КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ им. АЛЬ-ФАРАБИ

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Утверждено на заседании
Научно-методического совета
КазНУ им. аль-Фараби
протокол №_____
от «_____» _____2020 г.

ПРОГРАММА
ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОСТИ

ДЛЯ ПОСТУПАЮЩИХ В ДОКТОРАНТУРУ PhD ПО СПЕЦИАЛЬНОСТИ
«8D06301 – Системы информационной безопасности»
(для 3 годич.)

АЛМАТЫ 2020

Программа составлена в соответствии с Государственным общеобразовательным стандартом по специальности «8D06301 – Системы информационной безопасности». Программа составлена и.о. доцента Мусиралиевой Ш.Ж.

Программа рассмотрена на заседании кафедры Информационных систем
Протокол № ____ « ____ » _____ 2020г.

Зав.кафедрой _____ Мусиралиева Ш.Ж.

Одобрено на заседании методбюро факультета информационных технологий
Протокол № ____ « ____ » _____ 2020 г.

Председатель методбюро _____ Гусманова Ф.Р.

Утверждена на заседании Ученого совета
Протокол № ____ « ____ » _____ 2020 г.
Председатель Ученого совета,
декан факультета _____ Урмашев Б.А.

Ученый секретарь _____ Самбетбаева А.К.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Цели и задачи вступительного экзамена по специальности

1.1. Цель вступительного экзамена по специальности

Целью вступительного экзамена является выявление уровня теоретической подготовки, поступающих в докторантуру и формирование персональной рекомендации по поступлению на основе конкурсного участия.

Программа вступительного экзамена включает дисциплины: «Организация систем информационной безопасности», «Методы и средства защиты компьютерной информации», «Элементы средств защиты информации»

1.2. Задачи вступительного экзамена по специальности

В ходе экзамена выявляются:

- Знание абитуриентом фундаментальных основ информатики и информационных технологий; основные достижения и тенденции развития современной информатики; технологии профессиональной и научной деятельности; знание основных положений профессиональной и научной этики и использование их в трудовой деятельности.
- Умение находить, анализировать и обрабатывать научно-техническую, естественнонаучную и общенаучную информацию, приводя ее к проблемно-задачной форме; проектировать и осуществлять свою профессиональную, научную и научно-педагогическую деятельность; проектировать свое дальнейшее профессиональное развитие.
- Навыки самостоятельной научно-исследовательской работы и научно-изыскательной работы; научной проектной деятельности, решения стандартных научных и профессиональных задач, правильного и логичного оформления своих мыслей в устной и письменной форме.

2. Требования к уровню подготовки лиц, поступающих в докторантуру PhD

Предшествующий уровень образования:
академическая степень магистра по специальностям:
6М070300 – Информационные системы
6М100200 – Системы информационной безопасности
6М060200 – Информатика
6М011100 – Информатика
6М070200 – Автоматизация и управление
6М070400 – Вычислительная техника и программное обеспечение
6М060300 – Механика
6М070500 – Математическое и компьютерное моделирование
6М060100 – Математика
6М071900 – Радиотехника, электроника и телекоммуникации

Поступающий должен иметь документ государственного образца соответствующего уровня образования.

Программа вступительного экзамена для поступающих в докторантуру по направлению подготовки «8D06301 – Системы информационной безопасности» разработана на кафедре «Информационные системы».

3. Пререквизиты образовательной программы

Пререквизиты:

1. Организация систем информационной безопасности;
2. Методы и средства защиты компьютерной информации;
3. Элементы средств защиты информации.

4. Перечень экзаменационных тем

Дисциплина «Организация систем информационной безопасности»

1. Классические шифры и их вскрытие. Шифр сдвига и афинный шифр и их дешифрование и взлом методом перебора. Частотный метод вскрытия шифра замены. Недостатки классических шифров, частотный анализ таких шифров текстов на казахском и русском языках.
2. Кольцо целых чисел, алгоритм Евклида и следствия. Представление наибольшего общего делителя. Теория сравнений. Свойства сравнений по данному модулю. Обратимые элементы по данному модулю.
3. Функция Эйлера и ее свойства. Функция Эйлера на простых числах. Теорема о мультипликативности функции Эйлера. Формула нахождения значений функции Эйлера, возведение в степень с использованием функции Эйлера.
4. Теорема Ферма-Эйлера и основная теорема RSA-шифра.
5. RSA-шифр, процесс шифрования и чтения, обоснование. RSA-шифрование открытым ключем заданного текста. RSA-дешифрование закрытым ключем заданного текста.
6. RSA-электронная подпись, идея и обоснование.
7. Реализация процедуры RSA-электронной подписи, часть подписывания электронной подписью документа.
8. Реализация процедуры RSA-электронной подписи, часть шифрование подписи открытым ключом.
9. Распределение простых чисел в натуральном ряду и оценка RSA шифра.
10. Кольцо многочленов над полем $< F_2 ; +,* >$ алгоритм Евклида, представление наибольшего общего делителя двух многочленов. Неприводимые многочлены в этом кольце. Неприводимые многочлены степеней 2,3,4,5.
11. Конструкция поля $< F_2^n ; +,* >$ как поля построенного из остатков по модулю неприводимого многочлен. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению для ненулевых элементов этого поля. Построить поле $< F_{16} ; +, * >$.
12. Теорема Лагранжа о делимости порядка группы на порядок подгруппы. Следствия о том, что порядок элемента делит порядок группы. Примеры подгрупп группы Zn. Теорема о первообразном элементе в поле $< F_{2n} ; +,* >$. Первообразные элементы поля $< F_{16} ; +,* >$.
13. Конструкция поля, построенного из n-разрядных двоичных блоков. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению для ненулевых элементов этого поля, первообразные элементы этого поля. Построить поле 4-разрядных двоичных блоков, указать первообразные элементы этого поля.
14. Задача Дифи-Хеллмана. Создание общего секрета для удаленных пользователей, опираясь на «неразрешимость» задачи Дифи-Хеллмана. Решение проблемы обмена ключами для удаленных пользователей.
15. Шифр Эль-Гамаля, прецесс обмена ключами, шифрование и дешифрования. Реализация на примере.

Список рекомендуемой литературы

Основная:

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2010. – 381 с.
2. Черёмушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2012.
3. Кормен Т., Лейзер Ч., Риверс Р. АЛГОРИТМЫ: построение и анализ. М.: МЦНМО, 2010. – 900 с.
4. А. П. Алферов т.б. Основы криптографии. Москва, «Гелиос АРВ», 2002 ж.
5. В. И. Нечаев, ЭЛЕМЕНТЫ КРИПТОГРАФИИ. Основы защиты информации. М., Высшая школа, 1999 г.

Дополнительная:

1. А. А. Бухштаб. Основы теории чисел. М.: Просвещение, 1966.
2. D. R. Stinson. KRIPTOGRAPHY, Teory and Practice. CRC Press, Boca Raton, 1995.

Дисциплина «Методы и средства защиты компьютерной информации»

1. Краткие исторические сведения о возникновении и развитии методов криптологии. Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.
2. Модель Белла-Лападулы. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения секрета. Инфраструктура открытых ключей. Сертификаты. Центры сертификации. Формальные модели шифров. Модели открытых текстов. Математические модели открытого текста. Критерии распознавания открытого текста. Классификация шифров по различным признакам. Математическая модель шифра замены. Классификация шифров замены.
3. Модель Low-Water-Mark (LWM). Маршрутные перестановки. Элементы криптоанализа шифров перестановки. Шифры замены.
4. Модели J. Goguen, J. Meseguer. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Криптоанализ шифра Виженера. Ошибки шифровальщика.
5. Модель выявления нарушения безопасности. Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений. Шифры, не распространяющие искажений типа "замена знаков. Шифры, не распространяющие искажений типа "пропуск-вставка знаков.
6. Блочные системы шифрования. Принципы построения блочных шифров. Примеры блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Режимы использования блочных шифров. Комбинирование алгоритмов блочного шифрования. Методы анализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.
7. Поточные системы шифрования. Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем. Шифрсистема A5. Шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа—Месси. Усложнение линейных рекуррентных последовательностей. Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти. Методы анализа поточных шифров.
8. Управление безопасностью. Стандарты, аудит безопасности. Особенности речевых сигналов. Скремблирование. Частотные преобразования сигнала. Временные преобразования сигнала. Стойкость систем временных перестановок. Системы цифровой телефонии.
9. Системы шифрования с открытыми ключами. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе "проблемы рюкзака".
10. Идентификация. Правила составления паролей. Усложнение процедуры проверки паролей. "Подсоленные" пароли. Парольные фразы. Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли. «Запрос-ответ» (сильная идентификация). "Запрос-ответ" с использованием симметричных алгоритмов шифрования. "Запрос-ответ" с использованием асимметричных алгоритмов шифрования. Протоколы с нулевым разглашением. Атаки на протоколы идентификации.

11. Криптографические хэш-функции. Функции хэширования и целостность данных. Ключевые функции хэширования. Бесключевые функции хэширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хэширования.
12. Цифровые подписи. Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.
13. Протоколы распределения ключей. Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей. Открытое распределение ключей. Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета. Способы установления ключей для конференцсвязи. Возможные атаки на протоколы распределения ключей.
14. Управление ключами. Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.
15. Некоторые практические аспекты использования шифрсистем. Анализ потока сообщений. Ошибки операторов. Физические и организационные меры при использовании шифрсистем. Квантово-криптографический протокол открытого распределения ключей. Квантовый канал и его свойства. Протокол открытого распределения ключей.

Список рекомендуемой литературы

Основная:

1. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.
3. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.
4. Василенко О.Н. Современные способы проверки простоты чисел. Обзор // Кибернетич. сборн. 1988. Вып. 25. С. 162-188.
5. Гашков С. Б. Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. 1998. Т. 10 (4). С. 35—38.
6. Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. М.: Мир, 1991.
7. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М. – СПб. – Киев, 2000. 3-е издание.
8. Кострикин А.И. Введение в алгебру. М.: Наука, 1977.
9. Нечаев В.И. Элементы криптографии. М.: Высшая школа, 1999.
10. Ноден П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999.
11. Панкратьев Е.В. Компьютерная алгебра. Факторизация многочленов. М.: Изд-во МГУ, 1988.

Дополнительная:

1. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.
2. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.
3. Гантмахер Ф. Р. Теория матриц. М., 1954.
4. Касселс Дж. Введение в геометрию чисел. М.: Мир, 1965.
5. Ленг С. Введение в теорию диофантовых приближений. М.: Мир, 1970.
6. Ленг С. Эллиптические функции. М.: Наука, 1984.
7. Чебышев П.Л. Полное собрание сочинений. Т. 1. Теория чисел. Изд-во АН СССР, 1946.
8. Чистов А.Л. Алгоритм полиномиальной сложности для разложения многочленов и нахождения компонент многообразия в субэкспоненциальное время // Зап. науч. семин. ЛОМИ АН СССР. 1984. №137. с. 124-188.

Дисциплина «Элементы средств защиты информации»

1. Компьютерная система (КС). Основные понятия. Электронный документ (ЭД). Виды информации в КС.
2. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД.
3. Политика безопасности в компьютерных системах. Понятие политики безопасности и её основные базовые представления. Оценка защищенности
4. Идентификация пользователей КС-субъектов доступа к данным. Задача идентификации пользователя. Понятие протокола идентификации. Понятие идентифицирующей информации
5. Средства и методы ограничения доступа к файлам. Основные подходы к защите данных от НСД. Способы фиксации фактов доступа. Журналы доступа.
6. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Надежность систем ограничения доступа. Подход на основе формирования хэш-функции, требования к построению и способы реализации.
7. Программно-аппаратные средства шифрования. Построение программно-аппаратных комплексов шифрования. Проектирование модулей криптопреобразований на основе сигнальных процессоров.
8. Методы и средства ограничения доступа к компонентам ЭВМ. Компоненты ПЭВМ. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
9. Защита программ от несанкционированного копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.
10. Хранения ключевой информации. Пароли и ключи. Секретная информация, используемая для контроля доступа: ключи и пароли.
11. Управление криптографическими ключами. Генерация ключей. Распределение ключей.
12. Протокол аутентификации распределения ключей для симметричных криптосистем. Основные понятия и определения, типы криптографических протоколов, примеры.
13. Протокол для ассиметричных криптосистем с использованием сертификатов открытых ключей.
14. Организация хранения ключей (с примерами реализации). Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство TouchMemory.
15. Защита программ от изучения. Изучение и обратное проектирование ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение.

СПИСОК ЛИТЕРАТУРЫ

Основной:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.
2. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с. – (Сер. “Администрирование и защита”).
3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.
5. Столлингс В. Операционные системы. М.: Издательский дом «Вильямс», 2014. – 848 с.

Дополнительный:

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.
2. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
4. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010 – 784 с.

ШКАЛА ОЦЕНКИ РЕЗУЛЬТАТОВ ЭКЗАМЕНА

Ответ абитуриента оценивается на **«отлично»,** когда он демонстрирует полное понимание принципов организации систем информационной безопасности, умение использовать методы и средства защиты компьютерной информации, элементы средств защиты информации, понимание основных достижений и тенденций развития современной IT технологий в области защиты информации, технологий педагогической и научной деятельности. Абитуриент должен уметь четко, ясно и логично выражать свои мысли в письменной форме и устной речи; уметь применять полученные знания к решению практических задач; рассуждать и делать логические выводы.

Ответ абитуриента оценивается на **«хорошо»,** когда он демонстрирует значительное понимание принципов организации систем информационной безопасности, умение использовать методы и средства защиты компьютерной информации, элементы средств защиты информации, понимание основных достижений и тенденций развития современной IT технологий в области защиты информации, технологии педагогической и научной деятельности. Поступающий должен уметь четко, ясно и логично выражать свои мысли в письменной форме и устной речи; уметь применять полученные знания к решению практических задач; рассуждать и делать логические выводы.

Ответ поступающего оценивается на **«удовлетворительно»,** когда ответ свидетельствует о наличии ограниченного понимания принципов организации систем информационной безопасности, умения использовать методы и средства защиты компьютерной информации, элементы средств защиты информации, ограниченного понимания основных достижений и тенденций развития современной IT технологий в области защиты информации, технологии педагогической и научной деятельности. Не умеет четко, ясно и логично выражать свои мысли в письменной форме и устной речи; умеет применять полученные знания к решению практических задач; умение рассуждать и делать логические выводы.

Ответ поступающего оценивается на **«неудовлетворительно»,** когда ответ свидетельствует о полном отсутствии понимания принципов организации систем информационной безопасности, умения использовать методы и средства защиты компьютерной информации, элементы средств защиты информации, отсутствии понимания основных достижений и тенденций развития современной IT технологий в области защиты информации, технологии педагогической и научной деятельности. Не умеет четко, ясно и логично выражать свои мысли в письменной форме и устной речи; не умеет применять полученные знания к решению практических задач; неумение рассуждать и делать логические выводы.