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

Криптографические протоколы и стандарты

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: **2**
Семестр: **3, 4**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	3 семестр	4 семестр	Всего	Единицы
1	Лекции	2	2	4	часов
2	Практические занятия	2	4	6	часов
3	Всего аудиторных занятий	4	6	10	часов
4	Из них в интерактивной форме		4	4	часов
5	Самостоятельная работа	68	26	94	часов
6	Всего (без экзамена)	72	32	104	часов
7	Подготовка и сдача зачета		4	4	часов
8	Общая трудоемкость	72	36	108	часов
		3.0		3.0	З.Е

Контрольные работы: 4 семестр - 1
Зачет: 4 семестр

Томск 2017

Согласована на портале № 21761

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 № 21761

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Цель дисциплины «Криптографические протоколы и стандарты» — ознакомление с существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

1.2. Задачи дисциплины

– Задача дисциплины «Криптографические протоколы и стандарты» — формирование основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

2. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические протоколы и стандарты» (Б1.В.ДВ.2.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Математика.

Последующими дисциплинами являются: Безопасность систем баз данных, Основы информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-7 способностью к логическому мышлению, аргументированно и ясно строить устную и письменную речь, вести полемику и дискуссии;

В результате изучения дисциплины студент должен:

– **знать** нормативные правовые акты в области защиты информации; основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.

– **уметь** использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.

– **владеть** навыками обеспечения защиты информации, составляющей государственную тайну, и иной служебной 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	
		3 семестр	4 семестр
Аудиторные занятия (всего)	10	4	6
Лекции	4	2	2
Практические занятия	6	2	4
Из них в интерактивной форме	4		4
Самостоятельная работа (всего)	94	68	26
Проработка лекционного материала	8	6	2
Самостоятельное изучение тем (вопросов) теоретической части курса	62	54	8

Согласована на портале № 21761

Подготовка к практическим занятиям, семинарам	16	8	8
Выполнение контрольных работ	8		8
Всего (без экзамена)	104	72	32
Подготовка и сдача зачета	4		4
Общая трудоемкость ч	108	72	36
Зачетные Единицы	3.0	3.0	

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
3 семестр					
1 Основные понятия	1	0	10	11	ОК-7
2 Электронная подпись и инфраструктура открытых ключей	1	2	58	61	ОК-7
Итого за семестр	2	2	68	72	
4 семестр					
3 Стандарты в области криптографических протоколов	2	4	26	32	ОК-7
Итого за семестр	2	4	26	32	
Итого	4	6	94	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
3 семестр			
1 Основные понятия	Предназначение криптографических методов защиты информации. Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоко-	1	ОК-7

Согласована на портале № 21761

	лы.		
	Итого	1	
2 Электронная подпись и инфраструктура открытых ключей	Понятие электронной подписи. Схемы электронной подписи на основе симметричных и асимметричных криптосистем. Стандарты США и России электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытых ключей.	1	ОК-7
	Итого	1	
Итого за семестр		2	
4 семестр			
3 Стандарты в области криптографических протоколов	Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Проблемы автоматизации анализа криптографических протоколов.	2	ОК-7
	Итого	2	
Итого за семестр		2	
Итого		4	

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
Предшествующие дисциплины			
1 Математика	+	+	+
Последующие дисциплины			
1 Безопасность систем баз данных	+	+	+
2 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

	Виды занятий	Формы контроля

Согласована на портале № 21761

Компетенции	Лекции	Практические занятия	Самостоятельная работа	
ОК-7	+	+	+	Контрольная работа, Проверка контрольных работ, 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 практические занятия	Интерактивные лекции	Всего
3 семестр			
Итого за семестр:	0	0	0
4 семестр			
IT-методы	2	2	4
Итого за семестр:	2	2	4
Итого	2	2	4

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
3 семестр			
2 Электронная подпись и инфраструктура открытых ключей	Схемы электронной подписи RSA, ECDSA и ГОСТ. Сертификаты инфраструктуры открытых ключей и их структура. Функции удостоверяющего центра. Порядок отзыва сертификатов.	2	ОК-7
	Итого	2	
Итого за семестр		2	
4 семестр			
3 Стандарты в области криптографических протоколов	Примеры прикладных протоколов.	4	ОК-7
	Итого	4	

Согласована на портале № 21761

Итого за семестр		4	
Итого		6	

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
3 семестр				
1 Основные понятия	Самостоятельное изучение тем (вопросов) теоретической части курса	8	ОК-7	Зачет, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	10		
2 Электронная подпись и инфраструктура открытых ключей	Подготовка к практическим занятиям, семинарам	8	ОК-7	Зачет, Опрос на занятиях
	Самостоятельное изучение тем (вопросов) теоретической части курса	46		
	Проработка лекционного материала	4		
	Итого	58		
Итого за семестр		68		
4 семестр				
3 Стандарты в области криптографических протоколов	Выполнение контрольных работ	8	ОК-7	Зачет, Контрольная работа, Опрос на занятиях, Проверка контрольных работ
	Подготовка к практическим занятиям, семинарам	8		
	Самостоятельное изучение тем (вопросов) теоретической части курса	8		
	Проработка лекционного материала	2		
	Итого	26		
Итого за семестр		26		
	Подготовка и сдача зачета	4		Зачет
Итого		98		

9.1. Темы контрольных работ

1. Исследование уязвимостей криптографических протоколов.

Согласована на портале № 21761

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]. - 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 протоколы и стандарты. Методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kpis.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. Не предусмотрено.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

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

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения 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/

Согласована на портале № 21761

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 Ce1егоп 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 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	Тесты, письменные самостоятельные работы, вопросы к зачету,	Преимущественно проверка методами, исходя из состояния

Согласована на портале № 21761

показаниям	контрольные работы, устные ответы	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 № 21761

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

Криптографические протоколы и стандарты

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: **2**
Семестр: **3, 4**

Учебный план набора 2013 года

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

Зачет: 4 семестр

Томск 2017

Согласована на портале № 21761

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-7	способностью к логическому мышлению, аргументированно и ясно строить устную и письменную речь, вести полемику и дискуссии	Должен знать нормативные правовые акты в области защиты информации; основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.; Должен уметь использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.; Должен владеть навыками обеспечения защиты информации, составляющей государственную тайну, и иной служебной 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 ОК-7

ОК-7: способностью к логическому мышлению, аргументированно и ясно строить устную и

Согласована на портале № 21761

письменную речь, вести полемику и дискуссии.

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

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	нормативные правовые акты в области защиты информации; основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.	использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.	навыками обеспечения защиты информации, составляющей государственную тайну, и иной служебной информации.
Виды занятий	• Практические занятия; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Интерактивные лекции;	• Практические занятия; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Интерактивные лекции;	• Самостоятельная работа; • Интерактивные практические занятия;
Используемые средства оценивания	• Контрольная работа; • Опрос на занятиях; • Зачет;	• Контрольная работа; • Опрос на занятиях; • Зачет;	• 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 нормативные правовые акты в области защиты информации.; • Знает основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.;	• Умеет использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.;	• Владеет навыками обеспечения защиты информации, составляющей государственную тайну, и иной служебной информации.;
Хорошо (базовый уровень)	• Знает основные нормативные правовые акты в области защиты информации.;	• Умеет использовать некоторые методы и средства обеспечения информационной без-	• Владеет некоторыми навыками обеспечения защиты информации, составляющей государ-

Согласована на портале № 21761

	• Знает некоторые методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.;	опасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.;	ственную тайну, и иной служебной информации.;
Удовлетворительно (пороговый уровень)	• Имеет представление о нормативных правовых актах в области защиты информации и методах, способах и мероприятиях по обеспечению информационной безопасности в профессиональной деятельности.;	• Имеет представление об использовании методов и средств обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации.;	• Имеет представление об обеспечении защиты информации, составляющей государственную тайну, и иной служебной 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. Понятие криптографического протокола. Виды криптографических протоколов.
- 2. Основные функции сервисы безопасности.
- 3. Основные атаки на криптографические протоколы.
- 4. Протоколы идентификации.
- 5. Слабая аутентификация.
- 6. Сильная аутентификация.
- 7. Протоколы, основанные на технике доказательства знания.
- 8. Протоколы с нулевым разглашением.
- 9. Протоколы предварительного распределения ключей.
- 10. Протоколы обмена ключами.
- 11. Протоколы открытого распределения ключей.
- 12. Основные прикладные протоколы.
- 13. Управление ключами.
- 14. Инфраструктура открытого ключа.

3.2 Темы контрольных работ

- Исследование уязвимостей криптографических протоколов.

3.3 Темы опросов на занятиях

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

Согласована на портале № 21761

– Понятие электронной подписи. Схемы электронной подписи на основе симметричных и асимметричных криптосистем. Стандарты США и России электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытых ключей.

– Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Проблемы автоматизации анализа криптографических протоколов.

3.4 Темы контрольных работ

– Исследование уязвимостей криптографических протоколов.

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]. - 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 протоколы и стандарты. Методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kpis.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрено.

Согласована на портале № 21761