**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

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Прикладная криптография

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2013 года

Распределение рабочего времени

| № | Виды учебной деятельности | 8 семестр | 9 семестр | Всего | Единицы |
|---|---|---|---|---|---|
| 1 | Лекции | 2 | 4 | 6 | часов |
| 2 | Лабораторные работы | 4 | 8 | 12 | часов |
| 3 | Всего аудиторных занятий | 6 | 12 | 18 | часов |
| 4 | Из них в интерактивной форме | 2 | 4 | 6 | часов |
| 5 | Самостоятельная работа | 30 | 56 | 86 | часов |
| 6 | Всего (без экзамена) | 36 | 68 | 104 | часов |
| 7 | Подготовка и сдача зачета | | 4 | 4 | часов |
| 8 | Общая трудоемкость | 36 | 72 | 108 | часов |
| | | 1.0 | 2.0 | 3.0 | З.Е |

Контрольные работы: 9 семестр - 1
Зачет: 9 семестр

Томск 2017

Согласована на портале № 21191

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от « 1 » 6 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16 января 2017 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Программист каф. КИБЭВС _____ И. Ю. Поляков

Доцент каф. КИБЭВС _____ . . Конев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

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

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперт:

Декан, к.н. каф. КИБЭВС _____ . . Давыдова

Согласована на портале № 21191

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Основная цель дисциплины «Прикладная криптография» — формирование у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

### 1.2. Задачи дисциплины

– сформировать представление об основных проблемах, связанных с практическим использование криптографических методов защиты информации; изучить основные криптографические протоколы; изучить инфраструктуру открытого ключа.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Прикладная криптография» (Б1.В.ДВ.5.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Основы информационной безопасности.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-2 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа;

В результате изучения дисциплины студент должен:

– **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.

– **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.

– **владеть** навыками использования типовых криптографических алгоритмов.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры | |
|---|---|---|---|
| | | 8 семестр | 9 семестр |
| Аудиторные занятия (всего) | 18 | 6 | 12 |
| Лекции | 6 | 2 | 4 |
| Лабораторные работы | 12 | 4 | 8 |
| Из них в интерактивной форме | 6 | 2 | 4 |
| Самостоятельная работа (всего) | 86 | 30 | 56 |
| Оформление отчетов по лабораторным работам | 11 | 11 | |
| Проработка лекционного материала | 8 | 6 | 2 |
| Подготовка к практическим занятиям, семинарам | 48 | 13 | 35 |
| Выполнение контрольных работ | 19 | | 19 |
| Всего (без экзамена) | 104 | 36 | 68 |
| Подготовка и сдача зачета | 4 | | 4 |
| Общая трудоемкость ч | 108 | 36 | 72 |

Согласована на портале № 21191

| | | | |
|---|---|---|---|
| Зачетные Единицы | 3.0 | 1.0 | 2.0 |

## 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 | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|
| 8 семестр | | | | | |
| 1 Криптографические протоколы: общие понятия. | 1 | 4 | 10 | 15 | ПСК-2 |
| 2 Протоколы распределения ключей. | 1 | 0 | 9 | 10 | ПСК-2 |
| 3 Инфраструктура открытого ключа. | 0 | 0 | 11 | 11 | ПСК-2 |
| Итого за семестр | 2 | 4 | 30 | 36 | |
| 9 семестр | | | | | |
| 4 Протоколы идентификации и аутентификации. | 2 | 8 | 20 | 30 | ПСК-2 |
| 5 Безопасный канал обмена сообщениями. | 2 | 0 | 19 | 21 | ПСК-2 |
| 6 Практические аспекты реализации средств криптографической защиты информации. | 0 | 0 | 17 | 17 | ПСК-2 |
| Итого за семестр | 4 | 8 | 56 | 68 | |
| Итого | 6 | 12 | 86 | 104 | |

### 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 |
|---|---|---|---|
| 8 семестр | | | |
| 1 Криптографические протоколы: общие понятия. | Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы. | 1 | ПСК-2 |
| | Итого | 1 | |
| 2 Протоколы распределения | Управление секретными ключами. Рас- | 1 | ПСК-2 |

Согласована на портале № 21191

| | | | |
|---|---|---|---|
| ключей. | пределение секретных ключей. | | |
| | Итого | 1 | |
| Итого за семестр | | 2 | |
| 9 семестр | | | |
| 4 Протоколы идентификации и аутентификации. | Лекция "Протоколы идентификации и аутентификации" | 2 | ПСК-2 |
| | Итого | 2 | |
| 5 Безопасный канал обмена сообщениями. | Лекция "безопасный канал обмена сообщениями" | 2 | ПСК-2 |
| | Итого | 2 | |
| Итого за семестр | | 4 | |
| Итого | | 6 | |

### 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 |
| Предшествующие дисциплины | | | | | | |
| 1 Основы информационной безопасности | + | | | | | |

### 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

| Компетенции | Виды занятий | | | Формы контроля |
|---|---|---|---|---|
| | Лекции | Лабораторные работы | Самостоятельная работа | |
| ПСК-2 | + | + | + | Контрольная работа, Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест, Отчет по практическому занятию |

## 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в та-

Согласована на портале № 21191

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

| Методы | Интерактивные лабораторные занятия | Интерактивные лекции | Всего |
|---|---|---|---|
| 8 семестр | | | |
| Презентации с использованием слайдов с обсуждением | 1 | | 1 |
| Презентации с использованием мультимедиа с обсуждением | 1 | | 1 |
| Итого за семестр: | 2 | 0 | 2 |
| 9 семестр | | | |
| Презентации с использованием слайдов с обсуждением | 2 | 2 | 4 |
| Итого за семестр: | 2 | 2 | 4 |
| Итого | 4 | 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 |
|---|---|---|---|
| 8 семестр | | | |
| 1 Криптографические протоколы: общие понятия. | Установка и настройка Active Directory Certificate Services.Целью данной лабораторной является ознакомление с процессом установки службы Active Directory Certificate Services (службы сертификации) и особенностями работы с сертификатами. | 4 | ПСК-2 |
| | Итого | 4 | |
| Итого за семестр | | 4 | |
| 9 семестр | | | |
| 4 Протоколы идентификации и аутентификации. | Рассматриваются технические меры повышения защищенности систем. Изучаются методы, лежащие в основе соответствующих средств и механизмов в аспектах идентификации и аутентификации. | 8 | ПСК-2 |
| | Итого | 8 | |
| Итого за семестр | | 8 | |
| Итого | | 12 | |

## 8. Практические занятия (семинары)

Не предусмотрено РУП

Согласована на портале № 21191

## 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 |
|---|---|---|---|---|
| 8 семестр | | | | |
| 1 Криптографические протоколы: общие понятия. | Подготовка к практическим занятиям, семинарам | 5 | ПСК-2 | Опрос на занятиях, Отчет по лабораторной работе, Собеседование |
| | Проработка лекционного материала | 2 | | |
| | Оформление отчетов по лабораторным работам | 3 | | |
| | Итого | 10 | | |
| 2 Протоколы распределения ключей. | Подготовка к практическим занятиям, семинарам | 4 | ПСК-2 | Конспект самоподготовки, Отчет по лабораторной работе, Собеседование, Тест |
| | Проработка лекционного материала | 2 | | |
| | Оформление отчетов по лабораторным работам | 3 | | |
| | Итого | 9 | | |
| 3 Инфраструктура открытого ключа. | Подготовка к практическим занятиям, семинарам | 4 | ПСК-2 | Опрос на занятиях, Отчет по лабораторной работе, Собеседование |
| | Проработка лекционного материала | 2 | | |
| | Оформление отчетов по лабораторным работам | 5 | | |
| | Итого | 11 | | |
| Итого за семестр | | 30 | | |
| 9 семестр | | | | |
| 4 Протоколы идентификации и аутентификации. | Выполнение контрольных работ | 19 | ПСК-2 | Контрольная работа, Собеседование |
| | Проработка лекционного материала | 1 | | |
| | Итого | 20 | | |
| 5 Безопасный канал обмена сообщениями. | Подготовка к практическим занятиям, семинарам | 18 | ПСК-2 | Контрольная работа, Отчет по практическому занятию |
| | Проработка лекционного | 1 | | |

Согласована на портале № 21191

| | | | | |
|---|---|---|---|---|
| | материала | | | |
| | Итого | 19 | | |
| 6 Практические аспекты реализации средств криптографической защиты информации. | Подготовка к практическим занятиям, семинарам | 17 | ПСК-2 | Отчет по практическому занятию |
| | Итого | 17 | | |
| Итого за семестр | | 56 | | |
| | Подготовка и сдача зачета | 4 | | Зачет |
| Итого | | 90 | | |

### 9.1. Темы контрольных работ

1. Контрольная по теме "протоколы идентификации и аутентификации"

### 9.2. Вопросы для подготовки к практическим занятиям, семинарам

1. Практика по теме "криптографические средства защиты иноформации"
2. Практика по теме "безопасность канала обмена сообщениями"

## 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. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 143[1] с. : ил. - Загл. обл. : Криптография в упражнениях и задачах. - Загл. на корешке : Криптография в упражнениях и задачах. - Библиогр.: с. 139. - ISBN 5-85438-009-9 : 52.25 р. (наличие в библиотеке ТУСУР - 50 экз.)
2. Криптография : учебник для вузов: пер. с англ. / Н. Смарт ; пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М. : Техносфера, 2005. - 525[3] с. : ил. - (Мир программирования ; VIII-05). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1 : 402.00 р. (наличие в библиотеке ТУСУР - 11 экз.)

### 12.2. Дополнительная литература

1. Основы криптографии : учебное пособие для вузов / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 479, [1] с. : ил. - Библиогр.: с. 469-475. - ISBN 5-85438-137-0 (наличие в библиотеке ТУСУР - 30 экз.)

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf
2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.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:**

Согласована на портале № 21191

– 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. Google — поисковая система интернета, принадлежащая корпорации Google Inc.
2. Яндекс — поисковая система интернета, принадлежащий российской корпорации «Яндекс».

## 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 лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

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

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

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

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 7 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

Согласована на портале № 21191

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 средств | Формы контроля и оценки 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;

Согласована на портале № 21191

– 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 № 21191

**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

# Прикладная криптография

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**

Учебный план набора 2013 года

Разработчики:
- Программист каф. КИБЭВС И. Ю. Поляков
- Доцент каф. КИБЭВС . . Конев

Зачет: 9 семестр

Томск 2017

Согласована на портале № 21191

## 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 |
|---|---|---|
| ПСК-2 | способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа | Должен знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.;<br>Должен уметь эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.;<br>Должен владеть навыками использования типовых криптографических алгоритмов.; |

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 ПСК-2

ПСК-2: способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа.

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

Согласована на портале № 21191

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа. | ставить и решать прикладные задачи. | способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа. |
| Виды занятий | • Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Контрольная работа;<br>• Конспект самоподготовки;<br>• Собеседование;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Тест;<br>• Отчет по практическому занятию;<br>• Зачет; | • Контрольная работа;<br>• Конспект самоподготовки;<br>• Собеседование;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Тест;<br>• Отчет по практическому занятию;<br>• Зачет; | • Отчет по лабораторной работе;<br>• Отчет по практическому занятию;<br>• Зачет; |

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 в полном объеме условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа . ; | • В полном объеме умеет ставить и решать прикладные задачи. ; | • В полном объеме владеет способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа. ; |
| Хорошо (базовый | • Знает на продвину- | • На продвинутом | • На продвинутом |

Согласована на портале № 21191

| | | | |
|---|---|---|---|
| уровень) | том уровне условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа . ; | уровне умеет ставить и решать прикладные задачи. ; | уровне владеет способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа. ; |
| Удовлетворительно (пороговый уровень) | • Знает на базовом уровне условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа . ; | • На базовом уровне умеет ставить и решать прикладные задачи. ; | • На базовом уровне владеет способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа. ; |

## 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

– Дать содержательное объяснения таких услуг безопасности как конфиденциальность, целостность, подлинность, неотрекаемость и доступность.

– Перечислить известные механизмы обеспечения безопасности. Объяснить взаимосвязь услуг безопасности, механизмов и алгоритмов.

– Объяснить, что такое совершенная секретность, привести пример совершенного шифра. Объяснить смысл теоремы Шеннона.

– Сжато, но осмысленно, пояснить те аспекты алгебры и теории чисел, которые используются в современной криптографии. Мультипликативная группа конечного поля, по модулю составного числа. Теоремы Эйлера и Ферма. Эллиптические кривые. Группа точек эллиптической кривой.

– Режимы шифрования. Перечислить и объяснить различия.

– Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа.

– Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

– Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Пречислить и объяснить назначение составляющих компонент.

– Хэш-функции. Какие типы существуют, в чем их различие. Объяснить свойства. Перечислить области применения. Атаки на хэш-функции. Что такое парадокс «дней рождения»?

– Базовые принципы построения криптографичсеских пролтоколов.

– Анонимность и неотслеживаемость. Проблема «ужинающих криптогра-фов». «Слепая»

Согласована на портале № 21191

подпись Чаума. Объяснить принцип построения протоко-ла для анонимных чеков на основе «слепой» подписи.

– Принципы квантовой криптографии. Объяснить квантовый протокол рас-пределения ключей.

### 3.2 Тестовые задания

–

– Дать содержательное объяснения таких услуг безопасности как конфиденциальность, целостность, подлинность, неотрекаемость и доступность.

–

– Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Перечислить и объяснить назначение составляющих компонент.

– Хэш-функции. Какие типы существуют, в чем их различие. Объяснить свойства. Перечислить области применения. Атаки на хэш-функции. Что такое парадокс «дней рождения»?

– Базовые принципы построения криптографических протоколов.

### 3.3 Зачёт

– Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.

– Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

– Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.

– Построение безопасного коммуникационного канала на основе криптографических алгоритмов.

– Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.

### 3.4 Вопросы на собеседование

–

– Дать содержательное объяснения таких услуг безопасности как конфиденциальность, целостность, подлинность, неотрекаемость и доступность.

–

–

– Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Перечислить и объяснить назначение составляющих компонент.

– Хэш-функции. Какие типы существуют, в чем их различие. Объяснить свойства. Перечислить области применения. Атаки на хэш-функции. Что такое парадокс «дней рождения»?

– Базовые принципы построения криптографических протоколов.

### 3.5 Темы опросов на занятиях

– Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.

### 3.6 Темы контрольных работ

– Контрольная по теме "протоколы идентификации и аутентификации"

### 3.7 Вопросы для подготовки к практическим занятиям, семинарам

– Практика по теме "криптографические средства защиты иноформации"

– Практика по теме "безопасность канала обмена сообщениями"

### 3.8 Темы лабораторных работ

– Установка и настройка Active Directory Certificate Services

– Кросс-сертификация

Согласована на портале № 21191

– Использование клиентов электронной почты
– Шифрованная файловая система Windows
– Шифрование диска BitLocker
– Генератор ключей для криптосистемы RSA
– Реализовать программу-шифровщик

## 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. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 143[1] с. : ил. - Загл. обл. : Криптография в упражнениях и задачах. - Загл. на корешке : Криптография в упражнениях и задачах. - Библиогр.: с. 139. - ISBN 5-85438-009-9 : 52.25 р. (наличие в библиотеке ТУСУР - 50 экз.)
2. Криптография : учебник для вузов: пер. с англ. / Н. Смарт ; пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М. : Техносфера, 2005. - 525[3] с. : ил. - (Мир программирования ; VIII-05). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1 : 402.00 р. (наличие в библиотеке ТУСУР - 11 экз.)

### 4.2. Дополнительная литература

1. Основы криптографии : учебное пособие для вузов / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 479, [1] с. : ил. - Библиогр.: с. 469-475. - ISBN 5-85438-137-0 (наличие в библиотеке ТУСУР - 30 экз.)

### 4.3. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf
2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf

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

1. Google — поисковая система интернета, принадлежащая корпорации Google Inc.
2. Яндекс — поисковая система интернета, принадлежащий российской корпорации «Яндекс».

Согласована на портале № 21191