МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное образовательное учреждение высшего профессионального образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ **П.Е. Троян**
«1» 09 2016 г.

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 УЧ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уровень основной образовательной программы: бакалавриат

Направление подготовки (специальность): 11.03.03 Конструирование и технология электронных средств

Профиль: Проектирование и технология электронно-вычислительных средств

Форма обучения: очная

Факультет Безопасности

Кафедра Комплексной информационной безопасности электронно-вычислительных систем

Курс *1* **Семестр** *1*

Учебный план набора 2013 года и последующих лет.

Распределение рабочего времени:

№	Виды учебной работы	Семестр 1	Всего	Единицы
1.	Лекции	36	36	часов
2.	Лабораторные работы	16	16	часов
3.	Практические занятия	10	10	часов
4.	Курсовой проект/работа (КРС) (аудиторная)	не предусмотрено		часов
5.	Всего аудиторных занятий (Сумма 1-4)	62	62	часов
6.	Из них в интерактивной форме			часов
7.	Самостоятельная работа студентов (СРС)	46	46	часов
8.	Всего (без экзамена) (Сумма 5,7)	108	108	часов
9.	Самост. работа на подготовку, сдачу экзамена	36	36	часов
10.	Общая трудоемкость (Сумма 8,9)	144	144	часов
	(в зачетных единицах)	4	4	ЗЕТ

Экзамен 1 **семестр** **Диф. зачет** не предусмотрен

Томск 2016

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от « 12 » 4 2016 г.

Лист согласований

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) 11.03.03 Конструирование и технология электронных средств, утвержденного приказом № 1333 от 12.11.2015 г. рассмотрена и утверждена на заседании кафедры КИБЭВС «12» апреля 2016 г., протокол № 3.

Разработчики:
Профессор кафедры БИС _____ Р.В. Мещеряков

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

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

Декан Факультета Безопасности _____ /Е.М. Давыдова/

Зав. профилирующей кафедрой КИБЭВС _____ /А.А. Шелупанов/

Зав. выпускающей кафедрой КИБЭВС _____ /А.А. Шелупанов/

Эксперты:

Директор Центра Системного проектирования _____ /А.А. Конев/

Доцент кафедры БИС _____ /О.О. Евсютин/

1. Цели и задачи дисциплины

Целью дисциплины «Основы информационной безопасности» заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

Задачи дисциплины: ознакомление студентов с терминологией информационной безопасности; развитие мышления студентов; изучение методов и средств обеспечения информационной безопасности; обучение определению причин, видов, каналов утечки и искажения информации.

2. Место дисциплины в структуре ООП

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору профессионального цикла. Предшествующие дисциплины: Информатика. Последующие дисциплины: Безопасность программного обеспечения.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью использовать навыки работы с компьютером, владением методами информационных технологий, соблюдать основные требования информационной безопасности (ОПК-9).

В результате изучения дисциплины студент должен

Знать:

– сущность и понятие информационной безопасности и характеристику ее составляющих;

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

– источники и классификацию угроз информационной безопасности;

– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

Уметь:

– классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности;

– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.

Владеть:

– профессиональной терминологией в области информационной безопасности.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Вид учебной работы	Всего часов	Семестры	
		1	
Аудиторные занятия (всего)	62	62	
В том числе:	-	-	-
Лекции	36	36	
Лабораторные работы (ЛР)	16	16	
Практические занятия (ПЗ)	10	10	
Семинары (С)	не предусмотрены		

Коллоквиумы (К)	не предусмотрены		
Курсовой проект/(работа) (аудиторная нагрузка)	не предусмотрен		
Самостоятельная работа (всего)	46	46	
В том числе:	-	-	-
Курсовой проект (работа) (самостоятельная работа)	не предусмотрен		
Выполнение индивидуальных домашних заданий	18	18	
Проработка лекционного материала	7	7	
Подготовка к практическим занятиям	8	8	
Подготовка к контрольным работам	12	12	
Подготовка к тестовому опросу	7	7	
Вид промежуточной аттестации (зачет, экзамен)	36	36	
Общая трудоемкость час	144	144	
Зачетные Единицы Трудоемкости	4	4	

5. Содержание дисциплины

5.1. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции	Практич. занятия., лабораторные работы	Самост. работа студента	Всего час. (без экзам)	Формируемые компетенции (ОК, ОПК)
IV семестр						
1.	Понятие информационной безопасности, ее роль в национальной безопасности.	4		4	8	ОПК-9
2.	Терминологические основы информационной безопасности.	8	4	6	18	ОПК-9
3.	Угрозы. Классификация и анализ угроз информационной безопасности	4	6	9	18	ОПК-9
4.	Модель угроз, модель нарушителя.	4		7	11	ОПК-9
5.	Модели оценки угроз конфиденциальности, целостности, доступности	6	12	6	24	ОПК-9
6.	Функции и задачи защиты информации.	4	4	7	15	ОПК-9
7.	Проблемы региональной информационной безопасности.	6		1	7	ОПК-9
8.	Обсуждение результатов тестового опроса по курсу «Основы информационной безопасности».			6	6	ОПК-9

5.2. Содержание разделов дисциплины (по лекциям)

№ п/п	Наименование разделов	Содержание разделов	Трудоемкость (час.)	Формируемые компетенции (ОК, ОПК)
IV семестр				
1.	Понятие информационной безопасности, ее роль в национальной	Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи. Национальные инте-	4	ОПК-9

	безопасности.	ресы Российской Федерации в информационной сфере. Приоритетные направления в области защиты информации в Российской Федерации. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы. Правовое обеспечение защиты информации. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.		
2.	Терминологические основы информационной безопасности.	Понятие информации и смежных ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление. Идентификация, аутентификация, авторизация	8	ОПК-9
3.	Угрозы. Классификация и анализ угроз информационной безопасности	Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.	4	ОПК-9
4.	Модель угроз, модель нарушителя.	Классы каналов несанкционированного получения ин-	4	ОПК-9

		формации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Формирование модели нарушителя.		
5.	Модели оценки угроз конфиденциальности, целостности, доступности	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальных требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.	6	ОПК-9
6.	Функции и задачи защиты информации.	Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование	4	ОПК-9

		доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека.		
7.	Проблемы региональной информационной безопасности.	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	6	ОПК-9

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины из табл.5.1, для которых необходимо изучение обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин													
		1	2	3	4	5	6	7	8						
Предшествующие дисциплины															
1.	Информатика	+	+	+	+	+	+	+							
Последующие дисциплины															
1.	Безопасность программного обеспечения	+	+	+	+	+	+	+	+						

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Перечень компетенций	Виды занятий				Формы контроля
	Л	Лаб	Пр	СРС	
ОПК-9	+	+	+	+	Опрос на занятии, устный ответ на практическом занятии, тест, проверка конспекта, контрольная работа, защита индивидуального задания.

Л – лекция, Лаб – лабораторные работы, Пр – практические занятия, СРС – самостоятельная работа студента.

6. Методы и формы организации обучения. Технологии интерактивного обучения при разных формах занятий в часах

Не предусмотрено

7. Лабораторный практикум

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика практических занятий (семинаров)	Трудоемкость (час.)	Компетенции ОК, ПК
I семестр				
1.	3	Угрозы информации. Проведение анализа информации на предмет целостности	4	ОПК-9
2.	5	Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации	4	ОПК-9
3.	5	Классификация автоматизированных систем обработки информации по классу защиты информации	4	ОПК-9
4.	6	Оценка безопасности информации на объектах ее обработки	4	ОПК-9

8. Практические занятия (семинары)

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика практических занятий (семинаров)	Трудоемкость (час.)	Компетенции ОК, ОПК
IV семестр				
5.	2	Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы.	4	ОПК-9
6.	6	Оценка безопасности информации на объектах ее обработки	6	ОПК-9

9. Самостоятельная работа

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика самостоятельной работы *(детализация)*	Трудоемкость (час.)	Компетенции ОК, ПК	Контроль выполнения работы *(опрос, тест, дом. задание, и т.д)*
IV семестр					
1.	1,2,3,4,5,6,7	Проработка лекционного материала.	7	ОПК-9	Опрос, проверка домашнего задания
2.	2,3,5,6	Подготовка к практическим занятиям.	8	ОПК-9	Проверка на практических занятиях
3.	3,4	Выполнение индивидуального домашнего задания по теме	10	ОПК-9	Проверка индивидуального за-

		«Анализ безопасности информации».			дания
4.	1,2,3,4	Подготовка к контрольной работе.	12	ОПК-9	Проверка контрольной работы
5.	5,6	Выполнение индивидуального домашнего задания по теме «Создание системы защиты».	8	ОПК-9	Проверка индивидуального задания
6.	8	Подготовка к тестовому опросу.	7	ОПК-9	Тест

10. Примерная тематика курсовых проектов (работ)

Не предусмотрен

11. Рейтинговая система для оценки успеваемости студентов

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
Посещение занятий	4	5	4	**13**
Тестовый контроль	4	4	4	**12**
Индивидуальные домашние задания		5	5	**10**
Контрольные работы на практических занятиях		8	8	**16**
Устные ответы на практических занятиях	3	3	3	**9**
Выполнение индивидуального творческого задания		5	5	**10**
Итого максимум за период:	**11**	**30**	**29**	**70**
Сдача экзамена (максимум):				**30**
Два теоретических вопроса				20
Практическое задание				10
Нарастающим итогом	**11**	**41**	**70**	**100**

Таблица 11.2 Пересчет баллов в оценки за контрольные точки

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. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171 — Загл. с экрана.

2. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-6150-4 (21 экз в библ).

3. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс] : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179 — Загл. с экрана.

12.2 Дополнительная литература:

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163 — Загл. с экрана.

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 — Загл. с экрана.

12.3 Учебно-методические пособия и требуемое программное обеспечение:

Мещеряков Р.В. и др. Основы информационной безопасности. Электронный учебник. На сайте кафедры КИБЭВС. http://keva.tusur.ru. (включая методические указания к практическим работам).

Программное обеспечение
Операционная система Windows.
Среда Microsoft Office.

12.4 Необходимые базы данных, информационно-справочные и поисковые системы
http://www.portal.tusur.ru; http://www.lib.tusur.ru – образовательный портал университета;
http://www.iqlib.ru - электронная интернет библиотека;
http://www.biblioclub.ru – полнотекстовая электронная библиотека;
http://www.elibrary.ru - научная электронная библиотека;
http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
http://www.sec.ru – каталог фирм по информационной безопасности.

13. Материально-техническое обеспечение дисциплины

Мультимедийная лекционная аудитория.

Дисплейный класс с локальной вычислительной сетью.

Интерактивная доска с лицензионным программным обеспечением и мультимедиапроектор.

14. Методические рекомендации по организации изучения дисциплины

Не предусмотрены

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ **П. Е. Троян**
«1» 09 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ *ПО УЧЕБНОЙ ДИСЦИПЛИНЕ*

Основы информационной безопасности

Уровень основной образовательной программы	Бакалавриат
Направление подготовки	11.03.03 Конструирование и технология электронных средств
Профиль	Проектирование и технология электронно-вычислительных средств
Форма обучения	Очная

Факультет Безопасности (ФБ)

Кафедра Комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Курс 1 **Семестр 1**

Учебный план набора 2013 года и последующих лет.

Экзамен 1 семестр

Разработчик:

Профессор каф. БИС, д.т.н. _____ **/Р.В. Мещеряков/**

Томск 2016

Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины 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 используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенции
ОПК-9	способностью использовать навыки работы с компьютером, владением методами информационных технологий, соблюдать основные требования информационной безопасности	**Знать:** – сущность и понятие информационной безопасности и характеристику ее составляющих; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. **Уметь:** – классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. **Владеть:** – профессиональной терминологией в области информационной безопасности.

1 Реализация компетенций

1 Компетенция ОПК-9

ОПК-9: способностью использовать навыки работы с компьютером, владением методами информационных технологий, соблюдать основные требования информационной безопасности

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 2.

Таблица 2– Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	– сущность и понятие информационной безопасности и характеристику ее составляющих; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	– классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	– профессиональной терминологией в области информационной безопасности.
Виды занятий	– Лекции; – Практические занятия – Самостоятельная работа;	– Практические занятия – Самостоятельная работа;	– Практические занятия – Самостоятельная работа;
Используемые средства оценивания	– Опрос на лекции – Отчет по индивидуальной практической работе	– Отчет по индивидуальной практической работе	– Отчет по индивидуальной практической работе

Общие характеристики показателей и критериев оценивания компетенции на всех этапах приведены в таблице 3.

Таблица 3 – Общие характеристики показателей и критериев оценивания компетенции по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями по методам защиты информации и способам их применения	Обладает методами защиты информации	Способен описывать любые системы, определяя для них угрозы, а также предлагать способы защиты необходимые и достаточные для необходимого уровня защиты информации
Хорошо (базовый уровень)	Знает ключевые моменты, понимает значимость защиты информации, о непрерывности процессов по защите информации	Обладает практическими умениями по анализу угроз и определению необходимых способов защиты	Способен описывать любые системы, определяя для них угрозы, а также предлагать способы защиты
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, позволяющими осуществлять первичный анализ необходимости защиты информации	Способен определить перечень возможных угроз системы

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	• *представляет систематизированные результаты анализа необходимости защиты системы* • *предлагает обоснованные методы защиты информации*	• *свободно применяет методы защиты информации* • *умеет представлять и аргументированно доказывать полученные результаты*	• *использовать методы защиты информации, предлагать и обосновывать решения.*
Хорошо (базовый уровень)	• *представляет систематизированные результаты анализа необходимости защиты системы*	• *применяет простые методы защиты информации* • *умеет представлять полученные данные*	• *использовать методы защиты информации, предлагать решения.*

Удовлетворительно (пороговый уровень)	• *осуществляет первичные анализ системы по ключевым свойствам защиты информации*	• *применяет простые методы первичного анализа системы* • *умеет представлять полученные данные и их интерпретацию*	• *представлять сведения о необходимости защиты системы*

2 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются следующие материалы:

– 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 составе:

1. Опросы на лекции:

a. экспресс контрольные: список вопросов формируется из терминов, изученных на предыдущей лекции, а также принципиальных вопросов, имеющих краткие конкретные ответы.

i. назовите основные направления теории защиты информации

ii. раскройте понятие комплексности в теории защиты информации

iii. назовите основные методы и модели оценки уязвимости информации

iv. назовите основные классы каналов несанкционированного получения информации.

v. дайте характеристику модели защиты системы с полным перекрытием

vi. дайте характеристику источников угроз и предпоссылок появления угроз

vii. дайте характеристику основным стратегиям защиты информации

viii. какие общеметодологические принципы архитектуры системы защиты информации вы знаете.

b. опрос: диалог с аудиторией на предмет проведения анализа конкретного объекта информатизации, составления и обоснования перечня актуальных угроз, определение необходимых методов и средств для защиты информации на выбранном объекте.

Рассматривается офис компании, предназначенный для проведения конфиденциальных переговоров с партнерами. Задачи: необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

i. виды угроз;
ii. характер происхождения угроз;
iii. классы каналов несанкционированного получения информации;
iv. источники появления угроз;
v. причины нарушения целостности информации;
vi. потенциально возможные злоумышленных действий;
vii. определить класс защиты информации.

Необходимо предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

i. определить требования к защите информации;
ii. классифицировать автоматизированную систему;
iii. определить факторы, влияющие на требуемый уровень защиты информации;
iv. выбрать или разработать способы и средства защиты информации;
v. построить архитектуру систем защиты информации;
vi. сформулировать рекомендации по увеличению уровня защищенности.

3 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, в составе:

Основная литература:

1. Малюк, А.А. Введение в информационную безопасность [Электрон-

ный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171 — Загл. с экрана.

2. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-6150-4 (21 экз в библ).

3. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс] : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179 — Загл. с экрана.

Дополнительная литература:

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163 — Загл. с экрана.

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 — Загл. с экрана.

Учебно-методические пособия и требуемое программное обеспечение:

Мещеряков Р.В. и др. Основы информационной безопасности. Электронный учебник. На сайте кафедры КИБЭВС. http://keva.tusur.ru. (включая методические указания к практическим работам).