МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ **П. Е. Троян**
«8» 08 **2016 г.**

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Уровень основной образовательной программы: бакалавриат
Направление(я) подготовки (специальность): 09.03.01 Информатика и вычислительная техника
Специализация: Системы автоматизированного проектирования
Форма обучения: очная
Факультет Вычислительных систем
Кафедра Компьютерных систем в управлении и моделировании (КСУП)

Курс 4 **Семестр 7**

Учебный план набора 2013 г. и последующих лет.
Распределение рабочего времени:

№	Виды учебной работы	Семестр 1	Семестр 2	Семестр 3	Семестр 4	Семестр 5	Семестр 6	Семестр 7	Семестр 8	Всего	Единицы
1.	Лекции							24		24	часов
2.	Лабораторные работы							48		48	часов
3.	Практические занятия							-		-	часов
4.	Курсовой проект/работа (КРС) (аудиторная)							-		-	часов
5.	Всего аудиторных занятий (Сумма 1-4)							72		72	часов
6.	Из них в интерактивной форме							14		14	часов
7.	Самостоятельная работа студентов (СРС)							108		108	часов
8.	Всего (без экзамена) (Сумма 5,7)							180		180	часов
9.	Самост. работа на подготовку, сдачу экзамена							36		36	часов
10.	Общая трудоемкость (Сумма 8,9)							216		216	часов
	(в зачетных единицах)							6		6	ЗЕТ

Экзамен 7 семестр

Томск 2016

Согласована на портале № 11397

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «17» 6 2016 г.

Лист согласований

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего профессионального образования (ФГОС ВПО) по направлению подготовки (специальности) 09.03.01 Информатика и вычислительная техника «Системы автоматизированного проектирования», рассмотрена и утверждена на заседании кафедры «17» июня 2016 г., протокол № 6.

Разработчики:

Программист каф. КИБЭВС _____ /А.К. Новохрестов/

Зав. кафедрой КИБЭВС, профессор _____ /А.А. Шелупанов/

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

Декан факультета Вычислительных систем _____ /Е.В. Истигечева/

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

Зав. выпускающей кафедрой КСУП _____ /Ю.А. Шурыгин/

Эксперты:

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

Доцент каф. КИБЭВС _____ /М.А. Сопов/

Согласована на портале № 11397

1. Цели и задачи дисциплины:

Целью преподавания дисциплины является изучение комплекса проблем информационной безопасности предприятий и организаций различных типов и направлений деятельности, построения, функционирования и совершенствования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сфере охраны интеллектуальной собственности и сохранности информационных ресурсов.

2. Место дисциплины в структуре ООП:

Цикл дисциплины: Б1. Дисциплины (модули). Предшествующие дисциплины: Информатика; Операционные системы; Теория систем и системный анализ.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. (ОПК-5);

В результате изучения дисциплины студент должен:

Знать:

– базовые концепции и модели информационной безопасности;

– основы функционирования безопасности информационных систем;

– задачи информационной безопасности;

– законодательство по обеспечению информационной безопасности;

– стандарты в области информационной безопасности;

– методы и средства защиты информационной безопасности;

– направления и методы ведения аналитической работы по выявлению угроз;

– технические процедуры по действиям в нештатной ситуации;

– методологии оценки рисков и угроз информационной безопасности.

Уметь:

– выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем;

– проводить аудит для отображения уровням соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов;

– оценивать и выбирать необходимые средства защиты;

– осуществлять мониторинг состояния информационной безопасности объекта;

– обеспечивать противодействие атакам на информационную систему;

– выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности;

Владеть:

навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.

Согласована на портале № 11397

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6 (шесть) зачетных единиц.

Вид учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	24	24
Лабораторные работы (ЛР)	48	48
Практические занятия (ПЗ)	Не предусмотрено	
Семинары (С)	Не предусмотрено	
Коллоквиумы (К)	Не предусмотрено	
Курсовой проект/(работа) (аудиторная нагрузка)	Не предусмотрено	
Другие виды аудиторной работы	Не предусмотрено	
Самостоятельная работа (всего)	144	144
В том числе:		
Курсовой проект (работа) (самостоятельная работа)	Не предусмотрено	
Подготовка лабораторным занятиям	48	48
Индивидуальная работа	24	24
Контрольные работы	12	12
Лекционный материал	24	24
Вид промежуточной аттестации (экзамен)	36	36
Общая трудоемкость час	216	216
Зачетные Единицы Трудоемкости	6	6

5. Содержание дисциплины

5.1. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции	Лаборат. занятия	Практич. занятия.	Курсовой П/Р (КРС)	Самост. работа студента	Всего час. (без экзам)	Формируемые компетенции
1.	Базовые понятия в сфере обеспечения информационной безопасности.	2	-	Не предусмотрено	Не предусмотрено	2	4	ОПК-5
2.	Комплексный подход к обеспечению информационной безопасности.	2	-			2	4	ОПК-5
3.	Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	4	12			20	36	ОПК-5
4.	Методы оценки рисков и угроз информационной безопасности.	2	8			22	32	ОПК-5
5.	Программно-аппаратные, технические и криптографические средства защиты информации.	4	20			24	48	ОПК-5
6.	Основные принципы, направления и требования обеспечения информационной безопасности организации.	4	-			8	12	ОПК-5
7.	Концепция и политика информационной безопасности.	2	-			2	4	ОПК-5
8.	Реализации стратегии обеспечения информационной безопасности.	2	8			10	20	ОПК-5
9.	Менеджмент информационной безопасности.	2	-			18	20	ОПК-5
10.	**Итого**	**24**	**48**			**108**	**180**	

Согласована на портале № 11397

5.2. Содержание разделов дисциплины (по лекциям)

№ п/п	Наименование разделов	Содержание разделов	Трудоемкость (час.)	Формируемые компетенции (ОК, ПК, ПСК)
1.	Базовые понятия в сфере обеспечения информационной безопасности.	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	2	ОПК-5
2.	Комплексный подход к обеспечению информационной безопасности.	Структура системы защиты информации.	2	ОПК-5
3.	Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование.	4	ОПК-5
4.	Методы оценки рисков и угроз информационной безопасности.	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	2	ОПК-5
5.	Программно-аппаратные, технические и криптографические средства защиты информации.	Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа. Мандатное распределение доступа.	4	ОПК-5
6.	Основные принципы, направления и требования обеспечения информационной безопасности организации.	Определение организационных требований защиты ИТ.	4	ОПК-5
7.	Концепция и политика информационной безопасности.	Политика безопасности.	2	ОПК-5
8.	Реализации стратегии обеспечения информационной безопасности.	Определение организационных целей и стратегий защиты ИТ. Идентификация и анализ угроз активам ИТ в пределах организации. Определение соответствующих защитных мер.	2	ОПК-5
9.	Менеджмент информационной безопасности.	Контроль выполнения и функционирования защитных мер. Разработка и реализация программы осведомленности о защите. Обнаружение инцидентов и реагирование на них.	2	ОПК-5

Согласована на портале № 11397

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	9
Предшествующие дисциплины										
1.	Информатика	+	+		+	+	+			
2.	Операционные системы					+		+	+	+
3.	Теория систем и системный анализ		+		+			+	+	+

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

Перечень компетенций	Виды занятий					Формы контроля по всем видам занятий *(примеры)*
	Л	Лаб	Пр.	КР/КП	СРС	
ОПК-5	+	+			+	Опрос на лекции Отчет по лабораторной работе Контрольная работа Отчет по индивидуальному заданию Экзамен

Л – лекция, Пр – практические и семинарские занятия, Лаб – лабораторные работы, КР/КП – курсовая работа/проект, СРС – самостоятельная работа студента

6. Методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах

Методы \ Формы	Лекции (час)	Лабораторные работы (час)	Всего
IT-методы	-	7	7
Работы в малых группах	-	7	7
Итого интерактивных занятий	-	14	14

Согласована на портале № 11397

7. Лабораторный практикум

№ п/п	№ раздела дисциплины из табл. 5.1	Наименование лабораторных работ	Трудо-емкость (час.)	Компетенции ОК, ПК, ПСК
1	3	Защита персональных данных и коммерческой тайны	4	ОПК-5
2	3	Политика безопасности и инструкции для сотрудников предприятия	8	ОПК-5
3	4	Оценка рисков информационной безопасности	8	ОПК-5
4	5	Защита компьютерной информации на уроне доступа в систему	4	ОПК-5
5	5	Защита от атак по локальным и глобальным сетям	4	ОПК-5
6	5	Защита от вредоносного ПО	4	ОПК-5
7	5	Использование шифрования для защиты данных	4	ОПК-5
8	5	Использование физических носителей и защитных систем на их основе	4	ОПК-5
9	8	Разработка системы защиты предприятия	8	ОПК-5

8. Практические занятия (семинары)

Не предусмотрены

9. Самостоятельная работа

№ п/п	№ раздела дисциплины из табл. 5.1	Виды самостоятельной работы *(детализация)*	Трудо-емкость (час.)	Компетенции ОК, ПК, ПСК	Контроль выполнения работы (Опрос, тест, дом.задание, и т.д)
1.	1,2,3,4,5,6,7,8,9	Проработка лекционного материала	24	ОПК-5	Опрос на лекции
2.	3,4,5,8	Подготовка к лабораторным занятиям	48	ОПК-5	Отчет по лабораторной практической работе
3.	1,2,3,4,5,6,7,8,9	Подготовка к контрольным работам	12	ОПК-5	Контрольная работа
4.	4,8	Выполнение индивидуальных заданий	24	ОПК-5	Отчет по индивидуальному заданию
5.	1,2,3,4,5,6,7,8,9	Подготовка к экзамену	36	ОПК-5	Экзамен

10. Примерная тематика курсовых проектов (работ)

Не предусмотрено

Согласована на портале № 11397

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	2	3	3	**8**
Лабораторные работы	9	9	9	**27**
Индивидуальные задания	10	-	10	**20**
Контрольные работы	5	5	5	**15**
Итого максимум за период:	**26**	**17**	**27**	**70**
Экзамен	**-**	**-**	**-**	**30**
Нарастающим итогом	**26**	**43**	**70**	**100**

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

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)

Согласована на портале № 11397

12. Учебно-методическое и информационное обеспечение дисциплины

12.1 Основная литература:

1. **Основы защиты информации**. Учебное пособие / Шелупанов А.А., Сопов М.А. и др., Издание пятое, перераб. и допол. **Гриф СибРОУМО.** – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

12.2 Дополнительная литература

1. **Нормативно-правовые акты информационной безопасности**. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – **Гриф СибРОУМО** Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf
2. **Нормативно-правовые акты информационной безопасности**. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – **Гриф СибРОУМО** Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf
3. **Нормативно-правовые акты информационной безопасности**. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.3. Издание седьмое, перераб. и допол. – **Гриф СибРОУМО** Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

12.3 Учебно-методические пособия и программное обеспечение

Для обеспечения дисциплины используются следующие УМП:

1. **«Методические указания к лабораторным работам по дисциплине «Информационная безопасность»**, / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс]
URL: http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf
2. **«Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»»** / Сопов М.А., 2012г. – 2 с. [Электронный ресурс]
URL: http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf

12.4 Базы данных, информационно-справочные и поисковые системы

http://www.edu.tusur.ru – образовательный портал университета;
http://www.lib.tusur.ru – веб-сайт библиотеки университета;
http://www.elibrary.ru – научная электронная библиотека;
http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

13. Материально-техническое обеспечение дисциплины

1. Мультимедийная лекционная аудитория.
2. Компьютерный класс с выходом в Интернет.

14. Методические рекомендации по организации изучения дисциплины

Не предусмотрено.

Согласована на портале № 11397

Приложение к рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ЗАЩИТА ИНФОРМАЦИИ

Уровень основной образовательной программы:	бакалавриат
Направление(я) подготовки (специальность):	09.03.01 Информатика и вычислительная техника
Специализация:	Системы автоматизированного проектирования
Форма обучения:	очная
Факультет	Вычислительных систем
Кафедра	Компьютерных систем в управлении и моделировании (КСУП)
Курс 4	**Семестр 7**

Учебный план набора 2013 г. и последующих лет.

Экзамен 7 семестр

Томск 2016

Согласована на портале № 11397

Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины «Защита информации» 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 Защита информации 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-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и **с учетом основных требований информационной безопасности**	Знать: – базовые концепции и модели информационной безопасности; – основы функционирования безопасности информационных систем; – задачи информационной безопасности; – законодательство по обеспечению информационной безопасности; – стандарты в области информационной безопасности; – методы и средства защиты информационной безопасности; – направления и методы ведения аналитической работы по выявлению угроз; – технические процедуры по действиям в нештатной ситуации; – методологии оценки рисков и угроз информационной безопасности. Уметь: – выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; – проводить аудит для отображения уровням соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов; – оценивать и выбирать необходимые средства защиты; – осуществлять мониторинг состояния информационной безопасности объекта; – обеспечивать противодействие атакам на информационную систему; – выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности; Владеть: навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах

1 Реализация компетенций

1.1 Компетенция ОПК-5

Согласована на портале № 11397

ОПК-5: Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

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	– базовые концепции и модели информационной безопасности; – основы функционирования безопасности информационных систем; – задачи информационной безопасности; – законодательство по обеспечению информационной безопасности; – стандарты в области информационной безопасности; – методы и средства защиты информационной безопасности; – направления и методы ведения аналитической работы по выявлению угроз; – технические процедуры по действиям в нештатной ситуации; – методологии оценки рисков и угроз информационной безопасности	– выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; – проводить аудит для отображения уровням соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов; – оценивать и выбирать необходимые средства защиты; – осуществлять мониторинг состояния информационной безопасности объекта; – обеспечивать противодействие атакам на информационную систему; – выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности	навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах
Виды занятий	Лекции	Лабораторные работы Самостоятельная работа студентов Индивидуальное задание	Лабораторные работы Индивидуальное задание
Используемые средства оценивания	Контрольная работа Экзамен	Оформление отчетов и защита лабораторных работ Оформление и защита индивидуального задания Оценивание самостоятельной работы студента	Оформление отчетов и защита лабораторных Оформление и защита индивидуального задания Экзамен

Согласована на портале № 11397

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 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

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)	Знает: – базовые концепции и модели информационной безопасности; – основы функционирования безопасности информационных систем; – задачи информационной безопасности; – законодательство по обеспечению информационной безопасности; – стандарты в области информационной безопасности; – методы и средства защиты информационной безопасности; – направления и методы ведения аналитической работы по выявлению угроз; – технические процедуры по действиям в нештатной ситуации; – методологии оценки рисков и угроз	Умеет: – выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; – проводить аудит для отображения уровням соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов; – оценивать и выбирать необходимые средства защиты; – осуществлять мониторинг состояния информационной безопасности объекта; – обеспечивать противодействие атакам на информационную систему;	Навыками работы с программными и аппаратными средствами, обеспечивающими защиту информации в компьютерных системах

Согласована на портале № 11397

	информационной безопасности	– выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности	
Хорошо (базовый уровень)	Знает: – базовые концепции и модели информационной безопасности; – основы функционирования безопасности информационных систем; – задачи информационной безопасности; – стандарты в области информационной безопасности; – методы и средства защиты информационной безопасности;	Умеет: – оценивать и выбирать необходимые средства защиты; – осуществлять мониторинг состояния информационной безопасности объекта; – обеспечивать противодействие атакам на информационную систему; – выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности	Владеет навыками формирования и применения комплекса мер для обеспечения безопасности информации в организации.
Удовлетворительно (пороговый уровень)	Знает базовые концепции и модели информационной безопасности, а также методы и средства защиты информационной безопасности	Умеет: – обеспечивать противодействие атакам на информационную систему; – выполнять требования инструкции по обеспечению информационной безопасности	Владеет базовыми навыками необходимыми для обеспечения безопасности информации на организации.

2 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в составе:

- контрольная работа;
- лабораторные работы;
- самостоятельная работа;
- выполнение индивидуального задания;
- экзамен.

Согласована на портале № 11397

2.1. Темы контрольных работ

1. Основные понятия информационной безопасности. Организационно-правовое обеспечение информационной безопасности.
2. Оценка рисков. Программно-аппаратные средства защиты информации.
3. Политика безопасности. Менеджмент информационной безопасности.

2.2 Темы лабораторных работ

1. Защита персональных данных и коммерческой тайны
2. Политика безопасности и инструкции для сотрудников предприятия
3. Оценка рисков информационной безопасности
4. Защита компьютерной информации на уроне доступа в систему
5. Защита от атак по локальным и глобальным сетям
6. Защита от вредоносного ПО
7. Использование шифрования для защиты данных
8. Использование физических носителей и защитных систем на их основе
9. Разработка системы защиты предприятия

2.3 Тематика индивидуальных заданий

В семестре предусмотрено два индивидуальных задания:
1. Анализ защищенности объекта
2. Разработка (усовершенствование) системы защиты объекта.
Выбор объекта осуществляется студентами и согласовывается с преподавателем.

2.4 Вопросы к экзамену

1. Основные регуляторы
2. Основные нормативно-правовые акты
3. Определения: информация, безопасность информации, защита информации, информационная безопасность, информационный процесс, документ, носитель
4. Свойства информации
5. Виды информации и их определения
6. Государственная тайна
7. Определения: угрозы, несанкционированный доступ.
8. Формы представления информации
9. Классификация угроз
10. Способы реализации угроз
11. Определения: защищаемая информация, доступ, допуск, уязвимость, сзи...
12. Виды защиты информации
13. Конституционные основы в информационной сфере
14. Доктрина ИБ РФ (составляющие национальных интересов РФ)
15. ФЗ «Об информации, информационных технологиях и о защите информации»
16. Преступления в информационной сфере (УК)
17. Задачи организационного обеспечения ЗИ
18. Управление ИБ
19. Модель угроз и модель нарушителя

Согласована на портале № 11397

20. Сложности в работе с персоналом
21. Классификация инсайдерских угроз
22. Социальная инженерия
23. Определения (программно-аппаратная ЗИ): СВТ, доступ, допуск, идентификация, аутентификация
24. Дискреционное и мандатное управление доступом
25. Сертификация
26. Группы классов защищенности АС от НСД
27. Межсетевой экран, антивирус, СОВ
28. Криптографическое преобразование, зашифрование, расшифрование.
29. Хэш-функция и ее свойства
30. Электронная подпись

3 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

1. Основы защиты информации. Учебное пособие / Шелупанов А.А., Сопов М.А. и др., Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

2. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

4. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.3. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]
URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

Согласована на портале № 11397

5. «Методические указания к лабораторным работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс]
URL: http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf

6. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А., 2012г. – 2 с. [Электронный ресурс]
URL: http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf

Согласована на портале № 11397