**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

# Основы криптографии

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 № 21758

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «25» 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 №_____.

Разработчик:

доцент каф. БИС _____ О. О. Евсютин

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:

доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 21758

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «Основы криптографии» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

### 1.2. Задачи дисциплины

- дать представление о криптографических методах защиты информации;
- изучить современные стандарты симметричного шифрования;
- изучить криптографические функции хеширования;
- изучить основные криптографические алгоритмы с открытым ключом;
- дать общее представление об инфраструктуре открытых ключей.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Основы криптографии» (Б1.В.ДВ.5.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Математика, Организационное и правовое обеспечение информационной безопасности, 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** навыками использования типовых криптографических алгоритмов.
- **владеть** криптографическими методами и средствами защиты информации.

## 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 | 24 | 8 | 16 |
| Проработка лекционного материала | 14 | 6 | 8 |
| Самостоятельное изучение тем (вопросов) теоретической части курса | 40 | 16 | 24 |
| Выполнение контрольных работ | 8 | | 8 |

Согласована на портале № 21758

| | | | |
|---|---|---|---|
| Всего (без экзамена) | 104 | 36 | 68 |
| Подготовка и сдача зачета | 4 | | 4 |
| Общая трудоемкость ч | 108 | 36 | 72 |
| 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 Основные цели и задачи криптографии | 1 | 0 | 2 | 3 | ПСК-2 |
| 2 Симметричное шифрование | 1 | 4 | 28 | 33 | ПСК-2 |
| Итого за семестр | 2 | 4 | 30 | 36 | |
| 9 семестр | | | | | |
| 3 Хеширование | 1 | 0 | 10 | 11 | ПСК-2 |
| 4 Криптография с открытым ключом | 1 | 0 | 14 | 15 | ПСК-2 |
| 5 Электронная подпись | 2 | 8 | 32 | 42 | 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 Основные цели и задачи криптографии | Основная криптографическая терминология. Основные криптографические методы защиты информации: шифрование, хеширование, электронная подпись | 1 | ПСК-2 |
| | Итого | 1 | |
| 2 Симметричное шифрование | ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. AES. | 1 | ПСК-2 |

Согласована на портале № 21758

| | | | |
|---|---|---|---|
| | Итого | 1 | |
| Итого за семестр | | 2 | |
| 9 семестр | | | |
| 3 Хеширование | Криптографические хеш-функции. ГОСТ Р 34.11-2012. | 1 | ПСК-2 |
| | Итого | 1 | |
| 4 Криптография с открытым ключом | Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. | 1 | ПСК-2 |
| | Итого | 1 | |
| 5 Электронная подпись | Электронная подпись. ГОСТ Р 34.10-2012. Инфраструктура открытого ключа. | 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 |
| Предшествующие дисциплины | | | | | |
| 1 Математика | | + | + | + | + |
| 2 Организационное и правовое обеспечение информационной безопасности | + | | | | |
| 3 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 | |

Согласована на портале № 21758

| | | | | |
|---|---|---|---|---|
| ПСК-2 | + | + | + | Контрольная работа, Защита отчета, Проверка контрольных работ, Отчет по лабораторной работе, Зачет |

## 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 лабораторные занятия | Интерактивные лекции | Всего |
|---|---|---|---|
| 8 семестр | | | |
| IT-методы | 2 | | 2 |
| Итого за семестр: | 2 | 0 | 2 |
| 9 семестр | | | |
| IT-методы | 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 | | | |
| 2 Симметричное шифрование | Шифрованная файловая система Windows | 2 | ПСК-2 |
| | Средство криптографической защиты информации Secret Disk | 2 | |
| | Итого | 4 | |
| Итого за семестр | | 4 | |
| 9 семестр | | | |
| 5 Электронная подпись | Работа с криптопровайдерами | 8 | ПСК-2 |
| | Итого | 8 | |
| Итого за семестр | | 8 | |
| Итого | | 12 | |

## 8. Практические занятия (семинары)

Не предусмотрено РУП

## 9. Самостоятельная работа

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

Согласована на портале № 21758

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 8 семестр | | | | |
| 1 Основные цели и задачи криптографии | Проработка лекционного материала | 2 | ПСК-2 | Зачет, Контрольная работа, Проверка контрольных работ |
| | Итого | 2 | | |
| 2 Симметричное шифрование | Самостоятельное изучение тем (вопросов) теоретической части курса | 16 | ПСК-2 | Зачет, Защита отчета, Контрольная работа, Отчет по лабораторной работе, Проверка контрольных работ |
| | Проработка лекционного материала | 4 | | |
| | Оформление отчетов по лабораторным работам | 8 | | |
| | Итого | 28 | | |
| Итого за семестр | | 30 | | |
| 9 семестр | | | | |
| 3 Хеширование | Самостоятельное изучение тем (вопросов) теоретической части курса | 8 | ПСК-2 | Зачет, Контрольная работа, Проверка контрольных работ |
| | Проработка лекционного материала | 2 | | |
| | Итого | 10 | | |
| 4 Криптография с открытым ключом | Выполнение контрольных работ | 4 | ПСК-2 | Зачет, Контрольная работа, Проверка контрольных работ |
| | Самостоятельное изучение тем (вопросов) теоретической части курса | 8 | | |
| | Проработка лекционного материала | 2 | | |
| | Итого | 14 | | |
| 5 Электронная подпись | Выполнение контрольных работ | 4 | ПСК-2 | Зачет, Защита отчета, Контрольная работа, Отчет по лабораторной работе, Проверка контрольных работ |
| | Самостоятельное изучение тем (вопросов) теоретической части курса | 8 | | |
| | Проработка лекционного материала | 4 | | |
| | Оформление отчетов по лабораторным работам | 16 | | |
| | Итого | 32 | | |
| Итого за семестр | | 56 | | |

Согласована на портале № 21758

| | | | | |
|---|---|---|---|---|
| | Подготовка и сдача зачета | 4 | | Зачет |
| Итого | | 90 | | |

### 9.1. Темы контрольных работ

1. Схемы электронной подписи
2. Криптосистемы с открытым ключом

## 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. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — 2-е изд. — М.: Горячая линия – Телеком, 2013. — 232 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63244/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63244/

### 12.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с. (наличие в библиотеке ТУСУР - 28 экз.)

2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с. (наличие в библиотеке ТУСУР - 51 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]. - 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]. - 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:**

- 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. 1. Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).
2. 2. Интегрированная среда разработки программного обеспечения Microsoft Visual Studio 2012.

Согласована на портале № 21758

## 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 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. Вершинина, 47, 1 этаж, ауд. 126. 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 № 21758

| | 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 № 21758

**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

# Основы криптографии

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

Разработчик:
- доцент каф. БИС О. О. Евсютин

Зачет: 9 семестр

Томск 2017

Согласована на портале № 21758

## 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 навыками использования типовых криптографических алгоритмов.;<br>Должен владеть криптографическими методами и средствами защиты информации.; |

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.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|

Согласована на портале № 21758

| | | | |
|---|---|---|---|
| Содержание этапов | основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях. | навыками использования типовых криптографических алгоритмов. | криптографическими методами и средствами защиты информации. |
| Виды занятий | • Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа;<br>• Интерактивные лекции; | • Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа;<br>• Интерактивные лекции; | • Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Контрольная работа;<br>• Отчет по лабораторной работе;<br>• Зачет; | • Контрольная работа;<br>• Отчет по лабораторной работе;<br>• Зачет; | • Отчет по лабораторной работе;<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 основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.; | • Умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.; | • Владеет основными криптографическими методами и средствами защиты информации.; |
| Хорошо (базовый уровень) | • Знает некоторые криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.; | • Умеет использовать криптографические методы и средства защиты информации в автоматизированных системах.; | • Владеет некоторыми криптографическими методами и средствами защиты информации.; |
| Удовлетворительно (пороговый уровень) | • Имеет представление о криптографических методах, алгоритмах, протоколах, используемых для обеспечения безопасности в компьютерных сетях.; | • Имеет представлением об использовании криптографических методов и средств защиты информации в автоматизированных системах.; | • Имеет представление о криптографических методах и средствах защиты информации.; |

## 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 Зачёт

– 1. Цели и задачи криптографии. Основные понятия.

Согласована на портале № 21758

– 2. Простейшие шифры: простой замены, перестановочный, аффинный.
– 3. ГОСТ Р 34.12–2015.
– 4. AES.
– 5. Режимы работы симметричных блочных шифров.
– 6. Криптография с открытым ключом.
– 7. Криптосистема RSA.
– 8. Криптосистема Эль-Гамаля.
– 9. Криптосистема Рабина.
– 10. Протокол Диффи-Хеллмана.
– 11. Понятие хеш-функции. Свойства криптографических хеш-функций.
– 12. ГОСТ Р 34.11-2012.
– 13. Код аутентичности сообщений.
– 14. Электронная подпись.
– 15. ГОСТ Р 34.10-2012.
– 16. Инфраструктура открытого ключа.

### 3.2 Темы контрольных работ

– Схемы электронной подписи
– Криптосистемы с открытым ключом

### 3.3 Темы контрольных работ

– Схемы электронной подписи
– Криптосистемы с открытым ключом

### 3.4 Темы лабораторных работ

– Шифрованная файловая система Windows
– Средство криптографической защиты информации Secret Disk
– Работа с криптопровайдерами

## 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. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — 2-е изд. — М.: Горячая линия – Телеком, 2013. — 232 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63244/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63244/

### 4.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с. (наличие в библиотеке ТУСУР - 28 экз.)

2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с. (наличие в библиотеке ТУСУР - 51 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]. - 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]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf

Согласована на портале № 21758

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

1. 1. Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).
2. 2. Интегрированная среда разработки программного обеспечения Microsoft Visual Studio 2012.

Согласована на портале № 21758