

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Томский государственный университет систем управления и радиоэлектроники



УТВЕРЖДАЮ

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

« ____ » _____ 2016 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Уровень основной образовательной программы: бакалавриат

Направление(я) подготовки (специальность): 09.03.03 – Прикладная информатика

Профиль: Прикладная информатика в экономике

Форма обучения: очная

Факультет: ФСУ, Факультет систем управления

Кафедра: АСУ, Кафедра автоматизированных систем управления

Курс 4

Семестр 7

Учебный план набора 2016 и последующих лет

| Виды учебной работы | Семестр 7 | Всего | Единицы |
|---|------------------|------------------|---------|
| Лекции | 28 | 28 | часов |
| Лабораторные работы | 26 | 26 | часов |
| Практические занятия | 18 | 18 | часов |
| Курсовой проект/работа (КРС) (аудиторная) | не предусмотрено | не предусмотрено | часов |
| Всего аудиторных занятий | 72 | 72 | часов |
| Из них в интерактивной форме | 19 | 19 | часов |
| Самостоятельная работа студентов (СРС) | 72 | 72 | часов |
| Всего (без экзамена) | 144 | 144 | часов |
| Самост. работа на подготовку и сдачу экзамена | 36 | 36 | часов |
| Общая трудоемкость | 180 | 180 | часов |
| (в зачетных единицах) | 5 | 5 | ЗЕТ |

Экзамен: 7 семестр

Томск 2016

Рабочая программа по дисциплине составлена с учетом требований Федерального Государственного образовательного стандарта высшего профессионального образования (ФГОС ВО) по направлению подготовки 09.03.03 Прикладная информатика (квалификация (степень) "бакалавр"), утвержденного Приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г. № 207, рассмотрена и утверждена на заседании кафедры 12 февраля 2016 г., протокол № 5.

Разработчик д.т.н., профессор каф. АСУ _____ А.Н. Горитов

Зав. обеспечивающей кафедрой АСУ
д.т.н., профессор _____ А.М. Корилов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами специальности.

Декан, к.т.н., доцент _____ П.В. Сенченко

Заведующий профилирующей и выпускающей
кафедрой АСУ, д.т.н., профессор _____ А.М. Корилов

Эксперт:
Кафедра АСУ, _____ доцент _____ А.И. Исакова

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

В современных условиях хозяйствования актуальным становится требование подготовки специалистов, обладающих необходимыми навыками использования современных информационных систем и технологий в различных областях. Необходимой составляющей такой подготовки являются как теоретические знания, так и практические навыки в области защиты информации и информационной безопасности.

Цель дисциплины – дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации.

При этом **основными задачами дисциплины** являются:

- овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами;
- приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса;
- овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Информационная безопасность» относится к числу дисциплин вариативной части профессионального цикла. «Информационная безопасность» как учебная дисциплина в системе подготовки бакалавров по направлению 09.03.03 «Прикладная информатика» связана с дисциплинами учебного плана: «Математика», «Дискретная математика», «Информатика и программирование», «Основы алгоритмизации и языки программирования», «Вычислительные системы, сети и телекоммуникации», «Операционные системы».

Знания и навыки, полученные при изучении этой дисциплины, используются в дисциплине профессионального цикла: «Проектирование информационных систем» и выпускной квалификационной работе.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

общепрофессиональные компетенции (ПК):

– способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (**ОПК-4**).

После изучения дисциплины «Информационная безопасность» студент должен **знать**:

- основные понятия и направления в защите компьютерной информации,
- принципы защиты информации,
- принципы классификации и примеры угроз безопасности компьютерным системам,
- современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности,
- основные инструменты обеспечения многоуровневой безопасности в информационных системах.

уметь:

- выявлять угрозы информационной безопасности,
- обосновывать организационно-технические мероприятия по защите информации в ИС,
- проводить анализ защищенности компьютера и сетевой среды;
- организовывать безопасную работу в Интернет;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

владеть:

- навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

| Вид учебной работы | Всего часов | Семестры 7 |
|---|-------------|------------|
| Аудиторные занятия (всего) | 72 | 72 |
| В том числе: | | |
| Лекции | 28 | 28 |
| Лабораторные работы (ЛР) | 26 | 26 |
| Практические занятия (ПЗ) | 18 | 18 |
| Семинары (С) | – | – |
| Коллоквиумы (К) | – | – |
| Курсовой проект (работа) (аудиторная нагрузка) | – | – |
| <i>Другие виды аудиторной работы</i> | | |
| Самостоятельная работа (всего) | 72 | 72 |
| В том числе: | | |
| Курсовой проект (работа) (самостоятельная работа) | – | – |
| Расчетно-графические работы | – | – |
| Реферат | – | – |
| <i>Другие виды самостоятельной работы</i> | | |
| Проработка лекционного материала | 16 | 16 |
| Подготовка к практическим занятиям | 18 | 18 |
| Подготовка к лабораторным занятиям | 26 | 26 |
| Самостоятельное изучение тем теоретической части | 12 | 12 |
| Подготовка к экзамену | 36 | 36 |
| Вид промежуточной аттестации (зачет, экзамен) | экзамен | экзамен |
| Общая трудоемкость | 180 | 180 |
| час | 180 | 180 |
| зач. ед. | 5 | 5 |

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Разделы дисциплин и виды занятий

Таблица 5.1

| № п/п | Наименование раздела дисциплины | Лекц. | Лаб. зан. | Практ. зан. | СРС | Всего часов | Формируемые компетенции (ОК, ПК) |
|-------|---|-----------|-----------|-------------|-----------|-------------|----------------------------------|
| 1 | 2 | 3 | 4 | 5 | 7 | 8 | 9 |
| 1. | Введение в информационную безопасность. | 2 | – | 2 | 3 | 7 | ОПК-4 |
| 2. | Законодательные и правовые основы защиты компьютерной информации. | 3 | – | 4 | 6 | 13 | ОПК-4 |
| 3. | Математические методы и модели в задачах защиты информации. | 4 | 11 | 2 | 27 | 44 | ОПК-4 |
| 4. | Математические основы криптографических методов. | 3 | – | 2 | 4 | 9 | ОПК-4 |
| 5. | Криптография с открытым ключом | 4 | 15 | – | 17 | 36 | ОПК-4 |
| 6. | Методы идентификации и аутентификации пользователей. | 3 | – | 2 | 4 | 9 | ОПК-4 |
| 7. | Межсетевые экраны и VPN сети. | 4 | – | 2 | 4 | 10 | ОПК-4 |
| 8. | Защита компьютерных систем от вредоносных программ. | 3 | – | 2 | 4 | 9 | ОПК-4 |
| 9. | Комплексная защита информации. | 2 | – | 2 | 3 | 7 | ОПК-4 |
| | ИТОГО | 28 | 26 | 18 | 72 | 144 | |

5.2. Содержание разделов дисциплины (по лекциям)

Таблица 5.2

| № п/п | Наименование разделов | Содержание разделов | Трудоемкость (час.) | Формируемые компетенции (ОК, ПК) |
|-------|--|---|---------------------|----------------------------------|
| 1 | 2 | 3 | 4 | 5 |
| 1. | Введение в информационную безопасность | Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации, связь проблем ИБ с развитием информационных технологий и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Обзор и параметры классификации угроз безопасности информации. Принципы защиты информации. Классы средств защиты информации. Государственная стратегия обеспечения ИБ в России. | 2 | ОПК-4 |
| 2. | Законодательные и правовые основы защиты компьютерной информации | Основы российского законодательства в сфере защиты информации. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации. Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем. | 3 | ОПК-4 |
| 3. | Математические методы и модели в задачах защиты информации | Основные понятия криптографии. Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Исследования Шеннона в области криптографии. Методы шифрования. Основные понятия и определения. Классификация методов шифрования. Блочные шифры. Сеть Фейштеля. Алгоритмы блочного шифрования. Режимы выполнения алгоритмов шифрования. Вопросы стойкости блочных шифров. Потоковые шифры. Основные понятия. Алгоритмы потокового шифрования. | 4 | ОПК-4 |
| 4 | Математические основы криптографических методов | Основные понятия и определения теории информации. Основные теоремы теории чисел. Дискретные логарифмы в конечном поле. Элементы теории сложности проблем. Классы сложности проблем. | 3 | ОПК-4 |
| 5 | Криптография с открытым ключом | Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Алгоритмы шифрования с открытым ключом. Вопросы стойкости. Задача распределения ключей. Криптографические хеш-функции. Хеш-функции на базе блочных шифров. Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Вопросы стойкости электронной цифровой подписи. Сертификат открытого ключа. | 4 | ОПК-4 |

| | | | | |
|--------------|---|--|-----------|-------|
| 6. | Методы идентификации и аутентификации пользователей | Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя. | 3 | ОПК-4 |
| 7. | Межсетевые экраны и VPN сети | Межсетевые экраны. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Формирование политики межсетевого взаимодействия. Персональные межсетевые экраны. Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей (VPN). Основные понятия и функции. Достоинства применения технологии VPN. | 4 | ОПК-4 |
| 8. | Защита компьютерных систем от вредоносных программ. | Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них. | 3 | ОПК-4 |
| 9. | Комплексная защита информации | Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. | 2 | ОПК-4 |
| ИТОГО | | | 28 | |

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

| № п/п | Наименование обеспечивающих (предыдущих) дисциплин | № № разделов данной дисциплины, для которых необходимо изучение обеспечивающих (предыдущих) дисциплин | | | | | | | | |
|----------------------------------|--|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Предшествующие дисциплины | | | | | | | | | | |
| 1. | Математика | | | + | + | + | + | + | | |
| 2. | Дискретная математика | | | + | + | + | + | + | | |
| 3. | Информатика и программирование | + | + | + | + | + | | | | |
| 4. | Основы алгоритмизации и языки программирования | | | + | + | + | + | + | + | |
| 5. | Вычислительные системы, сети и телекоммуникации | | | | | | + | + | | + |
| 6. | Операционные системы | | | | | | + | + | + | + |
| Последующие дисциплины | | | | | | | | | | |
| 1. | Проектирование информационных систем | + | + | + | + | + | + | + | + | + |
| 2. | Выпускная квалификационная работа | + | + | + | + | + | + | + | + | + |

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

| Перечень компетенций | Л | Лаб | Прак. | СРС | Формы контроля |
|----------------------|---|-----|-------|-----|----------------|
| | | | | | ОПК-4 |

Л – лекция, Прак – практические работы, Лаб – лабораторные работы, СРС – самостоятельная работа студента

6. МЕТОДЫ И ФОРМЫ ОРГАНИЗАЦИИ ОБУЧЕНИЯ

Для успешного освоения дисциплины применяются различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме.

Технологии интерактивного обучения при разных формах занятий

| Методы \ Формы | Лекции (час) | Лабораторные занятия (час) | Практические занятия (час) | Всего (час) |
|------------------------------------|--------------|----------------------------|----------------------------|-------------|
| Работа в команде | | 8 | 4 | 12 |
| Пресс-конференция | 3 | | | 3 |
| Поисковый метод | | 4 | | 4 |
| Итого интерактивных занятий | 3 | 12 | 4 | 19 |

Примечание.

1. «Работа в команде» происходит при коллективном решении задачи на лабораторной работе № 4 и на практическом занятии № 5.
2. «Поисковый метод» студенты используют при выполнении лабораторной работы № 6.
3. «Пресс-конференция» используется для обсуждения вопросов, связанных с разработкой алгоритмов криптографической защиты информации.

7. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

| № п/п | № раздела дисциплины из табл. 5.1 | Наименование лабораторных работ | Трудоемкость (час.) | ОК, ПК |
|-------|-----------------------------------|---|---------------------|--------|
| 1. | 3 | Блочное симметричное шифрование | 4 | ОПК-4 |
| 2. | 3 | Изучение ППП систем криптографической защиты информации, классическая криптография | 4 | ОПК-4 |
| 3. | 5 | Асимметричное шифрование | 4 | ОПК-4 |
| 4. | 5 | Электронная цифровая подпись (ЭЦП) | 4 | ОПК-4 |
| 5. | 5 | Практическое применение криптографии с открытым ключом. Пакет PGP | 4 | ОПК-4 |
| 6. | 3, 5 | Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI | 6 | ОПК-4 |
| | ИТОГО | | 26 | |

8. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ (СЕМИНАРЫ)

| № п/п | № раздела дисциплины из табл. 5.1 | Темы практических занятий (семинарских) | Трудоемкость (час.) | ОПК, ПК |
|-------|-----------------------------------|--|---------------------|---------|
| 1. | 1 | Федеральный закон «Об информации, информационных технологиях и о защите информации» | 2 | ОПК-4 |
| 2. | 2 | Методы оценки уязвимости информации | 2 | ОПК-4 |
| 3. | 2 | Современные приложения криптографии | 2 | ОПК-4 |
| 4. | 3 | Федеральный закон «Об электронной цифровой подписи» | 2 | ОПК-4 |
| 5. | 4 | Сложные математические задачи и алгоритмы ЭЦП | 2 | ОПК-4 |
| 6. | 6 | Методы аутентификации | 2 | ОПК-4 |
| 7. | 7 | Основные технологии построения защищенных информационных систем | 2 | ОПК-4 |
| 8. | 8 | Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности | 2 | ОПК-4 |
| 9. | 9 | Комплексная система обеспечения информационной безопасности. | 2 | ОПК-4 |
| | ИТОГО | | 18 | |

9. САМОСТОЯТЕЛЬНАЯ РАБОТА

| № п/п | № раздела дисциплины из табл. 5.1 | Тематика самостоятельной работы (детализация) | Трудоемкость (час.) | ОК, ПК | Контроль выполнения работы |
|-------|-----------------------------------|--|---------------------|--------|--------------------------------------|
| 1. | 1 ÷ 9 | Проработка лекционного материала | 16 | ОПК-4 | Опрос на занятиях |
| 2. | 1 ÷ 9 | Подготовка к практическим занятиям | 18 | ОПК-4 | Дом. задание, проверка решения задач |
| 3. | 3 ÷ 9 | Подготовка к лабораторным занятиям | 26 | ОПК-4 | Отчет, защита лаб. работы |
| 4. | 3 | Самостоятельное изучение тем теоретической части | 12 | ОПК-4 | Дом. задание, опрос |
| 5. | 1 ÷ 9 | Подготовка и сдача экзамена | 36 | ОПК-4 | Оценка за экзамен |
| | ИТОГО | | 108 | | |

Темы для самостоятельного изучения

- 1) Блочный шифр BLOWFISH (3 час.).
- 2) Блочный шифр RC5 (3 час.).
- 3) Блочный шифр RC6 (3 час.).
- 4) Блочный шифр IDEA (3 час.).

Темы для самостоятельного изучения входят в раздел № 3 изучаемой дисциплины.

10. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ

Учебным планом не предусмотрены.

11. РЕЙТИНГОВАЯ СИСТЕМА ДЛЯ ОЦЕНКИ УСПЕВАЕМОСТИ СТУДЕНТОВ

Курс 4, семестр 7

Контроль обучения – Экзамен.

Максимальный семестровый рейтинг – 100 баллов.

По дисциплине «Информационная безопасность» итоговой формой отчетности в 7 семестре является **экзамен**, все 100 баллов входят в семестровую составляющую.

Для стимулирования плановости работы студента в семестре в раскладку баллов по элементам контроля введен компонент своевременности, который применяется только для студентов, без опозданий, отчитывающихся по предусмотренным элементам контроля (лабораторные работы).

На протяжении всего семестра текущая успеваемость **оценивается только в баллах** нарастающим итогом, в том числе и результаты контрольных точек.

В таблице 11.1 содержится распределение баллов в течение 7 семестра для дисциплины «Информационная безопасность», завершающейся **экзаменом** и содержащей 14 лекций (28 часов), 6 лабораторных работ (26 часов), 9 практических занятий и 3 итоговых теста во время проведения двух контрольных точек и между ними. В таблице 11.2 представлен пересчет суммы баллов по 1 и 2 контрольной точке в традиционную оценку.

Таблица 11.1 – Дисциплина «Информационная безопасность» (**экзамен**, лекции, лабораторные работы, практические занятия)

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|--|--|---|---|------------------|
| Посещение занятий | 4 | 3 | 3 | 10 |
| Тестовый контроль | 6 | 6 | 6 | 18 |
| Выполнение и защита лабораторных работ | 6 | 12 | 12 | 30 |
| Компонент своевременности | 4 | 4 | 4 | 12 |
| Итого максимум за период: | 20 | 25 | 25 | 70 |
| Сдача экзамена (максимум) | | | | 30 |
| Нарастающим итогом | 20 | 45 | 70 | 100 |

По результатам текущего контроля формируется допуск студента к итоговому контролю – экзамену по дисциплине. Экзамен осуществляется в форме опроса по теоретической части дисциплины. В составе суммы баллов, полученной студентом по дисциплине, заканчивающейся **экзаменом**, экзаменационная составляющая должна быть не менее 10 баллов. В противном случае экзамен считается не сданным, студент в установленном в ТУСУРе порядке обязан его пересдать.

Методика выставления баллов за ответы на **экзамене** определяется из расчета до **10 баллов** за каждый из **3 вопросов в билете**.

Неудовлетворительной сдачей экзамена считается экзаменационная составляющая **менее 10 баллов**. При неудовлетворительной сдаче экзамена (<10 баллов) или неявке на экзамен экзаменационная составляющая приравнивается к нулю (0).

Таблица 11.2 – Пересчет суммы баллов по 1 и 2 контрольной точке в традиционную оценку

| Оценка (ГОС) | Сумма баллов, на 1-ую контрольную точку с начала семестра | Сумма баллов, на 2-ую контрольную точку за период между 1КТ и 2КТ |
|-------------------------|---|---|
| 5 (отлично) | 18 – 20 | 40 – 45 |
| 4 (хорошо) | 15 – 17 | 31 – 39 |
| 3 (удовлетворительно) | 10 – 14 | 27 – 30 |
| 2 (неудовлетворительно) | Ниже 10 баллов | Ниже 27 баллов |

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|--|--|-------------------------|
| 5 (отлично) | 90 – 100 | A (отлично) |
| 4 (хорошо) | 85 – 89 | B (очень хорошо) |
| | 75 – 84 | C (хорошо) |
| | 70 – 74 | D (удовлетворительно) |
| 3 (удовлетворительно) | 65 – 69 | E (посредственно) |
| | 60 – 64 | F (неудовлетворительно) |
| 2 (неудовлетворительно), (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

12. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

12.1 Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (30 экз.)

12.2 Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (25 экз.)

2. Партыка Т.Л. Информационная безопасность: Учебное пособие. 3-е изд., исп. и доп. - М.: Форум, 2007. – 367 с. (20 экз.)

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (50 экз.)

4. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. : С. А. Клейменов. - М.: Academia, 2006. - 330 с. (30 экз.)

5. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М.: Academia, 2006. - 253 с. (50 экз.)

6. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с. (80 экз.)

7. Смарт Н. Криптография: учебник для вузов: пер. с англ. / пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М.: Техносфера, 2005. – 525 с. (11 экз.)

12.3 Учебно-методические пособия и программное обеспечение

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям. – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-pract.pdf>

2. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ. – Томск: ТУСУР, 2011. – 6 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-lab.pdf>

3. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов. – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-work.pdf>

12.4 Программное обеспечение

Лицензионное и свободно распространяемое программное обеспечение: ОС MS Windows XP, MS Office 2007, LibreOffice, ER-win.

12.5 Базы данных, информационно-справочные и поисковые системы

Информационно-справочные и поисковые системы сети Интернет.

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения практических занятий и лабораторных работ по дисциплине используются персональный ПК с процессором Pentium 4 и выше, установленные в компьютерных классах кафедры АСУ 437, 438, 439.

Приложение к рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Томский государственный университет систем управления и радиоэлектроники

У Т В Е Р Ж Д А Ю

Проректор по учебной работе

_____ П.Е. Троян

« ____ » _____ 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной образовательной программы: _____ бакалавриат _____

Направление(я) подготовки (специальность): _____ 09.03.03 – Прикладная информатика _____

Профиль: _____ Прикладная информатика в экономике _____

Форма обучения: _____ очная _____

Факультет: _____ ФСУ, Факультет систем управления _____

Кафедра: _____ АСУ, Кафедра автоматизированных систем управления _____

Курс _____ 4 _____

Семестр _____ 7 _____

Учебный план набора _____ 2016 и последующих лет _____

Экзамен: _____ 7 семестр _____

Томск 2016

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенции |
|--------------|---|---|
| ОПК-4 | способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4). | <p>Должен знать:</p> <ul style="list-style-type: none"> • основные понятия и направления в защите компьютерной информации, • принципы защиты информации, • принципы классификации и примеры угроз безопасности компьютерным системам, • современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, • основные инструменты обеспечения многоуровневой безопасности в информационных системах. <p>Должен уметь:</p> <ul style="list-style-type: none"> • выявлять угрозы информационной безопасности, • обосновывать организационно-технические мероприятия по защите информации в ИС, • проводить анализ защищенности компьютера и сетевой среды; • организовывать безопасную работу в Интернет; • использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов. <p>Должен владеть:</p> <ul style="list-style-type: none"> • навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации. |

2. Реализация компетенций

Компетенция ОПК-4

ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 2.

Таблица 2– Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|--|---|
| Содержание этапов | – Знает методы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности. | – Умеет решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности. | – Владеет методами решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности. |
| Виды занятий | <ul style="list-style-type: none"> • Лекции; • Практические занятия • Групповые консультации. | <ul style="list-style-type: none"> • Лабораторные работы; • Выполнение домашнего задания; • Самостоятельная работа студентов | <ul style="list-style-type: none"> • Лабораторные работы. |
| Используемые средства оценивания | <ul style="list-style-type: none"> • Тест; • Контрольная работа; • Выполнение домашнего задания; • Экзамен. | <ul style="list-style-type: none"> • Оформление отчетности и защита лабораторных работ; • Оформление и защита домашнего задания; • Конспект самостоятельной работы. | <ul style="list-style-type: none"> • Защита лабораторных работ • Защита курсового проекта, • Экзамен |

Общие характеристики показателей и критериев оценивания компетенции на всех этапах приведены в таблице 3.

Таблица 3 – Общие характеристики показателей и критериев оценивания компетенции по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|--|---|---|--|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования | Берет ответственность за завершение задач в исследовании, приспособляет свое поведение к обстоятельствам в решении проблем |
| Удовлетворительно (пороговый уровень) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми для выполнения простых задач | Работает при прямом наблюдении |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Показатели и критерии | Знать | Уметь | Владеть |
|--------------------------------------|--|--|---|
| Отлично (высокий уровень) | <ul style="list-style-type: none"> – Знает основные понятия и направления в защите компьютерной информации; – Знает принципы защиты информации; – Знает принципы классификации и примеры угроз безопасности компьютерным системам; – Знает современные подходы к защите продуктов и систем ин- | <p>Умеет конфигурировать встроенные средства безопасности в операционной системе, Умеет проводить анализ защищенности компьютера и сетевой среды;</p> <p>Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифро-</p> | Владеет навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации. |

| | | | |
|---|--|---|---|
| | <p>формационных технологий;</p> <p>– Знает основные инструменты обеспечения многоуровневой безопасности в информационных системах.</p> | <p>вой подписи;</p> <p>Умеет устанавливать и использовать один из межсетевых экранов;</p> <p>Умеет организовывать регистрацию пользователей в сетевой операционной системе;</p> <p>Умеет организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа,</p> <p>Умеет организовывать безопасную работу в Интернет;</p> <p>Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет;</p> <p>Умеет использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;</p> | |
| <p>Хорошо (базовый уровень)</p> | <p>Знает основные понятия и направления в защите компьютерной информации;</p> <p>Знает принципы защиты информации;</p> <p>Знает принципы классификации и примеры угроз безопасности компьютерным системам;</p> <p>Знает современные подходы к защите продуктов и систем информационных технологий;</p> <p>Имеет представление о основных инструментах обеспечения многоуровневой безопасности в информационных системах.</p> | <p>Умеет конфигурировать встроенные средства безопасности в операционной системе;</p> <p>Умеет проводить анализ защищенности компьютера и сетевой среды;</p> <p>Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи;</p> <p>Умеет устанавливать и использовать один из межсетевых экранов;</p> <p>Умеет организовывать регистрацию пользователей в сетевой операционной системе;</p> | <p>– Хорошо владеет навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.</p> |

| | | | |
|---|---|---|--|
| | | <p>Умеет организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;</p> <p>Умеет организовывать безопасную работу в Интернет;</p> <p>Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет;</p> <p>Умеет использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.</p> | |
| <p>Удовлетворительно (пороговый уровень)</p> | <p>Понимает важность защиты информации;</p> <p>Знает основные понятия и направления в защите компьютерной информации;</p> <p>Знает базовые принципы классификации и примеры угроз безопасности компьютерным системам;</p> <p>Имеет представление о современном подходе к защите продуктов и систем информационных технологий;</p> <p>Знает основные инструменты обеспечения безопасности в информационных системах.</p> | <p>Умеет конфигурировать встроенные средства безопасности в операционной системе;</p> <p>Умеет проводить анализ защищенности компьютера и сетевой среды;</p> <p>Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи;</p> <p>Умеет устанавливать и использовать один из межсетевых экранов;</p> <p>Умеет организовывать регистрацию пользователей в сетевой операционной системе;</p> <p>Умеет организовывать безопасную работу в Интернет;</p> <p>Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет;</p> <p>Умеет использовать</p> | <p>Владеет основными приемами применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.</p> |

| | | | |
|--|--|---|--|
| | | средства защиты данных от разрушающих программных воздействий компьютерных вирусов. | |
|--|--|---|--|

3. Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются следующие материалы: типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в составе, приведенном ниже.

Темы лабораторных работ

- 1) Блочное симметричное шифрование.
- 2) Изучение ППП систем криптографической защиты информации, классическая криптография.
- 3) Асимметричное шифрование.
- 4) Электронная цифровая подпись (ЭЦП).
- 5) Практическое применение криптографии с открытым ключом. Пакет PGP.
- 6) Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI.

Темы практических занятий

- 1) Принципы защиты информации. Методы оценки уязвимости информации.
- 2) Федеральное законодательство о защите информации.
- 3) Государственные стандарты и руководящие документы.
- 4) Современные приложения криптографии.
- 5) Математические основы криптографических методов.
- 6) Методы идентификации и аутентификации.
- 7) Основные технологии построения защищенных информационных систем.
- 8) Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности.
- 9) Комплексная система обеспечения информационной безопасности.

Пример типовых вопросов по тестам

1. *Вопрос:*

К какой главе УК РФ относятся ст. 272, ст. 273, ст. 274 в области информационной безопасности:

Выберите один из 3 вариантов ответа:

- 1) 25
- 2) 28
- 3) 27

2. *Вопрос:*

Что такое политика информационной безопасности организации:

Выберите один из 3 вариантов ответа:

- 1) совокупность механизмов компьютерных систем
- 2) инструкции администраторам по настройке информационных систем
- 3) набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию

3. *Вопрос:*

**К биометрической системе защиты относятся:
(выберите несколько вариантов ответа)**

4. *Выберите несколько из 5 вариантов ответа:*

- 1) Защита паролем
- 2) Физическая защита данных
- 3) Антивирусная защита
- 4) Идентификация по радужной оболочке глаз
- 5) Идентификация по отпечаткам пальцев

5. *Вопрос:*

Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

6. *Выберите один из 5 вариантов ответа:*

- 1) Загрузочный вирус
- 2) Макровирус
- 3) Файловый вирус
- 4) Сетевой червь
- 5) Троян

Темы для самостоятельной работы (темы рефератов)

- 1) Блочный шифр BLOWFISH.
- 2) Блочный шифр RC5.
- 3) Блочный шифр RC6.
- 4) Блочный шифр IDEA.

Вопросы для подготовки к экзамену

Экзаменационные вопросы:

- 1) Законодательные и нормативные документы информационной безопасности.
- 2) Алгоритмы симметричного шифрования.
- 3) Шифрование информации на основе сети Фейштеля.
- 4) Режимы выполнения алгоритмов симметричного шифрования.
- 5) Потокное шифрование.
- 6) Алгоритмы потокового шифрования.
- 7) Криптографические хеш-функции.
- 8) Хеш-функции на основе блочных шифров.
- 9) Функция хеширования MD4.
- 10) Основные теоремы теории чисел.
- 11) Наибольший общий делитель. Алгоритмы Евклида.
- 12) Односторонняя функция.
- 13) Криптография с открытым ключом.
- 14) Задача распределения ключей.

- 15) Алгоритм Диффи-Хеллмана.
- 16) Комбинированная криптосистема.
- 17) Электронная цифровая подпись.
- 18) Инфраструктура открытых ключей.
- 19) Сертификат открытого ключа.
- 20) Идентификация, аутентификация, авторизация.
- 21) Методы аутентификации, использующие одноразовые и многократные пароли.
- 22) Методы аутентификации, использующие симметричные и асимметричные алгоритмы.
- 23) Биометрическая аутентификация пользователя.
- 24) Межсетевые экраны. Функции межсетевых экранов.
- 25) Основные типы межсетевых экранов.
- 26) Виртуальные частные сети.

Примеры задач на экзамен:

1. С помощью шифра Шамира пользователь А передает пользователю В число 10 ($m = 10$). Для шифрования используются следующие параметры: $p = 19$, $s_A = 11$, $s_B = 5$.

Вычислите недостающие параметры и приведите все расчеты, которые выполняются в процессе передачи сообщения от А к В.

2. Пользователи А и В формируют сессионный ключ с помощью метода Диффи-Хеллмана. Для этого они выбрали общие параметры: $p = 13$, $g = 11$. Затем, пользователь А выбрал секретный ключ $x_A = 7$, а пользователь В выбрал секретный ключ $x_B = 5$.

Необходимо вычислить недостающие параметры и определить секретный сессионный ключ.

3. Пользователь А готовится передать пользователю В сообщение М, состоящее из числа 5 ($M = 5$) в зашифрованном виде. Для шифрования предполагается использовать алгоритм RSA со следующими параметрами: $p = 11$, $q = 7$, $e = 7$.

Вычислите открытый и закрытый ключи пользователя и приведите передаваемое сообщение в зашифрованном виде и сообщение, которое пользователь получит после расшифровывания шифротекста.

4. Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, в составе:

- Учебные пособия приведены в рабочей программе в разделе 12.1;
- Дополнительная литература приведена в рабочей программе в разделе 12.2;
- Методические указания по практике приведены в рабочей программе в разделе 12.3.

Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (30 экз.)

Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (25 экз.)

2. Партыка Т.Л. Информационная безопасность: Учебное пособие. 3-е изд., исп. и доп. - М.: Форум, 2007. – 367 с. (20 экз.)

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (50 экз.)

4. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред.: С. А. Клейменов. - М.: Academia, 2006. - 330 с. (30 экз.)

5. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М.: Academia, 2006. - 253 с. (50 экз.)

6. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др.] – М.: Горячая линия – Телеком, 2006. – 544 с. (80 экз.)

7. Смарт Н. Криптография: учебник для вузов: пер. с англ. / пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М.: Техносфера, 2005. – 525 с. (11 экз.)

Методические указания к практическим занятиям

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям. – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-pract.pdf>

Методические указания к лабораторным работам

1. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ. – Томск: ТУСУР, 2011. – 6 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-lab.pdf>

Методические указания по самостоятельной работе

1. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-work.pdf>