OSI отвечает за маршрутизацию пакетов?

Какие протоколы работают на транспортном уровне модели OSI?

Что такое MAC-адрес, для он чего нужен, чем отличается от IP адреса?

Что такое файрвол (брандмауэр)?

Какой протокол используется для безопасной передачи данных через интернет?

Для чего используется протокол FTP?

Что такое NAT (Network Address Translation)?

Какие существуют типы сетевого кабеля?

Что такое ARP-спуфинг?

Для чего применяется протокол DHCP?

Что такое VPN (Virtual Private Network)?

**Операционные системы и их защита**

Какие операционные системы вы знаете, приведите классификацию операционных систем, архитектурные различия, достоинства и недостатки.

Какие основные функции выполняют операционные системы?

Какие типы операционных систем существуют?

Что такое виртуализация в контексте операционных систем?

Какие механизмы безопасности обычно присутствуют в современных ОС?

Что такое UAC (User Account Control) в Windows?

Какие права доступа к файлам обычно можно настроить в Unix-подобных системах?

Что такое "песочница" (sandbox) в контексте безопасности ОС?

Какие действия рекомендуется выполнять для поддержания безопасности ОС?

Какие меры могут помочь защитить ОС от атак типа "повышение привилегий"?

**Основы криптографии и шифрования данных**

Что такое симметричное шифрование?

Что такое асимметричное шифрование?

Что такое хеширование, для чего применяется, основные алгоритмы?

Что такое цифровая подпись?

Какие преимущества имеет асимметричное шифрование перед симметричным?

Какой алгоритм используется в протоколе HTTPS для обмена ключами?

Какие алгоритмы шифрования используются в протоколе VPN?

**Управление доступом и аутентификация пользователей**

Какие существуют методы многофакторной аутентификации пользователей?

Какие существуют методы для авторизации пользователей?

Какие пароли можно считать безопасными, что такое политика управления паролями?

Какие методы можно использовать для управления идентификацией пользователей?

Какие факторы увеличивают стойкость паролей к подбору?

Какие методы аутентификации считаются биометрическими?

**Защита персональных данных и конфиденциальность**

Что относится к персональным данным согласно законодательству?

Какие принципы обработки персональных данных существуют?

Что такое псевдонимизация персональных данных?

Какие методы защиты персональных данных существуют?

Что такое согласие на обработку персональных данных?

Какие права имеет субъект персональных данных?

Какие меры должен принять оператор персональных данных для обеспечения их безопасности?

Что такое трансграничная передача персональных данных?

Какие санкции могут быть применены за нарушение законодательства о персональных данных?

**Угрозы информационной безопасности и методы защиты**

Что такое социальная инженерия, в контексте информационной безопасности?

Что такое фишинг?

Какой тип вредоносного програмного обеспечения предназначен для шифрования данных жертвы с целью вымогательства?

С помощью каких мер могут помочь защитить организацию от фишинговых атак?

Какие угрозы информационной безопасности относятся к категории внутренние угрозы?

Какие существуют комплексные методы защиты информации в организации?

Какие из следующих типов вредоносного ПО могут распространяться без участия пользователя?

Какие меры могут быть эффективны для предотвращения атак типа «человек посередине» (MITM)?

Какие виды вредоносного программного обеспечения предназначены для скрытия своего присутствия в системе?

Какие меры помогут защитить организацию от атак типа DDoS?

**Правовые аспекты информационной безопасности**

Какие существуют международные нормативные акты, по защите персональных данных?

Какие существуют виды киберпреступлений, какие из них могут повлечь уголовную ответственность?

Какие действия считаются нарушением авторских прав?

Какие действия могут рассматриваться как кибершпионаж?

Какие виды ответственности могут наступить за киберпреступления?

Какие меры нужно предпринять для защиты интеллектуальной собственности в интернете?

Какие существуют российские нормативные акты, по защите персональных данных?

## Рекомендуемая литература

Базы данных, информационно-справочные системы

1. Российская государственная библиотека www.rsl.ru
2. Российская национальная библиотека www.nlr.ru
3. Библиотека Академии наук www.rasl.ru
4. Библиотека по естественным наукам РАН www.benran.ru
5. Всероссийский институт научной и технической информации (ВИНИТИ) www.viniti.ru
6. Государственная публичная научно-техническая библиотека www.gpntb.ru elibrary.ru