МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

ИННОВАЦИОННЫЙ ЕВРАЗИЙСКИЙ УНИВЕРСИТЕТ

Научно-образовательный комплекс

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

по дисциплине «Системы компьютерной безопасности»
(СИЛЛАБУС)

ПАВЛОДАР 2013 ГОД

УТВЕРЖДАЮ
Директор Инженерной Академии
д.х.н., профессор_____А.К. Свидерский

“___” _____ 2013 г.

Автор: к.т.н., профессор Р.А. Шагиева _____

Кафедра «Математика и информационные технологии»

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Силлабус
по дисциплине Системы компьютерной безопасности

для магистрантов технических специальностей
очной формы обучения

Курс	2
Семестр	3
Количество кредитов	3
Лекции	15
Лабораторные работы	30
СРМП	15
СРМ	165
Всего	225
Форма контроля	экзамен

Разработан на основании Рабочей учебной программы и каталога Элективных дисциплин к базовому учебному плану специальности 6М0704 «Вычислительная техника и программное обеспечение».

Утвержден на заседании научно-методического совета Инженерной Академии и рекомендован к изданию
Протокол №___ от _____2013 г.

Председатель НМС Инженерной Академии
к.т.н., профессор ИнЕУ _____П.В. Дубровин

Рассмотрен на заседании кафедры «Математика и информационные технологии»
Протокол №___ от _____2013 г.

Зав. кафедрой «Математика и информационные технологии»
К.т.н., доцент _____ Ж.К.Даниярова

Начальник ИМО
к.п.н., проф._____Н.М.Ушакова

Контактная информация:

Ф.И.О. Преподавателя	Время и место проведения		Контактная информация
	Лекции	СРМП	
Роза Абдуллаевна Шагиева профессор кафедры «Математика и информационные технологии»	К-1 Аудитория согласно расписанию	К-1 Аудитория согласно расписанию	Кафедра «Математика и информационные технологии», К-1, кабинет 308 Тел. раб. 34-56-78, (внутр. 213) Время консультации: согласно графику консультаций на кафедре

Структура силлабуса учебного курса
«Системы компьютерной безопасности»

Пояснительная записка

Цель курса: научить магистрантов методологии построения систем защиты электронной информации, используемой при создании информационных систем.

Задачи курса:

- изучить источники и формы атак на информацию;
- изучить модели безопасности (в том числе, основных операционных систем);
- изучить разновидности вредоносных программ;
- изучить криптографические и административные методы защиты;
- изучить администрирование корпоративных и локальных сетей, методы защиты сетей и протоколов;
- изучить алгоритмы аутентификации пользователей.

Структура курса включает в себя лекции, СРМП, СРМ, экзамен.

В результате изучения курса **магистранты должны знать**:

– источники и формы атак на информацию;
– модели безопасности (в том числе, основных операционных систем);
– разновидности вредоносных программ;
– криптографические и административные методы защиты;
– администрирование корпоративных и локальных сетей, методы защиты сетей и протоколов;
– алгоритмы аутентификации пользователей.

В результате усвоения объема теоретических положений и проблем **магистранты должны уметь**:

1. использовать современные методы шифрования информации;
2. определять степень защищенности пароля доступа;
3. настраивать защиту часто используемых операционных систем;
4. определять источники и риски атак на информацию;
5. проектировать систему защиты информации на административном и техническом уровне.

В результате изучения курса **магистранты должны владеть:** методикой построения системы защиты информации.

В результате изучения курса **магистранты должны быть компетентными:** в вопросах защиты информации в компьютерных системах.

Форма контроля: экзамен.

Пререквизиты: При изучении дисциплины «Информационное обеспечение безопасности предприятий» магистранты должны опираться на знания, полученные в процессе изучения:

– «Алгоритмы и структуры данных»
– **Постреквизиты:**
– «Исследовательская практика»
– «Научно-исследовательская работа»

.

Таблица 1 - Тематико-содержательный план обучения УК (3-й семестр (15 недель))

№	Наименование и содержание УК (подтемы)	Последовательность учебных недель	Формы и содержание организации УК						Текущий контроль (ТК) следящий	Дата проведения ТК	Сроки обработки
			Лекции		Семинары (СРМП)		СРМ				
			Кол-во часов	Формы и методы организации УК	Кол-во часов	Формы и методы организации УК	Кол-во часов	Формы и методы организации УК			
Модуль 1. «Анализ безопасности информационных систем»											
6.	Современное состояние проблемы безопасности информационных систем.	1	1	Слайд-лекция	1	Индивидуальная работа	3		Устный опрос	1 неделя	В течение занятия
7.	Защита информации	2	1	Слайд-лекция	1	Индивидуальная работа	3	Реферат	Устный опрос	2 неделя	В течение занятия
8.	Безопасность информации	3	1	Слайд-лекция	1	Индивидуальная работа	3	Реферат	Устный опрос	3 неделя	В течение занятия
9.	Анализ программной и аппаратной платформы информационных систем	4	1	Слайд-лекция	1	Индивидуальная работа	3		Устный опрос	4 неделя	В течение занятия

10.	Модели безопасности информационных систем	5	1	Слайд-лекция	1	Индиви-дуальная работа	3	Самостоя-тельное изучение темы	Устный опрос	5 неделя	В течение занятия
11.	Примеры практической реализации систем защиты и безопасности	6	1	Слайд-лекция	1	Индиви-дуальная работа	3	Реферат	Устный опрос	6 неделя	В течение занятия
12.	Примеры практической реализации систем защиты и безопасности	7	1	Слайд-лекция	1	Индиви-дуальная работа	3	Оформлени е и подача работ	Устный опрос	7 неделя	В течение занятия
13.	Основные характеристики защищенной информационной системы	8	1	Слайд-лекция	1	Индиви-дуальная работа	3		Тестирова ние	8 неделя	В течение занятия
Всего часов:			8		8		24				
Промежуточный контроль (Модуль 1)											
Модуль 2. «Безопасность компьютерных систем»											
9.	Методология корректности информационной защиты	9	1	Слайд-лекция	1	Индиви-дуальная работа	3		Устный опрос	9 неделя	В течение занятия
10.	Мера защиты информации	10	1	Слайд-лекция	1	Индиви-дуальная работа	3	Реферат	Устный опрос	10 неделя	В течение занятия
11.	Оптимальное управление процессами защиты	11	1	Слайд-лекция	1	Индиви-дуальная работа	3		Устный опрос	11 неделя	В течение занятия

12.	Оценка системы защиты	12	1	Слайд-лекция	1	Индиви-дуальная работа	3	Реферат	Устный опрос	12 неделя	В течение занятия
13.	Оценка системы защиты	13	1	Слайд-лекция	1	Индиви-дуальная работа	3	Самостоя-тельное изучение темы	Устный опрос	13 неделя	В течение занятия
14.	Безопасность компьютерных систем	14	1	Слайд-лекция	1	Индиви-дуальная работа	3		Устный опрос	14 неделя	В течение занятия
15.	Безопасность компьютерных систем	15	1	Слайд-лекция	1		3	Оформлени е и подача работ	Тестирова ние	15 неделя	В течение занятия
Всего часов:			7		7		21				
Промежуточный контроль (Модуль 2)											

Таблица 2 – Модульно-интегративная структура УК с указанием программных вопросов по модулям

Содержание	Модуль 1	Модуль 2
Программные вопросы	1. Понятие национальной безопасности. Виды безопасности. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности. 2. Информационные угрозы. Противодействие информационным угрозам. Характеристические свойства систем защиты информации. Методы защиты информации. Предмет защиты. Средства защиты. 3. Характеристические свойства систем обеспечения безопасности информации. Методы обеспечения безопасности информации. Средства обеспечения безопасности информации. 4. Архитектура электронных систем обработки данных. Архитектура программного обеспечения. Системные средства обработки данных. Прикладные средства обработки данных. Аппаратные средства информационной защиты. Программные средства информационной защиты. 5. Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем. 6. Построение парольных систем. Особенности применения криптографических методов. Способы реализации криптографической подсистемы 7. Особенности реализации систем с симметричными и несимметричными ключами. Способы реализации стенографических систем. 8. Концепция защищенного ядра. Методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы	9. Исследование корректности систем защиты. Методология обследования и проектирования защитных механизмов. Модель политики контроля целостности. 10. Определение необходимой меры защиты информационных ресурсов. Методы оценки меры защиты информации. Основные показатели оценки уровня защиты информации. Характеристики мер защиты 11. Модели и методы оптимального управления процессами обеспечения безопасности 12. Комплексная оценка системы защиты информации. Тестирование программного обеспечения. Проблема тестирования программных продуктов, автоматическое тестирование, принципы написания самотестирующихся программных продуктов. Инсталляция тестов в готовые программные продукты Оценка надежности защитных механизмов. Принципы оценки надежности защиты. 13. Инсталляция тестов в готовые программные продукты Оценка надежности защитных механизмов. Принципы оценки надежности защиты. 14. Защита в локальных сетях. Программные средства индивидуальной защиты информации. Использование экспертных систем для распознавания попыток несанкционированного доступа. 15. Использование экспертных систем для распознавания попыток несанкционированного доступа.

Обязательная литература	1. Партыка Т.Л., Попов И.И. Информационная безопасность: Учеб.пособие для сред.проф.образования. - М.: ФОРУМ ИНФРА-М, 2005. - 368с. чзэ-5 2. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288с чзэ-5, аб-1 3. Мао В. Современная криптография.Теория и практика/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 768с. чзэ-2 4. Хорев П.Б. Методы и средства защиты в компьютерных системах: Учеб.пособие для вузов. - М.: Академия, 2006. - 256 с. чзэ-2 5. Фергюсон Н., Шнайер Б. Практическая криптография/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 424с. чзэ-1 6. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. - Киев: МК-Пресс, 2006. - 288 с. чзэ-1 Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Академия АйТи, 2006. - 400 с. чзэ-1 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учеб.пособие. - М.: Дашков и К, 2007. - 336 с. чзэ-1	1. Партыка Т.Л., Попов И.И. Информационная безопасность: Учеб.пособие для сред.проф.образования. - М.: ФОРУМ ИНФРА-М, 2005. - 368с. чзэ-5 2. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288с чзэ-5, аб-1 3. Мао В. Современная криптография.Теория и практика/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 768с. чзэ-2 4. Хорев П.Б. Методы и средства защиты в компьютерных системах: Учеб.пособие для вузов. - М.: Академия, 2006. - 256 с. чзэ-2 5. Фергюсон Н., Шнайер Б. Практическая криптография/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 424с. чзэ-1 6. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. - Киев: МК-Пресс, 2006. - 288 с. чзэ-1 Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Академия АйТи, 2006. - 400 с. чзэ-1 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учеб.пособие. - М.: Дашков и К, 2007. - 336 с. чзэ-1

Дополнительная литература	1. Аскеров Т. М. Защита информации и информационная безопасность. Учебное пособие / Под общей редакцией К. И. Курбакова. М.; Рос. экон. акад., 2001. 387 с. 2. Баричев С. В. Криптография без секретов. М: Наука. 1998. 120 с. 3. Барсуков В. С, Вододазский. В. В. Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей (часть 1). Технология электронных коммуникаций. М., 1993. 146 с. 4. Барсуков В. В., Физическая защита информационных систем /Jetlnfo online, 1997. № 1(32). 5. Вербицкий О. В. Вступление к криптологии. Львов: Издательство науково-техничмой литературы, 1998. 300 с. 6. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва. Компания «ЕДИНАЯ ЕВРОПА», 1994. 331 с. 7. Галатенко В. А. Информационная безопасность. М.: Финансы и статистика, 1997. 158 с. 8. Герасименко В. А. Зашита информации в автоматизированных системах обработки данных (кн. 1). М.: Энергоатомиздат, 1994. 400 с. 9. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: МИФИ, 1997.537 с. 10. Герасименко В. А., Партыка Т. Л. Каталог программных средств защиты информации от несанкционированного доступа в АСОД. Метод, указания. М.: ГКНТ, 1984. 214 с. 11. Герасименко В. А., Партыка Т. Л., Каталог каналов утечки информации в АСОД. Метод, указания. М.: ГКНТ, 1985. 273 с. 12. Герасименко В. А., Скворцов А. А., Харитонов И. Е. Новые направления применения криптографических методов защиты информации. М.; Радио и связь, 1989. 360 с.	1. Аскеров Т. М. Защита информации и информационная безопасность. Учебное пособие / Под общей редакцией К. И. Курбакова. М.; Рос. экон. акад., 2001. 387 с. 2. Баричев С. В. Криптография без секретов. М: Наука. 1998. 120 с. 3. Барсуков В. С, Вододазский. В. В. Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей (часть 1). Технология электронных коммуникаций. М., 1993. 146 с. 4. Барсуков В. В., Физическая защита информационных систем /Jetlnfo online, 1997. № 1(32). 5. Вербицкий О. В. Вступление к криптологии. Львов: Издательство науково-техничмой литературы, 1998. 300 с. 6. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва. Компания «ЕДИНАЯ ЕВРОПА», 1994. 331 с. 7. Галатенко В. А. Информационная безопасность. М.: Финансы и статистика, 1997. 158 с. 8. Герасименко В. А. Зашита информации в автоматизированных системах обработки данных (кн. 1). М.: Энергоатомиздат, 1994. 400 с. 9. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: МИФИ, 1997.537 с. 10. Герасименко В. А., Партыка Т. Л. Каталог программных средств защиты информации от несанкционированного доступа в АСОД. Метод, указания. М.: ГКНТ, 1984. 214 с. 11. Герасименко В. А., Партыка Т. Л., Каталог каналов утечки информации в АСОД. Метод, указания. М.: ГКНТ, 1985. 273 с. 12. Герасименко В. А., Скворцов А. А., Харитонов И. Е. Новые направления применения криптографических методов защиты информации. М.; Радио и связь, 1989. 360 с.

Содержание лекций	**Тема №1**.Современное состояние проблемы безопасности информационных систем. **Тема №2.** Защита информации. **Тема №3.** Безопасность информации. **Тема №4.** Анализ программной и аппаратной платформы информационных систем. **Тема №5.** Модели безопасности информационных систем. **Тема №6** Примеры практической реализации систем защиты и безопасности. **Тема №7.** Примеры практической реализации систем защиты и безопасности. **Тема №8.** Основные характеристики защищенной информационной системы	**Тема №9.** Методология корректности информационной защиты. **Тема №10.** Мера защиты информации. **Тема №11.** Оптимальное управление процессами защиты. **Тема №12.** Оценка системы защиты. **Тема №13.** Оценка системы защиты. **Тема №14.** Безопасность компьютерных систем. **Тема №15.** Безопасность компьютерных систем.
Лабораторные работы	**Лабораторная работа№1:** Математическая структура секретных систем. **Лабораторная работа №2:** Теоретическая секретность. **Лабораторная работа №3:** Практическая секретность. **Лабораторная работа №4:** Классификация защищаемых объектов. **Лабораторная работа №5:** Типы информационных ресурсов. **Лабораторная работа №6:** Классы защиты информации. **Лабораторная работа №7:** Определение необходимой меры защиты по различным критериям оценки степени защиты. **Лабораторная работа №8:** Составление модели оптимального управления процессами защиты.	**Лабораторная работа №9:** Исследование систем шифрования. **Лабораторная работа №10:** Разработка программ моделирования оптимального управления защитой. **Лабораторная работа №11:** Тестирование защитных процедур. **Лабораторная работа №12:** Разработка процедур защиты от отладчика и дизассемблера. **Лабораторная работа №13:** Исследование и комплексная оценка сложности процедур защиты. **Лабораторная работа №14:** Разработка программы определения надежности защиты**.** **Лабораторная работа №15:** Разработка экспертной системы для контроля атаки.

Планы СРМП	**СРМП №1:** Математическая структура секретных систем. **СРМП №2:** Теоретическая секретность. **СРМП №3:** Практическая секретность. **СРМП №4:** Классификация защищаемых объектов. **СРМП №5:** Типы информационных ресурсов. **СРМП №6:** Классы защиты информации. **СРМП №7:** Определение необходимой меры защиты по различным критериям оценки степени защиты. **СРМП №8:** Составление модели оптимального управления процессами защиты.	**СРМП №9:** Исследование систем шифрования. **СРМП №10:** Разработка программ моделирования оптимального управления защитой. **СРМП №11:** Тестирование защитных процедур. **СРМП №12:** Разработка процедур защиты от отладчика и дизассемблера. **СРМП №13:** Исследование и комплексная оценка сложности процедур защиты. **СРМП №14:** Разработка программы определения надежности защиты**.** **СРМП №15:** Разработка экспертной системы для контроля атаки.

Таблица 3 - Организация самостоятельной работы магистранта СРМ по модулям УК

№ модуля	Тематика СРМ	Задания для СРМ	Формы контроля СРМ	График контроля СРМ (сроки)
1	**«Анализ безопасности информационных систем»**			
	Защита и безопасность информации в современном информационном процессе.	Роль и место системы защиты и безопасности информации в современном информационном процессе.	Реферат	2 неделя
	Системы защиты информации.	Системы защиты информации. Особенность и основные характеристики.	Реферат	3 неделя
	Структура стандартов в области информационной защиты и безопасности Республики Казахстан.	Изучение стандартов в области информационной защиты и безопасности Республики Казахстан.	Самостоятельное изучение темы	5 неделя
	Законодательные и нормативные акты Республики Казахстан в области защиты и безопасности информации.	Изучение законодательных и нормативных актов Республики Казахстан в области защиты и безопасности информации.	Оформление и подача работ	7 неделя
2	**«Безопасность компьютерных систем»**			
	Разработать модель оптимального управления защитой комплекса ЭВМ, связанных локальной сетью на основе операционной системы WIMDOWS – NT,2000	Разработать модель оптимального управления защитой комплекса ЭВМ, связанных локальной сетью на основе операционной системы WIMDOWS – NT,2000	Реферат	10 неделя
	Тестирование защитной программы	Разработать алгоритм тестирования защитной программы на основе имеющегося исходного текста программы	Реферат	12 неделя
	Оценка комплекса защитных процедур сети	Дать оценку комплекса защитных процедур сети на основе операционных систем WIMDOWS – NT,2000	Самостоятельное изучение темы	13 неделя
	Разработать программу для фиксации попыток атаки на защищаемый объект	Разработать программу для фиксации попыток атаки на защищаемый объект	Оформление и подача работ	15 неделя

Понятийный аппарат

1.	Шифрование	процесс применения шифра и защищаемой информации, т.е. преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре.
2.	Дешифрирование	процесс, обратный шифрованию, и заключающийся в преобразовании шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.
3.	Криптология	наука, состоящая из двух направлений: криптографии и криптоанализа.
4.	Криптоанализ	это наука (и практика ее применения) о методах и способах вскрытия шифров.
5.	Кодирование	вид криптографического закрытия, когда некоторые элементы защищаемых данных (не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т.д.).
6.	Коммерческая разведка	это несанкционированное получение информации, представляющей собой коммерческую тайну компании.
7.	Паразитная связь	связь по электрическим или магнитным цепям, появляющуюся независимо от желания конструктора.
8.	Шифрование	способ защиты при передаче информации на большие расстояния по линиям связи.
9.	Метод «белого шума»	излучается широкополосный шумовой сигнал с постоянным энергетическим спектром, существенно превышающим максимальный уровень излучения электронной техники
10.	Спектрально-энергетический метод	заключается в генерировании помехи, имеющей энергетический спектр, определяемый модулем спектральной плотности информативных излучений техники и энергетическим спектром атмосферной помехи.
11.	Статистический метод ЗИ	заключается в изменении вероятностной структуры сигнала, принимаемого разведприемником, путем излучения специальным образом формируемого маскирующего сигнала.
12.	Полнота информации	это показатель, характеризующий меру достаточности оцениваемой информации для решения соответствующих задач.
13.	Адекватность информации	степень ее соответствия действительному состоянию тех объектов, процессов или явлений, которые отображает оцениваемая информация.
14.	Объективность генерирования информации	зависит от способа получения значений характеристик объекта, процесса или явления и качества реализации (использования) способа в процессе получения этих значений.
15.	Релевантность информации	это показатель, который характеризует соответствие ее потребностям решаемой задачи.
16.	Толерантность информации	это показатель, характеризующий удобство восприятия и использования информации в процессе решения той задачи, для решения которой она используется.
17.	Технические средства защиты информации	основная защитная функция реализуется техническим устройством (комплексом или системой).
18.	Акустический шум	понимают шум, который характеризуется нормальным распределением амплитудного спектра и постоянством спектральной плотности мощности на всех частотах.

19.	Программные СЗИ	специальные программы, входящие в состав программного обеспечения АС для решения в них (самостоятельно или в комплекте с другими средствами) задач защиты.
20.	Криптография	наука о методах преобразования (шифрования) информации с целью ее защиты от злоумышленников.
21.	Шифр	способ (метод), преобразования информации с целью ее защиты от незаконных пользователей.
22.	Стеганография	набор средств и методов сокрытия факта передачи сообщения
23.	Вскрытие шифра	процесс получения защищаемой информации (открытого текста) из шифрованного сообщения (шифртекста) без знания примененного шифра.

Материалы по овладению УК

Перечень тестовых заданий для рубежного и итогового контроля

1. К техническим аспектам безопасности систем и сетей относится область …
2. Объектами изучения криптографии являются …
3. Разработка и применение защищенных информационных технологий относится к аспекту …
4. Открытый текст зашифрован с помощью шифра Цезаря. Ключ К=4. Построить шифртекст для заданного текста: «УТРО».
5. Атаки на ошибки реализации программ основываются на …
6. Атаки на ограничения защиты основываются на …
7. Шифртекст получен применением шифра Цезаря. К открытому тексту с ключом К=6. Восстановить открытый текст, если шифртекст = «РФСФРФС»
8. Атаки троянскими программами основываются на …
9. Атаки на отказ в обслуживании основываются на …
10. Подбор ключей шифрования по частотному словарю или методом «грубой силы», а также сборе и сопоставлении образцов открытых и зашифрованных данных относится к …
11. Скрытая передача секретной информации за пределы контролируемой зоны объекта относится к …
12. Конфиденциальность – это …
13. Аутентификация – это …
14. Пассивные атаки связаны с …
15. Для использования Афинного шифра был применен ключ $k = (9, 4)$. Определить обратное значение 9^{-1} для расшифрования (алфавит для шифрования - латинский).
16. Шифр определяется как семейство обратимых преобразований, каждое из которых определяется параметром, называемым …
17. Пусть M – открытый текст, C – шифрованное сообщение, E – алгоритм зашифрования, D – алгоритм расшифрования, тогда формула $D_{k_2}(C) = M$ описывает процесс:
18. Криптоанализ – это наука, изучающая …
19. Открытый текст = «ЗАРЯ» был преобразован в шифртекст = «СКЪЙ» с помощью шифра Цезаря. Вычислить величину ключа
20. Для проверки целостности к сообщению М добавляется проверочная комбинация, которая называется …
21. Цифровая подпись является методом решения проблемы …
22. Если ключ зашифрования совпадает с ключом расшифрования, то такие шифры называют …
23. Если каждый знак сообщения шифруется отдельно, то такой шифр является …
24. Одноалфавтные шифры замены называют …
25. Открытый текст = «ЭКЗАМЕН» зашифрован с помощью шифра «Лесенка» со ступеньками длиной 3. Определить шифртекст:
26. Ключ шифра перестановки основывается на …

27. Шифртекст = «СОИТМЯЕЕРТЕР» получен с помощью шифра «Лесенка» со ступеньками длиной 5. Определить открытый текст.
28. Шифр, основанный на некоторой геометрической фигуре, называется …
29. Стандарт шифрования DES осуществляет шифрование …
30. Открытый текст = «МОНАРХИЯ» зашифрован с помощью шифра «Лесенка». В результате был получен шифртекст = «МРОХНИАЯ»
31. Открытый текст = «АББА» зашифрован с помощью шифра Виженера с ключевым словом «ДА». Определить шифртекст.
32. Дисковый шифр относят к шифрам …
33. Для вычисления функции шифрования в DES – алгоритме используется преобразование S, составленное из 8 преобразований S – блоков $S_1, S_2, \ldots, S_8$. Эти блоки используются для преобразования 6 – битовых блоков B_j в 4 – битовые блоки B_j' . Пусть $B_5 = 101110$. Тогда B_5' в двоичной форме имеет вид:
34. Открытый текст = «ЕХАЛ ГРЕКА ЧЕРЕЗ РЕКУ» зашифрован с помощью вертикальной перестановки с ключом (3, 1, 2). Прямоугольник 6×3 . Тогда шифротекст имеет вид:

    Шифртекст = «РЛТМВУЯООЕЕНС» получен с помощью вертикальной перестановки с ключом (2, 3,1, 4). Прямоугольник 4×4 . Получить открытый текст

Контрольные вопросы для итогового контроля

35. Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная.
36. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности.
37. Информационные угрозы. Противодействие информационным угрозам.
38. Характеристические свойства систем защиты информации.
39. Методы защиты информации. Предмет защиты. Средства защиты.
40. Характеристические свойства систем обеспечения безопасности информации.
41. Методы обеспечения безопасности информации.
42. Средства обеспечения безопасности информации.
43. Архитектура электронных систем обработки данных. Архитектура программного обеспечения.
44. Системные средства обработки данных. Прикладные средства обработки данных.
45. Аппаратные средства информационной защиты. Программные средства информационной защиты.
46. Формальные модели. Модели безопасности. Политика безопасности.
47. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.
48. Построение парольных систем.
49. Особенности применения криптографических методов.
50. Способы реализации криптографической подсистемы.
51. Особенности реализации систем с симметричными и несимметричными ключами. Способы реализации стенографических систем.
52. Концепция защищенного ядра. Методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы.
53. Исследование корректности систем защиты. Методология обследования и проектировании защитных механизмов. Модель политики контроля целостности.
54. Определение необходимой меры защиты информационных ресурсов. Методы оценки меры защиты информации.
55. Основные показатели оценки уровня защиты информации. Характеристики мер защиты.
56. Модели и методы оптимального управления процессами обеспечения безопасности.
57. Комплексная оценка системы защиты информации.
58. Тестирование программного обеспечения. Проблема тестирования программных продуктов, автоматическое тестирование, принципы написания самотестирующихся программных

продуктов.

59. Инсталляция тестов в готовые программные продукты Оценка надежности защитных механизмов. Принципы оценки надежности защиты.
60. Защита в локальных сетях. Программные средства индивидуальной защиты информации.
61. Использование экспертных систем для распознавания попыток несанкционированного доступа.

Условия успешного достижения ожидаемых результатов по окончании УК

Политика выставления оценок:

Выполнение требований обеспечивает допуск к экзамену:

- Полнота и глубина знаний;
- Выявление ключевых понятий и моментов определенной темы;
- Знание определений основных терминов и понятий темы;
- Умение делать выводы и обобщать однотипные явления;

По данному курсу предусмотрены 2 рубежных контроля, которые будут проводиться в письменной форме.

В ходе работы с магистрантами можно выделить следующие виды контроля:

Текущий контроль (60%):

- выполнение заданий на лабораторных занятиях, СРМП и СРМ;
- посещение лекционных и лабораторных занятий.

Рубежный контроль (40%) включает в себя тестирование магистрантов по материалам лекций, СРМП и СРМ в марте и мае.

Итоговый контроль - экзамен.

Таблица 4 - Организация менеджмента качества профессиональной подготовки магистрантов по УК

1.Предрубежный (тренинговый) контроль Модули: 1,2 ПК	**2.Рубежный (промежуточный) контроль Модули: 1,2 РК**	**3.Пострубежный анализ тестов Модули: 1,2 ПА**	**4.Итоговый квалификационный контроль Сумма модулей: 1,2 ИК**	**5.Поститоговый анализ тестов ПА**
1. ЗАДАЧИ				
1.1.Ознакомление с технологией выполнения тестовых заданий РК для целенаправленной подготовки магистрантов к написанию рубежного теста.	1.1.Определение уровня сформированности знаний и умений магистрантов по модулям 1,2 УК.	1.1.Выявление природы возникновения типичных ошибок и их анализ с целью их предотвращения при выполнении аналогичных тестовых заданий	1.1.Регистрация прогресса качества знаний и умений магистрантов, контроль уровня сформированности знаний и умений за весь период изучения УК.	1.1.Развитие у магистрантов стратегии самооценки и самообучения.
2.ФОРМЫ КОНТРОЛЯ				
СРМП 2.1.Тест: 30 заданий (3 варианта) а) закрытые задания – 25п б) открытые задания – 5п 2.2.Образцы выполнения тестовых заданий	СРМП 2.1.Тест: 30 заданий (3 варианта) а) закрытые задания – 25п б) открытые задания – 5п 2.2.Образцы выполнения тестовых заданий	2.1.Устный/письменный анализ типичных ошибок в тестовых заданиях (интерактивный режим: магистрант-преподаватель)	СРМП 2.1.Тест: 30 заданий (3 варианта) а) закрытые задания – 25п б) открытые задания – 5п	2.1.Индивидуальные консультации для магистрантов
3.ПОЛИТИКА ОЦЕНИВАНИЯ ЗНАНИЙ И УМЕНИЙ МАГИСТРАНТОВ ПО УК				
3.1.Критерий и параметры оценивания знаний и умений магистрантов (Таблица 6) (включая шкалу оценивания знаний и умений магистрантов по международному стандарту. Таблица 7)				
-	-	-	-	-
3.3.Единая формула вычисления рейтинга магистранта				
	РК(М1,2) = (ТР(тек.рейт) + тест РК(руб.рейт))/2		СИ – суммарный индекс СИ=(РД(ТК+РК)+ИК)/2	

Список сокращений:
УК – учебный курс
СРМП – самостоятельная работа магистрантов под руководством преподавателя
СРМ – самостоятельная работа магистрантов
РК – рубежный контроль
ПК – предрубежный контроль

ПА – пострубежный анализ тестов
СИ – суммарный индекс
РД – рейтинг допуск
ТК – результат текущего контроля
ИК – результат итогового контроля

Таблица 5 – Критериально-оценочный аппарат тестовых заданий

Виды Тестовых Заданий	**Общее количество вопросов**	**Характер действия**	**Критерии**	**Параметры**	**Время исполнения задания**
Закрытые тестовые задания	25	Выбор правильного ответа из числа данных ответов	а) выбор сделан правильно б) выбор сделан неправильно	3 балла 0 баллов	2 мин. на 1 тестовое задание
		Максимальная оценка закрытого тестового задания		3 балла	
Открытые тестовые задания	5	Использование комплексов мыслительных и вербальных операций и действий, выполняемых на креативном речемыслительном уровне	1) Критерий информативности (полнота, логичность, четкость и ясность изложенной в задании информации) 2) Критерий опоры на теоретические знания при выполнении задания 3) Корректное использование навыков и умений, необходимых для выполнения задания и обеспечивающих на основе теоретических знаний правильность выполнения задания 4) Критерий терминологической и языковой правильности 5) Оригинальность решения поставленной задачи	1.Оптимальный уровень - 5 баллов. Выполнение задания соответствует всем пяти критериям 2.Достаточный уровень – 4 баллов. Выполнение задания соответствует трем-четырем из перечисленных критериев 3. Удовлетворительный уровень – 3 балла. Выполнение задания соответствует только двум ведущим из перечисленных критериев, а именно 2-му и 3-му критериям 4. неудовлетворительный уровень – 0 баллов. Выполнение задания соответствует только одному (или ни одному) из перечисленных критериев	5 мин. на 1 тестовое задание
		Максимальная оценка закрытого тестового задания		5 баллов	

Исходя из 100-бальной системы оценивания, разбалловка максимальной суммы может быть представлена следующим образом:

1) 25 закрытых тестовых заданий х 3 балла = 75 балла;
2) 5 открытых тестовых заданий х 5 баллов = 25 баллов

Итого: 100 баллов

при итоговой форме контроля индивидуальный рейтинг магистранта в балльном выражении исчисляется по формуле среднеарифметического, т.е.

СИ=(РД(ТК+РК)+ИК)/2, где

СИ – суммарный индекс;

РД – рейтинг допуск (аттестационный балл – АБ);

ТК – результат текущего контроля;

ИК – результат итогового контроля.

В зачетную книжку магистранта выставляется оценки исходя из суммарного индекса по 4-балльной системе. Перевод балльной системы в традиционную форму оценки дан в таблице 7, в которой сопоставлены предложенная система оценивания и шкала оценивания по международному стандарту в буквенном выражении.

Таблица 6 – Примерный расчет текущего рейтинга магистранта по УК

Факультет Факультет Послевузовского образования
Кафедра Автоматизированные системы обработки информации и управления
Группа ВТиПО(м)-102

№	Ф.И.О. магистранта	Аудиторная работа	СРМП					СРМ				Текущий рейтинг магистранта
		1	1	2	3	4	5	1	2	3	4	
		лекции	Защита лабораторных работ	Выступление с докладами	Компьютерное конструирование систем	Тестирование	Контрольная работа	Подготовка к лабораторным работам	Освоение материалов электронного курса	Самостоятельное изучение отдельных тем	Оформление и подача работ	
1	Романов В.Л.	100	100	100	100	100	100	100	100	100	100	100

Каждая форма текущего контроля оценивается по 100-балльной системе:

ТР(тек. рейтинг)=(лекции+СРМП(1+2+3+4+5)+СРМ(1+2+3+4))/N
где N – общее количество форм текущего контроля

Таблица 7 – Шкала оценивания знаний и умений магистрантов по международному стандарту

Оценка по буквенной системе	Баллы	%-ное содержание	Оценка по традиционной системе
A	4,0	95-100	отлично
A-	3,7	90-94	
B+	3,3	85-89	хорошо
B	3,0	80-84	
B-	2,7	75-79	
C+	2,3	70-74	удовлетворительно
C	2,0	65-69	
C-	1,7	60-64	
Д+	1,3	57-59	
Д	1,0	53-56	
Д-	0,7	50-52	
F	0,0	Ниже 50	неудовлетворительно

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная:

1. Партыка Т.Л., Попов И.И. Информационная безопасность: Учеб.пособие для сред.проф.образования. - М.: ФОРУМ ИНФРА-М, 2005. - 368с. чзэ-5
2. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288с чзэ-5, аб-1
3. Мао В. Современная криптография.Теория и практика/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 768с. чзэ-2
4. Хорев П.Б. Методы и средства защиты в компьютерных системах: Учеб.пособие для вузов. - М.: Академия, 2006. - 256 с. чзэ-2
5. Фергюсон Н., Шнайер Б. Практическая криптография/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 424с. чзэ-1
6. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. - Киев: МК-Пресс, 2006. - 288 с. чзэ-1
   Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Академия АйТи, 2006. - 400 с. чзэ-1
7. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учеб.пособие. - М.: Дашков и К, 2007. - 336 с. чзэ-1

Дополнительная литература:

1. Аскеров Т. М. Защита информации и информационная безопасность. Учебное пособие / Под общей редакцией К. И. Курбакова. М.; Рос. экон. акад., 2001. 387 с.
2. Баричев С. В. Криптография без секретов. М: Наука. 1998. 120 с.
3. Барсуков В. С, Вододазский. В. В. Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей (часть 1).

Технология электронных коммуникаций. М., 1993. 146 с.
4. Барсуков В. В., Физическая защита информационных систем /Jetlnfo online, 1997. № 1(32).
5. Вербицкий О. В. Вступление к криптологии. Львов: Издательство науково-техничмой литературы, 1998. 300 с.
6. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва. Компания «ЕДИНАЯ ЕВРОПА», 1994. 331 с.
7. Галатенко В. А. Информационная безопасность. М.: Финансы и статистика, 1997. 158 с.
8. Герасименко В. А. Зашита информации в автоматизированных системах обработки данных (кн. 1). М.: Энергоатомиздат, 1994. 400 с.
9. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: МИФИ, 1997.537 с.
10. Герасименко В. А., Партыка Т. Л. Каталог программных средств защиты информации от несанкционированного доступа в АСОД. Метод, указания. М.: ГКНТ, 1984. 214 с.
11. Герасименко В. А., Партыка Т. Л., Каталог каналов утечки информации в АСОД. Метод, указания. М.: ГКНТ, 1985. 273 с.
12. Герасименко В. А., Скворцов А. А., Харитонов И. Е. Новые направления применения криптографических методов защиты информации. М.; Радио и связь, 1989. 360 с.
13. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Военное издательство, 1992. 39 с.
14. Гостсхкомиссия России. Руководящий документ. Зашита от несанкционированного доступа к информации. Термины и определения. М.: Военное издательство, 1992. 12 с.
15. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.; Военное издательство, 1992. 12 с.
16. Грегори С. Смит. Программы шифрования данных // Мир ПК, 1997. № 3. С. 58-68.
17. ДиффиУ. Первые десять лет криптографии с открытым ключом //ТИИЭР, т. 76(1988)6 Т5б. С. 54-74.