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

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **09.03.02 Информационные системы и технологии**
Направленность (профиль): **Информационные системы и технологии**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **ЭМИС, Кафедра экономической математики, информатики и статистики**
Курс: **4**
Семестр: **7**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные занятия	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	126	126	часов
5	Всего (без экзамена)	180	180	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е

Экзамен: 7 семестр

Томск 2016

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «15» 10 2016 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии, утвержденного 2015-03-12 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. ЭМИС _____ Шельмина Е. А.

Заведующий обеспечивающей каф. ЭМИС _____ Боровской И. Г.

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

Декан ФВС _____ Козлова Л. А.

Заведующий выпускающей каф. ЭМИС _____ Боровской И. Г.

Эксперты:

профессор каф. ЭМИС _____ Колесникова С. И.

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Дать систематический обзор современных методов защиты информации и обеспечения компьютерной безопасности при реализации процессов ввода, вывода, передачи, обработки, накопления и хранения информации, изучить и освоить принципы их построения, рассмотреть перспективные направления развития существующих систем.

1.2. Задачи дисциплины

– дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности;

– сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.В.ОД.7) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Инструментальные средства информационных систем.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны;

– ОПК-5 способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению;

В результате изучения дисциплины студент должен:

– **знать** основные принципы информационной безопасности; современные компьютерные технологии поиска и анализа информации в области информационной безопасности;

– **уметь** применять методы оценки важности и необходимости защиты информации к разделам информационных технологий; осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации;

– **владеть** способами обеспечения информационной безопасности; передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности;

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Лабораторные занятия	36	36
Самостоятельная работа (всего)	126	126
Оформление отчетов по лабораторным работам	36	36
Проработка лекционного материала	90	90

Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
Общая трудоемкость час	216	216
Зачетные Единицы Трудоемкости	6.0	6.0

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	Введение.	1	0	10	11	ОПК-4
2	Проблемы и методы защиты информации.	5	0	18	23	ОПК-4, ОПК-5
3	Математические и методологические средства защиты информации.	6	16	42	64	ОПК-4, ОПК-5
4	Криптографические алгоритмы обеспечения информационной безопасности.	4	20	46	70	ОПК-4, ОПК-5
5	Компьютерные средства реализации защиты в информационных системах.	2	0	10	12	ОПК-4
	Итого	18	36	126	180	

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
7 семестр			
1 Введение.	Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности. Программа информационной безопасности России и пути ее реализации.	1	ОПК-4

	Итого	1	
2 Проблемы и методы защиты информации.	Информационная безопасность. Проблемы защиты информации в компьютерных системах. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации. Организационное обеспечение информационной безопасности.	5	ОПК-4, ОПК-5
	Итого	5	
3 Математические и методологические средства защиты информации.	Криптографическая терминология. Сведения из теории информации и теории чисел. Алгоритмы и ключи. Симметричные алгоритмы. Алгоритмы с открытым ключом. Подстановочные и перестановочные шифры. Одноразовые блокноты. Однонаправленные хэш-функции. Передача информации с использованием криптографии с открытым ключом. Основные протоколы передачи информации.	6	ОПК-4, ОПК-5
	Итого	6	
4 Криптографические алгоритмы обеспечения информационной безопасности.	Алгоритм симметричного шифрования данных DES. Алгоритм криптографического преобразования ГОСТ 28147-89. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP. Защита информации от несанкционированного доступа.	4	ОПК-4, ОПК-5
	Итого	4	
5 Компьютерные средства реализации защиты в информационных системах.	Физический, сетевой, транспортный и прикладной уровни защиты информации. Обзор стандартов в области защиты информации. Методы и средства защиты локальной рабочей станции. Защита в локальных сетях. Защита информации при межсетевом взаимодействии. Типы вирусов и средства антивирусной защиты. Обеспечение информационной безопасности в корпоративных сетях.	2	ОПК-4
	Итого	2	
Итого за семестр		18	

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 представ-лены 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	Инструментальные средства информационных систем	+	+		+	
Последующие дисциплины						
1	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		+	+		+

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 занятия	Самостоятельная работа	
ОПК-4	+	+	+	Коллоквиум, Отчет по лабораторной работе
ОПК-5	+	+	+	Коллоквиум, Отчет по лабораторной работе

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

7. Лабораторный практикум

Содержание лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Содержание лабораторных работ

Названия разделов	Содержание лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
3 Математические и методологические средства защиты информации.	Программная реализация шифра, основанного на методе Полибия. Программная реализация шифра простой замены. Программная реализация шифра, основанного на	16	ОПК-4, ОПК-5

	методе умножения матриц.		
	Итого	16	
4 Криптографические алгоритмы обеспечения информационной безопасности.	Алгоритм симметричного шифрования данных DES. Программная реализация асимметричного алгоритма шифрования RSA.	20	ОПК-4, ОПК-5
	Итого	20	
Итого за семестр		36	

8. Практические занятия

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
7 семестр				
1 Введение.	Проработка лекционного материала	10	ОПК-4	Коллоквиум
	Итого	10		
2 Проблемы и методы защиты информации.	Проработка лекционного материала	18	ОПК-4, ОПК-5	Коллоквиум
	Итого	18		
3 Математические и методологические средства защиты информации.	Проработка лекционного материала	26	ОПК-4, ОПК-5	Коллоквиум, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	16		
	Итого	42		
4 Криптографические алгоритмы обеспечения информационной безопасности.	Проработка лекционного материала	26	ОПК-4, ОПК-5	Коллоквиум, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	20		
	Итого	46		
5 Компьютерные средства реализации защиты в информационных системах.	Проработка лекционного материала	10	ОПК-4	Коллоквиум
	Итого	10		
Итого за семестр		126		
	Подготовка к экзамену	36		Экзамен
Итого		162		

10. Курсовая работа

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Бальные 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
7 семестр				
Коллоквиум	5	5	5	15
Отчет по лабораторной работе	15	25	15	55
Итого максимум за период	20	30	20	70
Экзамен				30
Нарастающим итогом	20	50	70	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)
3 (удовлетворительно) (зачтено)	65 - 69	
	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. Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. —

М. : Горячая линия-Телеком, 2012. — 616 с. [Электронный ресурс]. - http://e.lanbook.com/book/5154

12.2. Дополнительная литература

1. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. [Электронный ресурс]. - http://e.lanbook.com/book/5170

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 374 с. [Электронный ресурс]. - http://e.lanbook.com/book/11381

12.3. Учебно-методическое пособие и программное обеспечение

1. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/2261, свободный.

2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 17 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1822, свободный.

12.4. Базы данных, информационно справочные и поисковые системы

1. Поисковая система google.ru

13. Материально-техническое обеспечение дисциплины

При выполнения практических заданий по дисциплине используются персональные ЭВМ с процессорами Pentium 4 и выше, операционная система MS Windows XP/7.

14. Фонд оценочных средств

Фонд оценочных средств приведен в приложении 1.

15. Методические рекомендации по организации изучения дисциплины

Без рекомендаций.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **09.03.02 Информационные системы и технологии**
Направленность (профиль): **Информационные системы и технологии**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **ЭМИС, Кафедра экономической математики, информатики и статистики**
Курс: **4**
Семестр: **7**

Учебный план набора 2016 года

Разработчики:

- доцент каф. ЭМИС Шельмина Е. А.

Экзамен: 7 семестр

Томск 2016

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ОПК-4	пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны	Должен знать основные принципы информационной безопасности; современные компьютерные технологии поиска и анализа информации в области информационной безопасности;; Должен уметь применять методы оценки важности и необходимости защиты информации к разделам информационных технологий; осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации;; Должен владеть способами обеспечения информационной безопасности; передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности;;
ОПК-5	способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению	

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	Работает при прямом наблюдении

		задач	

2 Реализация компетенций

2.1 Компетенция ОПК-4

ОПК-4: пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны.

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	основные принципы информационной безопасности	применять методы оценки важности и необходимости защиты информации к разделам информационных технологий	способами обеспечения информационной безопасности
Виды занятий	• Лабораторные занятия; • Лекции; • Самостоятельная работа; • Подготовка к экзамену;	• Лабораторные занятия; • Лекции; • Самостоятельная работа; • Подготовка к экзамену;	• Лабораторные занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• основные принципы информационной безопасности; • проблемы защиты информации в компьютерных системах; • принципы организационного обеспечения информационной безопасности; • основные понятия криптографии; • симметричные алгоритмы; • алгоритмы с открытым ключом;	• применять методы защиты информации к разделам информационных технологий; • применять принципы организационного обеспечения информационной безопасности в профессиональной деятельности; • реализовывать алгоритмы криптографии: симметричные алгоритмы, алгоритмы с открытым ключом,	• способами обеспечения информационной безопасности; • навыками программной реализации алгоритмов криптографии: симметричные алгоритмы, алгоритмы с открытым ключом, подстановочные и перестановочные шифры, алгоритм симметричного шифрования данных DES, асимметричный алгоритм шифрования

	• подстановочные и перестановочные шифры; • алгоритм симметричного шифрования данных DES; • асимметричный алгоритм шифрования данных RSA; • комплекс криптографических алгоритмов PGP;	подстановочные и перестановочные шифры, алгоритм симметричного шифрования данных DES, асимметричный алгоритм шифрования данных RSA комплекс криптографических алгоритмов PGP;	данных RSA комплекс криптографических алгоритмов PGP;
Хорошо (базовый уровень)	• проблемы защиты информации в компьютерных системах; • принципы организационного обеспечения информационной безопасности; • основные понятия криптографии; • алгоритмы с открытым ключом; • основные принципы информационной безопасности; • комплекс криптографических алгоритмов PGP; • алгоритм симметричного шифрования данных DES; • асимметричный алгоритм шифрования данных RSA;	• применять методы защиты информации к разделам информационных технологий; • реализовывать алгоритмы криптографии: алгоритмы с открытым ключом, подстановочные и перестановочные шифры, алгоритм симметричного шифрования данных DES, асимметричный алгоритм шифрования данных RSA;	• способами обеспечения информационной безопасности; • навыками программной реализации алгоритмов криптографии:алгоритмы с открытым ключом, подстановочные и перестановочные шифры, алгоритм симметричного шифрования данных DES, асимметричный алгоритм шифрования данных RSA;
Удовлетворительно (пороговый уровень)	• основные принципы информационной безопасности; • основные принципы информационной безопасности; • основные понятия криптографии; • алгоритмы с открытым ключом; • алгоритм симметричного шифрования данных	• применять методы защиты информации к разделам информационных технологий; • реализовывать алгоритмы криптографии: алгоритмы с открытым ключом, алгоритм симметричного шифрования данных DES, асимметричный	• способами обеспечения информационной безопасности; • навыками программной реализации алгоритмов криптографии: алгоритмы с открытым ключом, алгоритм симметричного шифрования данных DES, асимметричный

	DES; • асимметричный алгоритм шифрования данных RSA;	алгоритм шифрования данных RSA;	алгоритм шифрования данных RSA;

2.2 Компетенция ОПК-5

ОПК-5: способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	современные компьютерные технологии поиска и анализа информации в области информационной безопасности	осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации	передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности
Виды занятий	• Лабораторные занятия; • Лекции; • Самостоятельная работа; • Подготовка к экзамену;	• Лабораторные занятия; • Лекции; • Самостоятельная работа; • Подготовка к экзамену;	• Лабораторные занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;	• Отчет по лабораторной работе; • Коллоквиум; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• современные компьютерные технологии поиска и анализа информации в области информационной безопасности; • физический, сетевой, транспортный и прикладной уровни защиты информации; • стандарты в области защиты информации;	• осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации; • реализовывать физический, сетевой, транспортный и прикладной уровни защиты информации; • применять стандарты	• передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности; • навыками самостоятельной реализации различных уровней защиты

	• методы и средства защиты локальной рабочей станции; • типы вирусов и средства антивирусной защиты; • обеспечение информационной безопасности в корпоративных сетях;	защиты информации в профессиональной деятельности; • применять средства антивирусной защиты; • обеспечивать информационную безопасность в корпоративных сетях;	информации, применения стандартов защиты информации и средств антивирусной защиты;
Хорошо (базовый уровень)	• современные компьютерные технологии поиска и анализа информации в области информационной безопасности; • физический, сетевой, транспортный и прикладной уровни защиты информации; • типы вирусов и средства антивирусной защиты; • обеспечение информационной безопасности в корпоративных сетях;	• применять средства антивирусной защиты; • осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации; • реализовывать физический, сетевой, транспортный и прикладной уровни защиты информации; • применять стандарты защиты информации в профессиональной деятельности;	• передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности; • навыками реализации различных уровней защиты информации, применения стандартов защиты информации и средств антивирусной защиты при работе в команде;
Удовлетворительно (пороговый уровень)	• современные компьютерные технологии поиска и анализа информации в области информационной безопасности; • физический, сетевой, транспортный и прикладной уровни защиты информации; • типы вирусов и средства антивирусной защиты;	• осуществлять оптимальный поиск необходимой информации для обоснования принятых идей в области защиты информации; • применять стандарты защиты информации в профессиональной деятельности; • применять средства антивирусной защиты;	• передовыми технологиями комплексного анализа поисковой информации при принятии аргументированных решений в области информационной безопасности; • навыками реализации различных уровней защиты информации, применения стандартов защиты информации и средств антивирусной защиты при работе под руководством;

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 Темы коллоквиумов

– Сформулируйте правило Керкхоффа относительно стойкости шифра.
– Опишите принцип реализации электронной цифровой подписи.
– Охарактеризуйте моноалфавитный, однозвучный, и полиграмный подстановочные шифры.
– Охарактеризуйте операцию XOR.
– Опишите столбцовый перестановочный шифр.
– Дайте определение криптографического протокола.
– Опишите схему вскрытия сообщения, зашифрованного моноалфавитным шифром замены.
– Каким образом можно определить понятие однонаправленной хэш-функции?
– Охарактеризуйте смешанные криптосистемы.
– Каким образом осуществляется передача ключей и сообщений без предварительного выполнения протокола обмена ключами?
– Опишите способ подписи документа на основе криптографии с открытыми ключами.
– Опишите свойства меток времени в электронных цифровых подписях документов?
– Каким образом норма языка выражается через энтропию и длину сообщения?
– Определите понятие абсолютной нормы языка.
– Определите понятие расстояния уникальности.
– Опишите упрощенную модель шифрования битовой строки.
– Приведите схему и опишите принцип работы поточного шифра.
– Приведите схему и опишите принцип работы блочного шифра.
– Охарактеризуйте основные операции и приведите блок-схему работы шифра Фейстеля.
– Охарактеризуйте основные операции и приведите блок-схему работы шифра DES.
– Приведите описание алгоритма с открытым ключом RSA.
– Какие технологии шифрования применяются в PGP?

3.2 Экзаменационные вопросы

– Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности.
– Программа информационной безопасности России и пути ее реализации.
– Проблемы защиты информации в компьютерных системах.
– Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации.
– Организационное обеспечение информационной безопасности.
– Криптографическая терминология.
– Алгоритмы и ключи.
– Симметричные алгоритмы.
– Алгоритмы с открытым ключом.
– Подстановочные и перестановочные шифры.
– Одноразовые блокноты.
– Однонаправленные хэш-функции.
– Передача информации с использованием криптографии с открытым ключом.
– Алгоритм симметричного шифрования данных DES.
– Асимметричный алгоритм шифрования данных RSA.
– Комплекс криптографических алгоритмов PGP.
– Защита информации от несанкционированного доступа.
– Физический, сетевой, транспортный и прикладной уровни защиты информации.
– Обзор стандартов в области защиты информации.
– Методы и средства защиты локальной рабочей станции.
– Защита в локальных сетях.

– Защита информации при межсетевом взаимодействии.
– Типы вирусов и средства антивирусной защиты.
– Обеспечение информационной безопасности в корпоративных сетях.

3.3 Темы лабораторных работ

– Программная реализация шифра, основанного на методе Полибия. Программная реализация шифра простой замены. Программная реализация шифра, основанного на методе умножения матриц.

– Алгоритм симметричного шифрования данных DES. Программная реализация асимметричного алгоритма шифрования RSA.

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. Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 616 с. [Электронный ресурс]. - http://e.lanbook.com/book/5154

4.2. Дополнительная литература

1. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. [Электронный ресурс]. - http://e.lanbook.com/book/5170

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 374 с. [Электронный ресурс]. - http://e.lanbook.com/book/11381

4.3. Учебно-методическое пособие и программное обеспечение

1. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/2261, свободный.

2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 17 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1822, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. Поисковая система google.ru