

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

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

**История криптографии**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **10.03.01 Информационная безопасность**

Направленность (профиль): **Организация и технология защиты информации**

Форма обучения: **очная**

Факультет: **РТФ, Радиотехнический факультет**

Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**

Курс: **1**

Семестр: **1**

Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	1 семестр	Всего	Единицы
1	Лекции	16	16	часов
2	Лабораторные работы	24	24	часов
3	Всего аудиторных занятий	40	40	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	32	32	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Зачет: 1 семестр

Томск 2017

## ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры « \_\_\_ » \_\_\_\_\_ 20\_\_ года, протокол № \_\_\_\_\_.

Разработчик:

доцент каф. БИС

\_\_\_\_\_ О. О. Евсютин

Заведующий обеспечивающей каф.  
РЗИ

\_\_\_\_\_ А. В. Фатеев

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

Декан РТФ

\_\_\_\_\_ К. Ю. Попова

Заведующий выпускающей каф.  
РЗИ

\_\_\_\_\_ А. В. Фатеев

Эксперт:

доцент каф. РЗИ

\_\_\_\_\_ А. П. Кшнянкин

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «История криптографии» является формирование у студентов общих представлений о развитии криптографических методов защиты информации и роли криптографии в сфере информационной безопасности.

### 1.2. Задачи дисциплины

- дать общее представление о криптографических методах защиты информации;
- изучить исторические шифры;
- сформировать представление о методах криптоанализа исторических шифров.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «История криптографии» (Б1.В.ДВ.2.2) относится к блоку 1 (вариативная часть).

Последующими дисциплинами являются: Защита и обработка конфиденциальных документов, Защита информационных процессов в компьютерных системах, Криптографические методы защиты информации.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

В результате изучения дисциплины студент должен:

- **знать** виды и основные примеры исторических шифров; методы криптоанализа исторических шифров.
- **уметь** взламывать простейшие шифры.
- **владеть** методами криптоанализа исторических шифров.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		1 семестр
Аудиторные занятия (всего)	40	40
Лекции	16	16
Лабораторные работы	24	24
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	32	32
Оформление отчетов по лабораторным работам	24	24
Проработка лекционного материала	8	8
Всего (без экзамена)	72	72
Общая трудоемкость ч	72	72
Зачетные Единицы	2.0	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
1 семестр					
1 Основные цели и задачи криптографии	2	0	2	4	ОК-5
2 Шифры разных эпох	8	12	14	34	ОК-5
3 Криптоанализ исторических шифров	2	12	14	28	ОК-5
4 Современная криптография	4	0	2	6	ОК-5
Итого за семестр	16	24	32	72	
Итого	16	24	32	72	

### 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
1 семестр			
1 Основные цели и задачи криптографии	Место криптографии в сфере защиты информации. Основные термины и определения.	2	ОК-5
	Итого	2	
2 Шифры разных эпох	Античные шифры. Средневековые шифры. Шифры XIX - начала XX вв. Шифры времен Второй мировой войны.	8	ОК-5
	Итого	8	
3 Криптоанализ исторических шифров	Понятие криптографической стойкости. Криптоанализ подстановочного шифра, перестановочного шифра, шифра гаммирования.	2	ОК-5
	Итого	2	
4 Современная криптография	Симметричное и асимметричное шифрование. Хеширование. Электронная подпись.	4	ОК-5
	Итого	4	
Итого за семестр		16	

### 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
Последующие дисциплины				
1 Защита и обработка конфиденциальных документов	+			+
2 Защита информационных процессов в компьютерных системах	+			+
3 Криптографические методы защиты информации	+	+	+	+

### 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	
ОК-5	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, 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
1 семестр			
IT-методы	12	8	20
Итого за семестр:	12	8	20
Итого	12	8	20

### 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
1 семестр			
2 Шифры разных эпох	Реализация шифра простой замены.	4	ОК-5
	Реализация перестановочного шифра.	4	
	Реализация шифра гаммирования.	4	
	Итого	12	
3 Криптоанализ исторических шифров	Криптоанализ шифра простой замены.	4	ОК-5
	Криптоанализ перестановочного шифра.	4	
	Криптоанализ шифра гаммирования.	4	
	Итого	12	
Итого за семестр		24	

### 8. Практические занятия (семинары)

Не предусмотрено РУП

### 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
1 семестр				
1 Основные цели и задачи криптографии	Проработка лекционного материала	2	ОК-5	Зачет, Опрос на занятиях
	Итого	2		
2 Шифры разных эпох	Проработка лекционного материала	2	ОК-5	Зачет, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	12		
	Итого	14		
3 Криптоанализ исторических шифров	Проработка лекционного материала	2	ОК-5	Зачет, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	12		
	Итого	14		
4 Современная криптография	Проработка лекционного материала	2	ОК-5	Зачет, Опрос на занятиях

	Итого	2		
Итого за семестр		32		
Итого		32		

### 10. Курсовая работа (проект)

Не предусмотрено РУП

### 11. Рейтинговая система для оценки успеваемости студентов

#### 11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
1 семестр				
Защита отчета	15	15	15	45
Опрос на занятиях	5	5		10
Отчет по лабораторной работе	15	15	15	45
Итого максимум за период	35	35	30	100
Нарастающим итогом	35	70	100	100

#### 11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

#### 11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

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

## 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. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_pk.pdf](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.

## 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 версий 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 видеовеличителей 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 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;
- 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.

**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**

**История криптографии**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **10.03.01 Информационная безопасность**

Направленность (профиль): **Организация и технология защиты информации**

Форма обучения: **очная**

Факультет: **РТФ, Радиотехнический факультет**

Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**

Курс: **1**

Семестр: **1**

Учебный план набора 2013 года

Разработчик:

– доцент каф. БИС О. О. Евсютин

Зачет: 1 семестр

Томск 2017

## 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
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Должен знать виды и основные примеры исторических шифров; методы криптоанализа исторических шифров.; Должен уметь взламывать простейшие шифры.; Должен владеть методами криптоанализа исторических шифров.;

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 ОК-5

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

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 эта-	виды и основные приме-	взламывать простейшие	методами криптоанализа

пов	ры исторических шифров; методы криптоанализа исторических шифров.	шифры.	исторических шифров.
Виды занятий	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Интерактивные лекции;</li> <li>• Лабораторные работы;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Интерактивные лекции;</li> <li>• Лабораторные работы;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Лабораторные работы;</li> <li>• Самостоятельная работа;</li> </ul>
Используемые средства оценивания	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Зачет;</li> </ul>

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)	<ul style="list-style-type: none"> <li>• Знает виды и основные примеры исторических шифров; методы криптоанализа исторических шифров.;</li> </ul>	<ul style="list-style-type: none"> <li>• Умеет взламывать простейшие шифры.;</li> <li>• Умеет анализировать выбирать методы взлома неизвестных шифров.;</li> </ul>	<ul style="list-style-type: none"> <li>• Владеет основными методами криптоанализа исторических шифров.;</li> </ul>
Хорошо (базовый уровень)	<ul style="list-style-type: none"> <li>• Знает основные примеры исторических шифров; некоторые методы криптоанализа исторических шифров.;</li> </ul>	<ul style="list-style-type: none"> <li>• Умеет взламывать простейшие шифры;</li> </ul>	<ul style="list-style-type: none"> <li>• Владеет некоторыми методами криптоанализа исторических шифров.;</li> </ul>
Удовлетворительно (пороговый уровень)	<ul style="list-style-type: none"> <li>• Знает некоторые примеры исторических шифров.;</li> </ul>	<ul style="list-style-type: none"> <li>• Умеет взламывать некоторые простейшие шифры;</li> </ul>	<ul style="list-style-type: none"> <li>• Имеет представление о криптоанализе исторических шифров.;</li> </ul>

### 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. Перечислите и кратко охарактеризуйте основные задачи обеспечения информационной безопасности, решаемые с помощью криптографических методов.
- 2. Раскройте определения: шифрование, зашифрование, расшифрование, дешифрование.
- 3. Чем шифрование отличается от кодирования?
- 4. Приведите известные вам классификации криптосистем.
- 5. Укажите основные отличия между современной и классической криптографией.
- 6. Сравните аффинный шифр и шифр Хилла с точки зрения криптостойкости.
- 7. Опишите способы криптоанализа:

- а) аффинного шифра;
- б) шифра Хилла;
- в) шифра гаммирования.
- 8. Укажите основные отличия между современными и классическими блочными шифрами.
- 9. Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
- 10. Сравните DES и ГОСТ 28147-89.
- 11. Сравните AES и ГОСТ 28147-89.
- 12. Перечислите основные свойства хеш-функций.
- 13. Чем хеширование отличается от выработки контрольных сумм?
- 14. Чем хеширование отличается от выработки имитовставки?
- 15. Укажите два основных подхода к построению функций хеширования.
- 16. Укажите основной недостаток кодов аутентичности сообщений.
- 17. В чем заключается проблема управления симметричными ключами?
- 18. Сравните криптосистему RSA и криптосистему Рабина.
- 19. Сравните криптосистему RSA и криптосистему Эль-Гамала.
- 20. Решение каких задач обеспечивает электронная подпись?
- 21. Как построить схему выработки и проверки электронной подписи на основе криптосистемы RSA?
- 22. Что такое эллиптическая криптография?
- 23. Дайте понятие криптографического протокола.

### **3.2 Темы опросов на занятиях**

- Место криптографии в сфере защиты информации. Основные термины и определения.
- Античные шифры. Средневековые шифры. Шифры XIX - начала XX вв. Шифры времен Второй мировой войны.
- Понятие криптографической стойкости. Криптоанализ подстановочного шифра, перестановочного шифра, шифра гаммирования.
- Симметричное и асимметричное шифрование. Хеширование. Электронная подпись.

### **3.3 Темы лабораторных работ**

- Реализация шифра простой замены.
- Реализация перестановочного шифра.
- Реализация шифра гаммирования.
- Криптоанализ шифра простой замены.
- Криптоанализ перестановочного шифра.
- Криптоанализ шифра гаммирования.

## **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 формирования 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. (на-

личие 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. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_pk.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf)

#### **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.