Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»

ПРОГРАММА

вступительных испытаний при поступлении в магистратуру

по направлению 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

на факультет
КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

Магистерская программа:

10.04.01.02 - Безопасность объектов критической информационной инфраструктуры нефтегазового комплекса

Москва, 2019 г.

ПРОГРАММА
вступительных испытаний в магистратуру
по направлению 10.04.01 – Информационная безопасность
программа 10.04.01.02 «Безопасность объектов критической информационной инфраструктуры нефтегазового комплекса»

Введение

Программа вступительных испытаний в магистратуру по направлению 10.04.01 «Информационная безопасность» составлена на основании полученных абитуриентом компетенций при изучении направления 10.03.01 «Информационная безопасность» (уровень – бакалавр).

Вступительное испытание в магистратуру предназначено для определения теоретической и практической подготовленности поступающего.

1. Требования к вступительному испытанию

Вступительное испытание представляет собой письменный экзамен или собеседование.

Экзамен предусматривает письменные ответы на 2 вопроса из числа представленных в настоящей программе.

Собеседование, по решению экзаменационной комиссии, может сочетать в себе элементы экзамена как в устной, так и в письменной формах. Собеседование предполагает ответ на 2 вопроса из числа представленных в настоящей программе. После ответа на вопросы члены экзаменационной комиссии могут задать уточняющие или дополнительные вопросы, не выходящие за рамки содержания экзаменационных вопросов.

На вступительном испытании поступающий в магистратуру должен подтвердить свои знания в области общих изученных дисциплин направления подготовки 10.04.01 «Информационная безопасность» (уровень магистратуры), достаточных для обучения по магистерской программе.

Поступающий должен иметь сформированное научное мировоззрение и продемонстрировать на вступительном испытании знание и владение системой научных понятий; фактами научных теорий; методами и процедурами профессиональной деятельности.

Объявление итогов вступительного испытания происходит в соответствии с Положением «О порядке приема на 1-й курс магистратуры РГУ нефти и газа (НИУ) имени И.М. Губкина».

Образцы билетов для вступительных испытаний в магистратуру приведены в Приложении 1.

2. Перечень основных учебных модулей (дисциплин, разделов), выносимых на вступительный экзамен

К поступающим на программу подготовки магистров по направлению 10.04.01 «Информационная безопасность» предъявляются требования к освоению программ следующих учебных дисциплин: Теория информации, Теория вероятностей и математическая статистика, Технологии программирования, (алгоритмы и структуры данных), Базы данных и экспертные системы, Теория информационной безопасности, основы криптографической и стеганографической защиты информации, технические каналы утечки информации, защита информации от несанкционированного доступа, защита от вредоносного программного обеспечения, Сетевая безопасность, Комплексные системы зашиты информации, организационное и правовое обеспечение информационной безопасности.

3. Вопросы к экзамену для поступления в магистратуру

Теория информации

1. Понятие информации. Жизненный цикл информации.
2. Количество информации и энтропия. Формулы Хартли и Шеннона.
3. Математические модели каналов связи. Помехоустойчивость каналов.
4. Типы сигналов, их дискретизация и восстановление.
5. Сжимающее и помехоустойчивое кодирование информации

Теория вероятностей и математическая статистика

1. Случайные величины, функции распределения, их свойства.
2. Типовые распределения: биномиальное, пуассоновское, нормальное.
3. Схема Бернулли и полиномиальная схема.
4. Независимость событий. Условные вероятности, формулы Байеса.
5. Математическое ожидание и дисперсия случайной величины.

6. Цепи Маркова, их свойства.

7. Задача проверки статистических гипотез. Статистические критерии. Ошибки 1-го и 2-го родов при проверке гипотез. Метод статистических испытаний.

8. Оценка результатов измерений. Точечные оценки и их определение. Надёжность оценки, доверительная вероятность и доверительный интервал.

Технологии программирования, алгоритмы и структуры данных

1. Жизненный цикл программного обеспечения. Тестирование программ.
2. Параллельные методы программирования.
3. Основные алгоритмы поиска данных, их временная сложность.
4. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных.
5. Временная сложность алгоритмов. Оценка времени выполнения программ.
6. Основные абстрактные типы данных: списки, стеки, очереди, деревья, ориентированные и неориентированные

Базы данных и экспертные системы

1. Основные понятия: определение данных, системы баз данных.
2. Основные этапы проектирования баз данных.
3. Представление статических и динамических свойств реального мира.
4. Базовые структурные компоненты модели данных: домены и атрибуты, отношение сущности, схема отношения.
5. Общая характеристика ограничений целостности. Уровни абстракции представления данных.
6. Информация о сущностях и связях.
7. Типы ограничений целостности. Реляционная модель данных.
8. Средства языка SQL как языка описания данных. Описание структуры и ограничений целостности (предложение CREATE TABLE).

9. Формирование запросов. Предложение SELECT.

10. Проектирование реляционных баз данных: возникающие проблемы, основные цели проектирования.

11. Функциональные зависимости. Определение ключа.

12. Назначение и суть индексирования.

13. Структуры типа двоичное дерево, многоходовое дерево. Методы доступа к данным в БД. Структуры типа B-дерево.

14. Информационно-аналитические и экспертные системы обеспечения информационной безопасности.

Теория информационной безопасности

1. Место проблем защиты информации в общей совокупности информационных проблем современного общества.

2. Информационное противоборство в современных условиях

3. Определение информационной безопасности, защиты информации.

4. Постановка задачи защиты информации. Современные задачи защиты информации.

5. Риски информационной безопасности. Уязвимости информационных систем.

6. Системная классификация угроз безопасности информации.

Основы криптографической и стеганографической защиты информации

1. Обеспечение секретности, подлинности, целостности, неотказуемости от авторства с помощью криптографических методов.

2. Определение криптографической системы, виды криптосистем.

3. Базовые криптографические примитивы. Шифры перестановки и замены.

4. Блочные и поточные шифры.

5. Вычислительно сложные задачи и однонаправленные функции, используемые в криптографии.

6. Электронная цифровая подпись.

7. Криптографические хэш-функции.
8. Понятие о криптографическом протоколе. Свойства протокола.
9. Компьютерная стеганография и ее возможности для защиты информации
10. Цифровые водяные знаки и защита авторских прав цифрового мультимедийного контента.

Технические каналы утечки информации

11. Построение модели технических каналов утечки информации и оценка возможностей нарушителя по их использованию.
12. Технические каналы утечки акустической и речевой информации. Основные характеристики.
13. Технические каналы утечки информации при передаче по каналам связи. Основные характеристики.
14. Технические каналы утечки информации средств вычислительной техники. Основные характеристики.
15. Технические каналы утечки видовой информации. Основные характеристики.
16. Противодействие комплексному использованию технических каналов утечки информации нарушителем.

Защита информации от несанкционированного доступа

1. Методы идентификации и аутентификации, общая характеристика функции аутентификации.
2. Методы реализации контроля и разграничения доступа.
3. Функции контроля и разграничения доступа.
4. Модель нарушителя доступа при защите автоматизированных систем от несанкционированного доступа.
5. Методы контроля защищенности автоматизированных систем от несанкционированного доступа.

6. Аппаратно-программные средства защиты информации от несанкционированного доступа.
7. Возможности биометрических систем для обеспечения защиты от НСД

Защита от вредоносного программного обеспечения.

1. Общее описание компьютерных вирусов. Видовая классификация компьютерных вирусов.
2. Методы и средства антивирусной защиты.
3. Организационно-правовые методы защиты от вирусов
4. Защита от вирусов в статике процессов.
5. Защита от вирусов в динамике процессов.
6. Антивирусная политика на объекте информатизации.
7. Основные направления антивирусной борьбы в компьютерных и телекоммуникационных системах.
8. Основные механизмы внедрения компьютерных вирусов в поражаемую систему.

Сетевая безопасность

1. Понятия интранета, экстранета и портала.
2. Угрозы ИБ их ресурсам. Специфика информационной безопасности в сетях.
3. Политика обеспечения безопасности для сетей. Обеспечение конфиденциальности, целостности, доступности, аутентичности, неотказуемости, учетности и надежности в сетевой среде.
4. Программно-аппаратные средства обеспечения ИБ в сетях.
5. Уязвимости и угрозы информационной безопасности в сетевой среде.
6. Удаленные атаки на сетевые ресурсы. Средства реализации атак. Примеры.
7. Аутентификация в сетях.
8. Уязвимости, угрозы и средства защиты в интернете.

9. Способы адресации в сетях. Управление потоками. Маршрутизация пакетов

Комплексные системы зашиты информации

1. Системный подход при комплексной защите информации.
2. Объект защиты. Системность и комплексность защиты информации.
3. Макроструктурные компоненты комплексной системы зашиты информации (функциональные и обеспечивающие подсистемы). Подсистемы обеспечения информационной безопасности.
4. Процессный подход к обеспечению информационной безопасности.
5. Политики обеспечения информационной безопасности.
6. Управление информационной безопасностью.
7. Информационная безопасность в аспекте управления персоналом.
8. Организационно-правовые меры защиты информации в корпоративных информационных системах.

Организационное и правовое обеспечение информационной безопасности

1. Основные положения Доктрины информационной безопасности Российской Федерации.
2. Стратегия национальной безопасности Российской Федерации.
3. Государственная система защиты информации и ее структура.
4. Лицензирование, сертификация и аттестация в области защиты информации.
5. Основные положения закона РФ «Об информации, информационных технологиях и о защите информации», закона РФ «О персональных данных».
6. Основные положения Федеральных Законов РФ «О государственной тайне», «О коммерческой тайне».
7. Основные положения закона РФ 187 «О комплексной безопасности критической информ инфраструктуры» (уточнить правильное название)

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

4. Рекомендованная литература

Нормативные акты

1. Конституция Российской Федерации. [Электронный документ]. Режим доступа: URL: http://base.consultant.ru/cons/cgi/online.cgi
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный документ]. Режим доступа: URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#
3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [Электронный документ]. Режим доступа: URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#
4. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”
5. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: http://www.27000.org/
6. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
7. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
8. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
9. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной

безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

Основная литература

1. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А.А. – М. Горячая линия-Телеком, 2004. – 280 с.
2. Этика в сфере информационных технологий / Малюк А.А., Полянская О.Ю., Алексеева И.Ю. – М.: Горячая линия – Телеком, 2011 – 344 с. URL: http://iprbookshop.ru/6991.html.
3. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М. Горячая линия-Телеком, 2014. – 244 с.
4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: (Высшее образование) ISBN 978-5-369-01450-9.
5. Шустова Лариса Ивановна Шустова Л.И. Базы данных : учебник / Л.И. Шустова, О.В. Тараканов. — М. : ИНФРА-М, 2017. — 304 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/11549.
6. Комплексная система защиты информации на предприятии / Грибунин В.Г - М.: Академия, 2009.
7. Математические и компьютерные основы криптологии / Харин Ю.С.- М.: Новое знание, 2008.
8. Организация комплексной системы защиты информации / Гришина Н.В - М.: Гелиос АРВ, 2007.
9. Инженерно-техническая защита информации / Торокин А.А. -М.: Аспект Пресс, 2006.
10. Основы защиты информации: Учебное пособие / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов .-М.: Издательский центр «Академия», 2006.
11. Защита информации в телекоммуникационных системах / Коханович Г.Ф. и др. - М.: Пресс, 2005.
12. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации (Учебное пособие) / Горбатов В.С., Дворянкин С.В., Дураковский А.П., Енгалычев Р.С. и др. Под общей редакцией Лаврухина Ю.Н. - М: НИЯУ МИФИ, 2014. -560 с.

13. Введение в информационную безопасность (Учебное пособие) / Горбатов В.С., Дураковский А.П., и др. – М. Горячая линия – Телеком 2014.
14. Семь безопасных информационных технологий / Марков А.С. и др. 2017

Дополнительная литература

1. Безопасность глобальных сетевых технологий / Игнатов В.Г. - СПб.: Питер, 2007.
2. Методы и средства защиты информации в компьютерных системах / Хорев П.Б. - М.: Академия, 2006.
3. Защита информации в системах мобильной связи / Чекалин А. А.- М.: Горячая линия- Телеком, 2005.
4. Дискретная математика и криптология / Фомичев В.М.. 2-е изд. -М,: ДИАЛОГ-МИФИ, 2009.
5. Комплексная защита информации в корпоративных системах / Шаньгин В.Ф. - М.: ИД Форум: НИЦ Инфра-М, 2012.
6. Теория информации / Духнин А.А. - М.: Гелиос, 2008.
7. Информационная безопасность / Ярочкин В. И. - М.: Академия - проспект, 2006.
8. Основы информационной безопасности / Белов Е.Б. - М.: Горячая линия-Телеком, 2006.
9. Защита компьютерной информации от несанкционированного доступа / Щеглов Ю.А. - М.: Наука и техника, 2004.
10. Теоретико-числовые методы в криптографии / Маховенко Е.Б. - М.: Гелиос, 2006.

Декан факультета КБ ТЭК С.Н. Гриняев

Приложение 1

Образцы билетов для вступительных испытаний в магистратуру

РГУ НЕФТИ И ГАЗА (НИУ) ИМЕНИ И.М. ГУБКИНА

Кафедра комплексной безопасности
критически важных объектов

НАПРАВЛЕНИЕ **10.04.01 Информационная безопасность**
ПРОГРАММА **10.04.01.02 Безопасность объектов критической информационной инфраструктуры нефтегазового комплекса**
ДИСЦИПЛИНА **Вступительные испытания в магистратуру**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Понятие информации. Жизненный цикл информации.
2. Базовые структурные компоненты модели данных: домены и атрибуты, отношение сущности, схема отношения.

РГУ НЕФТИ И ГАЗА (НИУ) ИМЕНИ И.М. ГУБКИНА

Кафедра комплексной безопасности
критически важных объектов

НАПРАВЛЕНИЕ **10.04.01 Информационная безопасность**
ПРОГРАММА **10.04.01.02 Безопасность объектов критической информационной инфраструктуры нефтегазового комплекса**
ДИСЦИПЛИНА **Вступительные испытания в магистратуру**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Жизненный цикл программного обеспечения. Тестирование программ.
2. Базовые криптографические примитивы. Шифры перестановки и замены.

РГУ НЕФТИ И ГАЗА (НИУ) ИМЕНИ И.М. ГУБКИНА

Кафедра комплексной безопасности
критически важных объектов

НАПРАВЛЕНИЕ **10.04.01 Информационная безопасность**
ПРОГРАММА **10.04.01.02 Безопасность объектов критической информационной инфраструктуры нефтегазового комплекса**
ДИСЦИПЛИНА **Вступительные испытания в магистратуру**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3

1. Случайные величины, функции распределения, их свойства.
2. Риски информационной безопасности. Уязвимости информационных систем.