**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **09.03.03 Прикладная информатика**
Направленность (профиль): **Прикладная информатика в экономике**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **АСУ, Кафедра автоматизированных систем управления**
Курс: **5**
Семестр: **10**
Учебный план набора 2016 года

Распределение рабочего времени

| № | Виды учебной деятельности | 10 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 8 | 8 | часов |
| 2 | Практические занятия | 4 | 4 | часов |
| 3 | Лабораторные работы | 6 | 6 | часов |
| 4 | Всего аудиторных занятий | 18 | 18 | часов |
| 5 | Из них в интерактивной форме | 6 | 6 | часов |
| 6 | Самостоятельная работа | 153 | 153 | часов |
| 7 | Всего (без экзамена) | 171 | 171 | часов |
| 8 | Подготовка и сдача экзамена | 9 | 9 | часов |
| 9 | Общая трудоемкость | 180 | 180 | часов |
| | | 5.0 | 5.0 | З.Е |

Контрольные работы: 10 семестр - 1
Экзамен: 10 семестр

Томск 2017

Согласована на портале № 17482

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «24» 1 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.03 Прикладная информатика, утвержденного 12 марта 2015 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

| | | |
|---|---|---|
| профессор каф. АСУ | _____ | А. Н. Горитов |
| Заведующий обеспечивающей каф. АСУ | _____ | А. М. Кориков |

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

| | | |
|---|---|---|
| Декан ЗиВФ | _____ | И. В. Осипов |
| Заведующий выпускающей каф. АСУ | _____ | А. М. Кориков |

Эксперты:

| | | |
|---|---|---|
| Доцент Каф. АСУ | _____ | А. И. Исакова |

Согласована на портале № 17482

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

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

### 1.2. Задачи дисциплины

– 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 ОПОП

Дисциплина «Информационная безопасность» (Б1.Б.16) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Дискретная математика, Математика, Мировые информационные ресурсы, Операционные системы, Основы алгоритмизации и программирования, Проектирование информационных систем.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– 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;

В результате изучения дисциплины студент должен:

– **знать** основные понятия и принципы защиты информации; современные подходы к защите продуктов и систем информационных технологий; основные методы обеспечения многоуровневой безопасности в информационных системах.

– **уметь** выявлять угрозы информационной безопасности; использовать средства защиты данных для организации безопасной работы компьютеров.

– **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 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 10 семестр |
| Аудиторные занятия (всего) | 18 | 18 |
| Лекции | 8 | 8 |
| Практические занятия | 4 | 4 |
| Лабораторные работы | 6 | 6 |
| Из них в интерактивной форме | 6 | 6 |
| Самостоятельная работа (всего) | 153 | 153 |
| Оформление отчетов по лабораторным работам | 14 | 14 |
| Проработка лекционного материала | 108 | 108 |
| Самостоятельное изучение тем (вопросов) теоретической части курса | 15 | 15 |

Согласована на портале № 17482

| | | |
|---|---|---|
| Подготовка к практическим занятиям, семинарам | 8 | 8 |
| Выполнение контрольных работ | 8 | 8 |
| Всего (без экзамена) | 171 | 171 |
| Подготовка и сдача экзамена | 9 | 9 |
| Общая трудоемкость ч | 180 | 180 |
| Зачетные Единицы | 5.0 | 5.0 |

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|---|
| 10 семестр | | | | | | |
| 1 Введение в информационную безопасность. | 1 | 2 | 0 | 8 | 11 | ОПК-4 |
| 2 Математические методы и модели в задачах защиты информации. | 1 | 2 | 4 | 53 | 60 | ОПК-4 |
| 3 Математические основы криптографических методов. | 1 | 0 | 0 | 16 | 17 | ОПК-4 |
| 4 Криптография с открытым ключом. | 1 | 0 | 2 | 22 | 25 | ОПК-4 |
| 5 Методы идентификации и аутентификации пользователей. | 1 | 0 | 0 | 12 | 13 | ОПК-4 |
| 6 Межсетевые экраны и VPN сети. | 1 | 0 | 0 | 12 | 13 | ОПК-4 |
| 7 Защита компьютерных систем от вредоносных программ. | 1 | 0 | 0 | 14 | 15 | ОПК-4 |
| 8 Комплексная защита информации. | 1 | 0 | 0 | 16 | 17 | ОПК-4 |
| Итого за семестр | 8 | 4 | 6 | 153 | 171 | |
| Итого | 8 | 4 | 6 | 153 | 171 | |

### 5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 10 семестр | | | |

Согласована на портале № 17482

| | | | |
|---|---|---|---|
| 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. Основы российского законодательства в сфере защиты информации. | 1 | ОПК-4 |
| | Итого | 1 | |
| 2 Математические методы и модели в задачах защиты информации. | Основные понятия и определения криптографии. Классификация методов шифрования. Блочные шифры. Алгоритмы блочного шифрования. Режимы выполнения алгоритмов шифрования. Вопросы стойкости блочных шифров. Потоковые шифры. Основные понятия. Алгоритмы потокового шифрования. | 1 | ОПК-4 |
| | Итого | 1 | |
| 3 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. | 1 | ОПК-4 |
| | Итого | 1 | |
| 4 Криптография с открытым ключом. | Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Задача распределения ключей. Алгоритмы шифрования с открытым ключом. Вопросы стойкости. Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Сертификат открытого ключа. | 1 | ОПК-4 |
| | Итого | 1 | |
| 5 Методы идентификации и аутентификации пользователей. | Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя. | 1 | ОПК-4 |
| | Итого | 1 | |
| 6 Межсетевые экраны и VPN сети. | Межсетевые экраны. Режимы функционирования межсетевых экранов и их | 1 | ОПК-4 |

Согласована на портале № 17482

| | | | |
|---|---|---|---|
| | основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей. Достоинства применения технологии виртуальных защищенных сетей. | | |
| | Итого | 1 | |
| 7 Защита компьютерных систем от вредоносных программ. | Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них. | 1 | ОПК-4 |
| | Итого | 1 | |
| 8 Комплексная защита информации. | Концепция комплексной защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. | 1 | ОПК-4 |
| | Итого | 1 | |
| Итого за семестр | | 8 | |

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

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

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Предшествующие дисциплины | | | | | | | | |
| 1 Дискретная математика | + | + | | + | + | + | + | + |
| 2 Математика | + | + | + | + | + | + | + | + |
| 3 Мировые информационные ресурсы | + | + | + | + | + | + | + | + |
| 4 Операционные системы | | | | | + | + | + | + |
| 5 Основы алгоритмизации и программирования | + | + | + | + | + | + | + | + |
| 6 Проектирование информационных систем | + | + | + | + | + | + | + | + |

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| | Виды занятий | Формы контроля |
|---|---|---|

Согласована на портале № 17482

| Компетенции | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | |
|---|---|---|---|---|---|
| ОПК-4 | + | + | + | + | Контрольная работа, Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Тест |

## 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

| Методы | Интерактивные практические занятия | Интерактивные лабораторные занятия | Интерактивные лекции | Всего |
|---|---|---|---|---|
| 10 семестр | | | | |
| Поисковый метод | 2 | | | 2 |
| Мозговой штурм | | 2 | | 2 |
| Презентации с использованием слайдов с обсуждением | | | 2 | 2 |
| Итого за семестр: | 2 | 2 | 2 | 6 |
| Итого | 2 | 2 | 2 | 6 |

## 7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 10 семестр | | | |
| 2 Математические методы и модели в задачах защиты информации. | Изучение ППП систем криптографической защиты информации, классическая криптография | 4 | ОПК-4 |
| | Итого | 4 | |
| 4 Криптография с открытым ключом. | Практическое применение криптографии с открытым ключом. Пакет PGP | 2 | ОПК-4 |
| | Итого | 2 | |
| Итого за семестр | | 6 | |

Согласована на портале № 17482

## 8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 10 семестр | | | |
| 1 Введение в информационную безопасность. | Базовые понятия информационной безопасности | 2 | ОПК-4 |
| | Итого | 2 | |
| 2 Математические методы и модели в задачах защиты информации. | Методы защиты информации | 2 | ОПК-4 |
| | Итого | 2 | |
| Итого за семестр | | 4 | |

## 9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 10 семестр | | | | |
| 1 Введение в информационную безопасность. | Проработка лекционного материала | 8 | ОПК-4 | Опрос на занятиях |
| | Итого | 8 | | |
| 2 Математические методы и модели в задачах защиты информации. | Выполнение контрольных работ | 8 | ОПК-4 | Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен |
| | Подготовка к практическим занятиям, семинарам | 6 | | |
| | Самостоятельное изучение тем (вопросов) теоретической части курса | 15 | | |
| | Проработка лекционного материала | 16 | | |
| | Оформление отчетов по лабораторным работам | 8 | | |
| | Итого | 53 | | |
| 3 Математические основы криптографических методов. | Подготовка к практическим занятиям, семинарам | 2 | ОПК-4 | Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного | 14 | | |

Согласована на портале № 17482

| | | | | |
|---|---|---|---|---|
| | материала | | | |
| | Итого | 16 | | |
| 4 Криптография с открытым ключом. | Проработка лекционного материала | 16 | ОПК-4 | Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен |
| | Оформление отчетов по лабораторным работам | 6 | | |
| | Итого | 22 | | |
| 5 Методы идентификации и аутентификации пользователей. | Проработка лекционного материала | 12 | ОПК-4 | Опрос на занятиях, Тест, Экзамен |
| | Итого | 12 | | |
| 6 Межсетевые экраны и VPN сети. | Проработка лекционного материала | 12 | ОПК-4 | Опрос на занятиях, Тест, Экзамен |
| | Итого | 12 | | |
| 7 Защита компьютерных систем от вредоносных программ. | Проработка лекционного материала | 14 | ОПК-4 | Опрос на занятиях, Тест, Экзамен |
| | Итого | 14 | | |
| 8 Комплексная защита информации. | Проработка лекционного материала | 16 | ОПК-4 | Опрос на занятиях, Тест, Экзамен |
| | Итого | 16 | | |
| Итого за семестр | | 153 | | |
| | Подготовка и сдача экзамена | 9 | | Экзамен |
| Итого | | 162 | | |

### 9.1. Темы контрольных работ

1. Организация защиты информации.
2. Правовое обеспечение защиты информации.
3. Основные модели политик безопасности.
4. Технические средства защиты информации.
5. Инфраструктура открытых ключей.

### 9.2. Темы для самостоятельного изучения теоретической части курса

1. Блочные шифры BLOWFISH, RC5, RC6 и IDEA

## 10. Курсовая работа (проект)

Не предусмотрено РУП

## 11. Рейтинговая система для оценки успеваемости студентов

Не предусмотрено

## 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. (наличие в библиотеке ТУСУР - 30 экз.)

### 12.2. Дополнительная литература

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

2. 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. –

Согласована на портале № 17482

144 с. (наличие в библиотеке ТУСУР - 50 экз.)

3. 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. (наличие в библиотеке ТУСУР - 30 экз.)

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

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

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

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

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

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

#### 12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

### 12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Информационно-справочные и поисковые системы сети Интернет.
2. Лицензионное и свободно распространяемое программное обеспечение: ОС MS Windows XP, MS Office 2007, LibreOffice, CodeBlocks.

## 13. Материально-техническое обеспечение дисциплины

### 13.1. Общие требования к материально-техническому обеспечению дисциплины

#### 13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

#### 13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, рас-

Согласована на портале № 17482

положенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. 438. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

#### 13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. 439. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

#### 13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 74, 1 этаж, ауд. 100. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

### 13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

## 14. Фонд оценочных средств

### 14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

### 14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

| Категории студентов | Виды дополнительных оценочных | Формы контроля и оценки |
|---|---|---|

Согласована на портале № 17482

| | средств | результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

### 14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 17482

**Приложение 1**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

# Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **09.03.03 Прикладная информатика**
Направленность (профиль): **Прикладная информатика в экономике**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **АСУ, Кафедра автоматизированных систем управления**
Курс: **5**
Семестр: **10**

Учебный план набора 2016 года

Разработчики:
- профессор каф. АСУ А. Н. Горитов

Экзамен: 10 семестр

Томск 2017

Согласована на портале № 17482

## 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 компетенций |
|---|---|---|
| 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 | Должен знать основные понятия и принципы защиты информации; современные подходы к защите продуктов и систем информационных технологий; основные методы обеспечения многоуровневой безопасности в информационных системах.;<br>Должен уметь выявлять угрозы информационной безопасности; использовать средства защиты данных для организации безопасной работы компьютеров. ;<br>Должен владеть навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.; |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций 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, приспосабливает 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 |

## 2 Реализация компетенций

### 2.1 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.

Согласована на портале № 17482

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – 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 | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Контрольная работа;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Конспект самоподготовки;<br>• Тест;<br>• Экзамен; | • Контрольная работа;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Конспект самоподготовки;<br>• Тест;<br>• Экзамен; | • Отчет по лабораторной работе;<br>• Экзамен; |

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • Знает методы эффективного решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и обеспечения информационной безопасности на высоком уровне; | • Умеет использовать средства защиты данных для организации безопасной работы компьютера при различной степени сложности; | • Владеет навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации; |
| Хорошо (базовый уровень) | • Знает основные методы решения стандартных задач профессио- | • Умеет использовать основные средства защиты данных для орга- | • Хорошо владеет навыками применения методов и средств защиты |

Согласована на портале № 17482

| | | | |
|---|---|---|---|
| | нальной деятельности с применением информационно-коммуникационных технологий и обеспечения информационной безопасности на хорошем уровне; | низации безопасной работы компьютера в случаях средней сложности; | информации для обеспечения информационной безопасности на предприятии или организации; |
| Удовлетворительно (пороговый уровень) | • Знает простые методы решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и обеспечения информационной безопасности на удовлетворительном уровне; | • Умеет использовать базовые средства защиты данных для организации безопасной работы компьютера в простых случаях; | • Владеет основными приемами применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации; |

## 3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются 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 следующем составе.

### 3.1 Вопросы на самоподготовку

- Блочный шифр BLOWFISH
- Блочный шифр RC5
- Блочный шифр RC6
- Блочный шифр IDEA

### 3.2 Тестовые задания

- 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
- 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
- К биометрической системе защиты относятся: (выберите несколько вариантов ответа) 1) Защита паролем 2) Физическая защита данных 3) Антивирусная защита 4) Идентификация по радужной оболочке глаз 5) Идентификация по отпечаткам пальцев
- Вирус внедряется в исполняемые файлы и при их запуске активируется. Это... 1) Загрузочный вирус 2) Макровирус 3) Файловый вирус 4) Сетевой червь 5) Троян

### 3.3 Темы опросов на занятиях

- Блочные шифры BLOWFISH, RC5, RC6 и IDEA

### 3.4 Экзаменационные вопросы

- Законодательные и нормативные документы информационной безопасности.
- Алгоритмы симметричного шифрования.
- Шифрование информации на основе сети Фейштеля.
- Режимы выполнения алгоритмов симметричного шифрования.
- Потоковое шифрование.
- Алгоритмы потокового шифрования.
- Криптографические хеш-функции.

Согласована на портале № 17482

– Хеш-функции на основе блочных шифров.
– Функция хеширования MD4.
– Основные теоремы теории чисел.
– Наибольший общий делитель. Алгоритмы Евклида.
– Односторонняя функция.
– Криптография с открытым ключом.
– Задача распределения ключей.
– Алгоритм Диффи-Хеллмана.
– Комбинированная криптосистема.
– Электронная цифровая подпись.
– Инфраструктура открытых ключей.
– Сертификат открытого ключа.
– Идентификация, аутентификация, авторизация.
– Методы аутентификации, использующие одноразовые и многоразовые пароли.
– Методы аутентификации, использующие симметричные и асимметричные алгоритмы.
– Биометрическая аутентификация пользователя.
– Межсетевые экраны. Функции межсетевых экранов.
– Основные типы межсетевых экранов.
– Виртуальные частные сети.

### 3.5 Темы контрольных работ

– Организация защиты информации.
– Правовое обеспечение защиты информации.
– Основные модели политик безопасности.
– Технические средства защиты информации.
– Инфраструктура открытых ключей.

### 3.6 Темы лабораторных работ

– Изучение ППП систем криптографической защиты информации, классическая криптография
– Практическое применение криптографии с открытым ключом. Пакет PGP

## 4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

### 4.1. Основная литература

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

### 4.2. Дополнительная литература

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

2. 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. (наличие в библиотеке ТУСУР - 50 экз.)

3. 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. (наличие в библиотеке ТУСУР - 30 экз.)

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

Согласована на портале № 17482

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

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

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

### 4.3. Обязательные учебно-методические пособия

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

### 4.4. Базы данных, информационно справочные и поисковые системы

1. Информационно-справочные и поисковые системы сети Интернет.

2. Лицензионное и свободно распространяемое программное обеспечение: ОС MS Windows XP, MS Office 2007, LibreOffice, CodeBlocks.

Согласована на портале № 17482