МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КЫЗЫЛОРДИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ КОРКЫТ АТА

Политехнический институт

Кафедра «Вычислительная техника и информационные системы»

ОК 2302 «ОСНОВЫ КРИПТОГРАФИИ»

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

5В070400-“ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ”

ОЧНОЕ

Кызылорда

20__ г

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КЫЗЫЛОРДИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ КОРКЫТ АТА

Политехнический институт

Кафедра «Вычислительная техника и информационные системы»

«Утверждаю»
Директор политехнического института
_____ Шомантаев А.А.
«_____» _____ 2013 г

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ ОК 2302 «ОСНОВЫ КРИПТОГРАФИИ» ДЛЯ СТУДЕНТОВ 3 КУРСА СПЕЦИАЛЬНОСТИ 5В070400-“ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ”

Кызылорда
20__ г

Составитель: старший преподаватель кафедры «Вычислительная техника и информационные системы» Махамбаева Индира Утепбергеновна

Учебно-методический комплекс дисциплины составлен на основе ГОСО РК по специальности 5В070400 (ГОСО РК 5.04.019 – 2011) и учебной программы дисциплины «Основы криптографии», разработанной и утвержденной на кафедре «ВТиИС» (прот № 1 от 31.08.13, Кызылорда, КГУ им Коркыт Ата)

Учебно-методический комплекс рассмотрен на кафедре «Вычислительная техника и информационные системы»

«____» _____201__ г

Зав. каф «ВТиИС **Дауренбеков К.К.**

Учебно-методический комплекс по дисциплине «Основы криптографии» одобрен Комитетом по рабочим учебным планам и рабочим программам Политехнического института

«____» _____201__ г

Председатель комитета **Шомантаев А.А.**

Содержание

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КЫЗЫЛОРДИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени КОРКЫТ АТА

УЧЕБНАЯ ПРОГРАММА

ОК 2302 «ОСНОВЫ КРИПТОГРАФИИ»

5В070400 - Вычислительная техника и программное обеспечение
3 кредита

Кызылорда, 2013 г.

1. РАЗРАБОТАЛИ И ВНЕДРИЛИ

старший преподаватель кафедры «Вычислительная техника и информационные системы» Махамбаева Индира Утепбергеновна

2. РАССМОТРЕНА И УТВЕРЖДЕНА

Комитет по рабочим учебным планам и программам политехнического института КГУ имени Коркыт Ата протокол № ___ "____" _____ 2013г.

3. РАССМОТРЕНА И ОБСУЖДЕНА

на заседании научно-методического семинара кафедры «Вычислительная техника и информационные системы» протокол № ___ "____" _____ 2013г.

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Цели и задачи преподавания дисциплины, ее роль и значение и **подготовке специалистов**

1.1. Цель преподавания дисциплины

Целью изучения данного курса состоит в том, чтобы дать студентам основополагающие знания в области информационной безопасности. По окончании изучения дисциплины студенты должны владеть информацией о возможных угрозах и методах предотвращения потери информации, уметь анализировать возможные недостатки политик безопасности, составлять собственные политики и уметь реализовывать их.

1.2. Задача изучения дисциплин

По окончании изучения дисциплины студенты должны

- владеть информацией о возможных угрозах и методах предотвращения потери информации,
- уметь анализировать возможные недостатки политик безопасности,
- составлять собственные политики и уметь реализовывать их

1.3. Перечень базовых дисциплин для изучения курса "Основы криптографии"

- "Информатика" - представление и кодирование информации
- Программирование на алгоритмических языках
– Технология программирования

2 .Содержание дисциплины

2.1 Темы лекционных занятий, их содержание

Введение. Основные понятия информационной безопасности. Важность и сложность проблемы информационной безопасности. Объектно-ориентированный подход.

Распространение на информационную безопасность. Основные понятия объектно-ориентированного подхода

2.1.1. Угрозы информационной безопасности. Основные определения и критерии классификации угроз. Доступность, целостность и конфиденциальность угроз.
Стандарты и спецификация в области информационной безопасности. Основные понятия. Классы сетевые сервисы безопасности Средства администрирования безопасности. Основные понятия Критерия оценки безопасности информационных технологий. . Основные понятия. «Оранжевая книга».
2.1.2Информационная безопасность административного уровня.
Политика безопасности, программа безопасности с жизненным циклом систем и ее синхронизация.Управление рисками. Ликвидация, уменьшение, принятие, переадресация риска.Подготовительные этапы. Основные понятия управления рисками.
2.1.3. Меры процедурного уровня информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Реагирование на нарушение режима безопасности.Программно-технические меры. Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем.Идентификация и аутентификация. Управление доступом.
Основные понятия идентификации и аутентификации. Управление доступом. Ролевое управления доступом
2.1.4. Протоколирование и аудит, шифрование, контроль целостности. Основные понятия. Активный аудит. Шифрование. Контроль целостности. Цифровые сертификаты
Экранирование, анализ защищенности. Основные понятия**.**
Ограничивающий интерфейс. Архитектурные аспекты. Эшелонированность обороны.
2.1.5. Классификация межсетевых экранов. Экранирующие агенты.
Анализ защищенности. Антивирусная защита. Обеспечение высокой доступности.
Доступность. Основные понятия. Эффективность услуг. Основы мер обеспечения высокой доступности. Группы повышения доступности.
2.1.6. Отказоустойчивость и зона риска. Одиночные точки. Обеспечение отказоустойчивости. Основные понятия.Программное обеспечение промежуточного слоя. Основные понятия. Обеспечение обслуживаемости. Обслуживаемость пользователей.
2.1.7. Туннелирование и управление. Туннелирование. Виртуальные частные сети. Управление. Основные понятия.
2.1.8. Функциональные области. Менеджер/агент Возможности типичных систем. Основные понятия. Высокая доступность. Контроль производительности
Заключение
Перспективы развития защиты информации криптографическим способом.
2.2. Лабораторные работы, их наименование
2.2.1. Вопросы компьютерной безопасности. Методы защиты от компьютерных вирусов. Средства антивирусной защиты. Защита информации в Интернете.
2.2.2. Защита информации. Терминология. Сети. Организация защиты информации в локальной сети. Протоколы сетевого уровня.
2.2.3 Классификация вирусов и средства антивирусной защиты. Программные закладки и защита от них. Идентификация. Аутентификация. Глобальные сети. Устройства разрушения. Электронная почта. Почтовые бомбы как угроза безопасности
2.2.4. Криптография. Авторизация. Комплексная криптографическая информация Алгоритмы шифрования.
2.2.5. Хакеры и крекеры. Функция и применение паролей.
2.2.6. Функция и применение паролей. Полномочная политика безопасности.
2.2.7. Методы оценки вероятностного проявления безопасности информации.
2.2.8. Построение системы защиты информации.Порядок ввода в действие средств защиты информации.
2.4. Самостоятельная работа
2.4.1. Информационная безопасность в Windows. Протоколы
2.4.2. Встроенные учётные записи. Сети, глобальные сети
2.4.3. Группы безопасности. Грани объекта и уровни детализации

2.4.4. Средства управления учётными записями.
2.4.5. Создание надёжных паролей. Информационная безопасность
2.4.6 Проблема: забытые пароли. Компьютерные сети и их безопасность
2.5.7. Управление информационной безопасностью в сетях предприятий
2.6.8. Планирование восстановительных работ

Основная и дополнительная литература:

Основная литература

1. В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.
2. Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г
3. В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г
4. Е.А. Степанов «Информационная безопасность и защита информации», М., Инфра-М, 2001 г
5. А.Г.Ростовцев «Элементы криптологии», М., Инфра-М, 2000 г
6. «Теория и практика обеспечения информационной безопасности» под ред. Зегжды П.Д., С-П, Питер, 2000 г
7. Г. Винтон «Феномен Internet», М., Русская редакция, 2002 г
8. В.Гайкович, А.Першин «Безопасность электронных банковских систем», С-П, Питер, 2001 г
9. «Компьютерные системы и сети» под ред. В.П.Косарева и Л.В.Еремина , М., Финансы и статистика, 1999 г
10. Ю.И.Никифоров «Компьютерные преступления. Уголовные меры борьбы с компьютерной преступностью», М., Мир, 2000 г
11. И.Денис Ферн «Секреты супер-хакеров», С-П, «Невский проспект», 2000

Дополнительная литература

1. Диффи У., Хеллман Н.Э. Защищенность т помехостойкость. ВВедение в криптографию. // ТИИРЭ, 1999. – Т. 667. – N3 – С. 71-109.
2. Симионс Г.Дж. Обзор методов аутентификации информации ТИИРЭ, 2008. – Т. – N5. – 105-125.
3. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие. – Алматы: Каз НТУ, 2000.125 с.
4. Борсуков В. Бизнес и безопасность связи // Монитор Аспект, 1993. – N1. – С. 56-62.
5. Герасименко В.А. Защита информации в автоматизированныхз системах. Ч. 1,2. М.: «Высшая школа», 1995.
6. Кнут Д. Искусство программирование на ЭВМ. Т.2. Получисленные алгоритмы. – М.: Мир, 2000 – 724 с.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КЫЗЫЛОРДИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени КОРКЫТ АТА

«УТВЕРЖДАЮ»
Председатель Комитета по рабочим учебным планам и программам
_____Шомантаев А.А.

«_____» _____2013 г.

Рабочая учебная программа

Дисциплина: « Основы криптографии»
Специальность: 5В070400 – «ВТиПО»
Форма обучения: очная
Курс: 3
Семестр 5
Количество кредитов: 3
Из них:
лекции 30 часов,
лабораторные занятия 15 часов,
СРОП 15 часов
Ст.преп. Махамбаева И.У.

Кызылорда, 2013 г.

Рабочая учебная программа разработана на основании учебной программы, разработанной и утвержденной на кафедре «ВТиИС» (31.08.2013 г. протокол № 1)

Рабочую учебную программу подготовила: ст. преп. Махамбаева И.У.

Рабочая учебная программа рассмотрена и обсуждена на заседании кафедры «Вычислительнаятехника и информационные системы»
протокол № 1 "____"августа 2013 г.

Заведующий кафедрой:_____ к.т.н. Дауренбеков К.К.

Рабочая учебная программа рассмотрена и утверждена на заседании Комитета по рабочим учебным планам и программам.
протокол № 1 '____"сентября 2013 г.

Председатель Комитета: _____д.с.-х.н., проф. Шомантаев А.А.

УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. Информация о дисциплине: курс по выбору, OK 2302- Основы криптографии
2. Пререквизиты: AT 2203- Теория информации, OZH 2302 -Операционные системы
3. Постреквизиты: KZh YN 3204 -Теоретические основы компьютерных систем»,

KS 4306 -Компьютерные сети, IT 4305 -Интернет-технологии.

4. **Краткое содержание дисциплины**

Курс «Основы криптографии» является основополагающим по основам криптографии в системах персональных компьютеров организации и в локальных и глобальных сетях, он спроектирован для специалистов всех информационных технологий, включая администраторов по вопросам безопасности, аудиторов, проектировщиков сетей, системных аналитиков и т.д. в этом курсе изучаются: анализ систем с точки зрения потенциальных угроз для безопасности и их защита. Даются рекомендации по реализации стратегии безопасности. Дисциплина отвечает необходимому уровню современных научных и практических методов подхода к безопасному управлению сложными системами в различных организациях. Цель изучения данного курса состоит в том, чтобы дать студентам основополагающие знания в области информационной безопасности. По окончании изучения дисциплины студенты должны владеть информацией о возможных угрозах и методах предотвращения потери информации, уметь анализировать возможные недостатки политик безопасности, составлять собственные политики и уметь реализовывать их.

Выписка из рабочего учебного плана

Курс	Семестр	Кол-во кредитов	лек	прак	Лаб. занятия	СРОП	СРО	Всего	Форма контроля
3	5	3	30	-	15	15	75	135	экзамен

5. Календарно-тематический план лекционных, практических и лабораторных занятий

5.1. Содержание лекционных занятий

Неделя	Темы лекций	Кол-во часов	Наглядные пособия и другое материально-техническое оборудование	Методика проведения лекций	Используемая литература
1	2	3	4	5	6
1.	Введение. Основные понятия информационной безопасности. Важность и сложность проблемы информационной безопасности. Объектно-ориентированный подход.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде пресс-конференции	Основная литература [1-3]
2.	Распространение на информационную безопасность. Основные понятия объектно-ориентированного подхода	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
3.	Угрозы информационной безопасности. Основные определения и критерии классификации угроз. Доступность, целостность и конфиденциальность угроз	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
4.	Стандарты и спецификация	1	Презентации,	Визуальная	Основная

	в области информационной безопасности. Основные понятия. Классы сетевые сервисы безопасности		интерактивная доска, электронный учебник	лекция	литература [1-3]
5.	Средства администрирования безопасности. Основные понятия	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения конкретных примеров	Основная литература [1-3]
6.	Критерия оценки безопасности информационных технологий. Основные понятия. «Оранжевая книга».	1	Презентации, интерактивная доска, электронный учебник	Проблемная лекция	Основная литература [1-3]
7.	Информационная безопасность административного уровня	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде пресс-конференции	Основная литература [1-3]
8.	Политика безопасности, программа безопасности с жизненным циклом систем и ее синхронизация	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
9.	Управление рисками. Ликвидация, уменьшение, принятие, переадресация риска	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
10.	Подготовительные этапы Основные понятия управления рисками	1	Презентации, интерактивная доска, электронный учебник	Визуальная лекция	Основная литература [1-3]
11.	Меры процедурного уровня информационной безопасности. Основные классы мер процедурного уровня.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения конкретных примеров	Основная литература [1-3]
12.	Управление персоналом. Реагирование на нарушение режима безопасности	1	Презентации, интерактивная доска, электронный учебник	Проблемная лекция	Основная литература [1-3]
13.	Программно-технические меры. Основные понятия программно-технического уровня информационной безопасности	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде пресс-конференции	Основная литература [1-3]
14.	Особенности современных	1	Презентации,	Лекция в виде	Основная

	информационных систем.		интерактивная доска, электронный учебник	обсуждения	литература [1-3]
15.	Идентификация и аутентификация. Управление доступом.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
16.	Основные понятия идентификации и аутентификации. Управление доступом. Ролевое управления доступом	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
17.	Протоколирование и аудит, шифрование, контроль целостности. Основные понятия	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
18.	Активный аудит. Шифрование. Контроль целостности. Цифровые сертификаты	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
19.	Экранирование, анализ защищенности. Основные понятия	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
20.	Ограничивающий интерфейс. Архитектурные аспекты. Эшелонированность обороны	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
21.	Классификация межсетевых экранов. Экранирующие агенты	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
22.	Анализ защищенности. Антивирусная защита	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
23.	Обеспечение высокой доступности. Доступность. Основные понятия	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
24.	Эффективность услуг. Основы мер обеспечения	1	Презентации, интерактивная	Лекция в виде обсуждения	Основная литература

	высокой доступности. Группы повышения доступности		доска, электронный учебник		[1-3]
25.	Отказоустойчивость и зона риска. Одиночные точки.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
26.	Обеспечение отказоустойчивости. Основные понятия.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
27.	Программное обеспечение промежуточного слоя. Основные понятия.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
28.	Обеспечение обслуживаемости. Обслуживаемость пользователей	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде обсуждения	Основная литература [1-3]
29.	Туннелирование и управление. Туннелирование. Виртуальные частные сети. Управление. Основные понятия.	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
30.	Функциональные области. Менеджер/агент Возможности типичных систем. Основные понятия. Высокая доступность. Контроль производительности	1	Презентации, интерактивная доска, электронный учебник	Лекция в виде дискуссии	Основная литература [1-3]
31.		30			

5.2. Содержание лабораторных занятий

Неделя	Темы лабораторных занятий	Кол-во часов	Используемые на занятии технические средства и др.	Методические рекомендации для выполнения работы
1	2	3	4	5
1.	Вопросы компьютерной безопасности.	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
2.	Методы защиты от компьютерных вирусов. Средства антивирусной	2	Интерактивная доска, ПК, презентация	Методические указания, электронный

	защиты. Защита информации в Интернете.			учебник, слайды
3.	Защита информации. Терминология. Сети. Организация защиты информации в локальной сети. Протоколы сетевого уровня	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
4.	Классификация вирусов и средства антивирусной защиты	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
5.	Глобальные сети. Устройства разрушения. Электронная почта. Почтовые бомбы как угроза безопасности.	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
6.	Программные закладки и защита от них. Идентификация. Аутентификация	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
7.	Криптография. Авторизация. Комплексная криптографическая информация	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
8.	Алгоритмы шифрования	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
9.	Система бесперебойного электроснабжения.	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
10.	Хакеры и крекеры	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
11.	Функция и применение паролей	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
12.	Полномочная политика безопасности.	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
13.	Построение системы защиты информации.	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды
14.	Методы оценки вероятностного проявления безопасности информации	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды

15.	Порядок ввода в действие средств защиты информации	2	Интерактивная доска, ПК, презентация	Методические указания, электронный учебник, слайды

5.3. План самостоятельной работы обучающегося с преподавателем

Неделя	Тема	Кол-во часов	Вид занятия	Информационные источники: литература, интернет
1	2	3	4	5
1.	Информационная безопасность в Windows.	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
2.	Встроенные учётные записи	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
3.	Группы безопасности	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
4.	Средства управления учётными записями	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
5.	Средства управления учётными записями	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
6.	Создание надёжных паролей	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
7.	Проблема: забытые пароли	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
8.	Политики учётных записей Средства управления учётными записями	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
9.	Управление	1	Творческая	Основная

	информационной безопасностью в сетях предприятий		самостоятель-ная работа(доклад, презентация)	литература [1-3], www.twirpx.com, www.studfiles.ru
10	Контроль доступа -базовый элемент защиты	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
11	Создание политики безопасности	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
12	Элементы защиты от несанкционированного доступа.	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
13	Расширенные возможности сбора статистики и генерация предупреждений	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
14	Аутентификация пользователей	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
15	Трансляция сетевых адресов Средства управления учётными записями	1	Творческая самостоятель-ная работа(доклад, презентация)	Основная литература [1-3], www.twirpx.com, www.studfiles.ru
16		15		

5.4. Самостоятельная работа обучающегося

неделя	**Задания СРО**	**Академические часы**	**Предлагаемая литература и другие информационные источники**	**Сроки выполнения работы**	**Форма выполнения СРО**
1	Протоколы. Информацион-ная безопасность в Windows.	5	В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.	3 неделя	Презентация
2	Криптография. Встроенные учётные записи.	5	В.В.Герасименко «Защита информации в	4 неделя	Презентация

	Средства управления учётными записями		автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.		
3	Сети. Глобальные сети	5	Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г	5 неделя	Презентация
4	Криптосистемы Комплексная криптографии-ческая инфор-мация	5	В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.	6 неделя	Презентация
5	Авторизация. Создание надёжных паролей.	5	Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г	7 неделя	Презентация
6	Грани объекта. Уровни детализации.	5	Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г	8 неделя	Презентация
7	Атаки. Группы безопасности.	5	В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г	10 неделя	Презентация
8	Защита информации. Информацион-ная безопасность	5	В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г. Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г	11 неделя	Презентация
9	Шифрование. Алгоритм шифрования.	5	В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г	12 неделя	Презентация
10	Политика безопасности. Программа без-опасности с жиз-ненным циклом систем и ее синхронизация	5	В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г	13 неделя	Презентация
11	Создание	5	Л.Дж. Хоффман «Современные	12	Презентация

	политики безопасности		методы защиты», С-П, Питер, 1999 г	неделя	
12	Хакеры и крекеры.	5	Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г	13 неделя	Презентация
13	Компьютерные сети и их безопасность.	5	В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.	14 неделя	Презентация
14	Аутентификация .Идентификация	5	В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.	14 неделя	Презентация
15	Методы оценки и безопасность информации. Оценки вероятностного проявления безопасности информации	5	В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г	15 неделя	Презентация
		75			

6. Вопросы 1,2-ого рубежных контролей.

1. Конфиденциальная система обеспечивает уверенность в том, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен такие пользователи называются…
2. Реализованная угроза называется…
3. Любое потенциальное действие, которое направлено на нарушение конфиденциальности целостности и доступности информации называется…
4. Умышленные угрозы подразделяются на
5. Защита информации ориентирована на борьбу с так называемыми…
6. Несанкционированный доступ к информации без изменения состояния системы
7. Несанкционированное изменение системы
8. Программные код встроенный в другую программу или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере…
9. Блоки программного кода, целенаправленно внедренные внутрь других прикладных программ…
10. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков или в содержании других программ. Этот процесс называется…
11. К компьютерным вирусам примыкают и так называемые…
12. По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям нарушению работы

программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется…

13. Существует два подхода построения системы защиты информации
14. Сколько существует подходов построения системы защиты информации
15. Совокупность организованных и технологических мер, программно-технологических средств, правовых и морально-этических норм, направленных на противодействий угрозам нарушителей с целью сведения до минимализма возможного ущерба пользователям и владельцам системы…
16. Фрагментарный подход
17. Комплексный подход
18. Существует много возможных направлений в утечке информации путей несанкционированного доступа к ней системах и в сетях
19. Под элементом защиты понимается…
20. Под объектом защиты понимается…
21. Процессы по нарушению надежности информации можно разделить на
22. Доступ к объектам и элементам защиты информации может или возможен для … категорий лиц
23. Доступ к объектам и элементам защиты информации может или возможен для двух категорий лиц
24. Несанкционированное ознакомление с информацией подразделяется на…
25. При построении защиты информации сложилось… подхода
26. При фрагментарном подходе
27. При построении защиты информации сложилось два подхода
28. При комплексном подходе
29. Протокол –
30. Компьютер-отправитель в соответствии с протоколом выполняет следующие действия:
31. Существует … основных момента, касающихся протоколов
32. .Компьютер-получатель в соответствии с протоколом выполняет действия, но в обратном порядке
33. Маршрутизируемый протокол – это
34. .Маршрутизируемые протоколы могут использоваться для объединения … локальных сетей в глобальную сеть
35. Несколько протоколов, которые работают в сети одновременно, обеспечивают следующие операции с данными:
36. Стек протоколов – это
37. Прикладной уровень –
38. Представительский уровень –
39. Сеансовый –
40. Коммуникационные задачи, которые возложены на сеть, позволяют выделить среди протоколов … типа
41. Сетевой –
42. Транспортный уровень –
43. E -mail легко:
44. Индивидуальное планирование
45. Каталоги обычно предоставляют следующую информацию о сетевых пользователях
46. Программные планирования
47. Групповое планирование-
48. Канальный уровень
49. Физический уровень
50. Какой протокол является базовым в Интернет?
51. Компьютер, подключенный к Интернет, обязательно имеет...
52. Гиперссылки на Web - странице могут обеспечить переход...

53. Задан адрес электронной почты в сети Internet: user_name@int.glasnet.ru. Каково имя владельца электронного адреса?
54. Браузеры (например, Microsoft Internet Explorer) являются...
55. Web - страницы имеют формат (расширение)...
56. Защита информации в системах и сетях –это
57. Объект защиты информации – это
58. Элемент защиты информации – это
59. Защитить информацию – это значит

7. Перечень литературы (основная, дополнительная)

Основная литература

12. В.В.Герасименко «Защита информации в автоматизированных системах обработки данных», М., «Русская редакция», 2000 г.
13. Л.Дж. Хоффман «Современные методы защиты», С-П, Питер, 1999 г
14. В.В. Мельников «Защита информации в компьютерных системах», М., «Русская редакция», 2000 г
15. Е.А. Степанов «Информационная безопасность и защита информации», М., Инфра-М, 2001 г
16. А.Г.Ростовцев «Элементы криптологии», М., Инфра-М, 2000 г
17. «Теория и практика обеспечения информационной безопасности» под ред. Зегжды П.Д., С-П, Питер, 2000 г
18. Г. Винтон «Феномен Internet», М., Русская редакция, 2002 г
19. В.Гайкович, А.Першин «Безопасность электронных банковских систем», С-П, Питер, 2001 г
20. «Компьютерные системы и сети» под ред. В.П.Косарева и Л.В.Еремина , М., Финансы и статистика, 1999 г
21. Ю.И.Никифоров «Компьютерные преступления. Уголовные меры борьбы с компьютерной преступностью», М., Мир, 2000 г
22. И.Денис Ферн «Секреты супер-хакеров», С-П, «Невский проспект», 2000

Дополнительная литература

7. Диффи У., Хеллман Н.Э. Защищенность т помехостойкость. Введение в криптографию. // ТИИРЭ, 1999. – Т. 667. – N3 – С. 71-109.
8. Симионс Г.Дж. Обзор методов аутентификации информации ТИИРЭ, 2008. – Т. – N5. – 105-125.
9. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие. – Алматы: Каз НТУ, 2000.125 с.
10. Борсуков В. Бизнес и безопасность связи // Монитор Аспект, 1993. – N1. – С. 56-62.
11. Герасименко В.А. Защита информации в автоматизированныхз системах. Ч. 1,2. М.: «Высшая школа», 1995.
12. Кнут Д. Искусство программирование на ЭВМ. Т.2. Получисленные алгоритмы. – М.: Мир, 2000 – 724 с.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КЫЗЫЛОРДИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ КОРКЫТ АТА

«УТВЕРЖДАЮ»
Директор политехнического
института_____Шомантаев А.А.
«___»_____ 2013г.

Рабочая учебная программа обучающегося по дисциплине

“Основы криптографии” **(SYLLABUS)**

5В070400 - “Вычислительная техника и программное обеспечение”

Кызылорда, 2013г.

Рабочую учебную программу (Syllabus) разработал:ст. преподаватель Махамбаева И.У.

Рабочая учебная программа обучающегося (Syllabus) рассмотрена и обсуждена на заседании кафедры «Вычислительная техника и информационные системы»

протокол № 1 "31 " августа 2013 г.

Заведующий кафедрой: к.т.н., ст преподаватель Дауренбеков К.К

Рабочая учебная программа обучающегося (Syllabus) рассмотрена и утверждена на заседании Комитета по рабочим учебным планам и программам.

протокол № 1 " 1 " сентябрь 2013г.

Председатель Комитета: д.с-х-н., профессор А.А.Шомантаев

1. Основная информация	
Факультет/институт	Политехнический
Специальность (шифр, наименование)	5В070400 - Вычислительная техника и программное обеспечение
Курс, семестр	3курс, 5 семестр
Статус дисциплины (обязательный, компонент по выбору)	Курс по выбору
Кол-во кредитов	3 кредита
Место проведения занятия (аудитория)	Понедельник 11.30-12.20 (1-15 лек) 401 ауд;; Среда 12.50-14.40, (1-15 лаб) 307 ауд; 13.50-14.40. (1-15 срсп). Четверг 9.30-10.20 (1-15 лек) 401 ауд;
Преподаватель	ст. преподаватель Махамбаева И.У.,235512. вторник 12.30-13.30
Преподаватель, ведущий практические, семинарские, лабораторные занятия	ст. преподаватель Махамбаева И.У.,235512 Indira_mah
2. Пререквизиты и постреквизиты	
Пререквизиты	Inf 1105 - Информатика, PAYa 1204 – Программирование на алгоритмических языках, TP 1301 – Технология программирования
Постреквизиты	EZhZhU 3211 – Организация вычислительных систем и сетей, ТК 3601 –Теоретические основы компьютерных систем, ТК 3301 – Организация ЭВМ
3. Цели и задачи дисциплины	
Цели: Целью дисциплины "Основы криптографии" является изучение принципов построения и функционирования, взаимодействия как отдельных аппаратных компонентов ЭВМ и периферийных систем, так и функционирование ЭВМ в целом	
Задачи: По окончании изучения дисциплины студенты должны - владеть информацией о возможных угрозах и методах предотвращения потери информации, - уметь анализировать возможные недостатки политик безопасности, - составлять собственные политики и уметь реализовывать их	

4. Содержание дисциплины

Раскладка рабочего времени обучающегося по видам занятий

Общее кол-во часов	Кол-во академических часов				
	Лекции	Практические/ семинарские	Лабораторные	СРОП	СРО
135	30		15	15	75