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): **38.03.05 Бизнес-информатика**
Направленность (профиль): **Бизнес-информатика**
Форма обучения: **очная**
Факультет: **ФСУ, Факультет систем управления**
Кафедра: **АОИ, Кафедра автоматизации обработки информации**
Курс: **4**
Семестр: **7**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные занятия	18	18	часов
3	Всего аудиторных занятий	36	36	часов
4	Из них в интерактивной форме	6	6	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Зачет: 7 семестр

Томск 2016

Рассмотрена и одобрена на заседании кафедры
протокол № 11 от «30» 12 2016 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.03.05 Бизнес-информатика, утвержденного 2016-08-11 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

ассистент преподавателя каф.
КИБЭВС _____ Ганюшкин И. Г.

Заведующий обеспечивающей каф.
КИБЭВС _____ Шелупанов А. А.

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

Декан ФСУ _____ Сенченко П. В.

Заведующий выпускающей каф.
АОИ _____ Ехлаков Ю. П.

Эксперты:

Доцент ТУСУР ИСИБ КИБЭВС _____ Конев А. А.

1. Цели и задачи дисциплины

1.1. Цели дисциплины

заложить терминологический фундамент
научить правильно проводить анализ угроз информационной безопасности
научить выполнять основные этапы решения задач информационной безопасности
рассмотреть основные методологические принципы теории информационной безопасности
изучить методы и средства обеспечения информационной безопасности
изучить методы нарушения конфиденциальности, целостности и доступности информации

1.2. 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 ОПОП

Дисциплина «Информационная безопасность» (Б1.Б.36) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Базы данных, Вычислительные системы, сети и телекоммуникации, Информатика, Программирование, Теоретические основы информатики, Электронный бизнес.

Последующими дисциплинами являются: .

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности;

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 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	36	36
Лекции	18	18
Лабораторные занятия	18	18
Из них в интерактивной форме	6	6
Самостоятельная работа (всего)	36	36
Подготовка к контрольным работам	2	2
Выполнение домашних заданий	6	6

Выполнение индивидуальных заданий	8	8
Оформление отчетов по лабораторным работам	16	16
Проработка лекционного материала	4	4
Всего (без экзамена)	72	72
Общая трудоемкость час	72	72
Зачетные Единицы Трудоемкости	2.0	2.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

№	Названия разделов дисциплины	Лекции	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
1	Понятие информационной безопасности, ее роль в национальной безопасности	2	0	2	4	ОК-4
2	Терминологические основы информационной безопасности	2	0	2	4	ОК-4
3	Угрозы	2	0	1	3	ОК-4
4	Классификация и анализ угроз информационной безопасности	2	0	1	3	ОК-4
5	Модель угроз, модель нарушителя	4	8	10	22	ОК-4
6	Модели оценки угроз конфиденциальности, целостности, доступности	2	6	8	16	ОК-4
7	Функции и задачи защиты информации	2	4	8	14	ОК-4
8	Проблемы региональной информационной безопасности	2	0	4	6	ОК-4
	Итого	18	18	36	72	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Понятие информационной безопасности, ее роль в	Понятие информационной безопасности. Информационное право	2	ОК-4

национальной безопасности	в теории государства и права. Информация как объект правового регулирования. Национальные интересы Российской Федерации в информационной сфере. Правовое обеспечение защиты информации.		
	Итого	2	
2 Терминологические основы информационной безопасности	Основные термины и определения. Общедоступная информация и информация ограниченного доступа.	2	ОК-4
	Итого	2	
3 Угрозы	Угрозы. Уязвимости. Факторы. Характер происхождения угроз.	2	ОК-4
	Итого	2	
4 Классификация и анализ угроз информационной безопасности	Виды угроз. Источники угроз. Предпосылки появления угроз.	2	ОК-4
	Итого	2	
5 Модель угроз, модель нарушителя	Классы каналов несанкционированного получения информации. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Архитектура систем защиты информации.Семирубежная модель защиты информации.	4	ОК-4
	Итого	4	
6 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. Фундаментальные требования к вычислительным системам, которые используются для обработки конфиденциальной информации.	2	ОК-4
	Итого	2	
7 Функции и задачи защиты информации	Методы формирования функций защиты. Управление системой защиты информации. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на	2	ОК-4

	психику человека. Применение криптографии.		
	Итого	2	
8 Проблемы региональной информационной безопасности	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	2	ОК-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	6	7	8
Предшествующие дисциплины									
1	Базы данных	+	+	+			+		+
2	Вычислительные системы, сети и телекоммуникации		+	+		+			
3	Информатика		+						
4	Программирование			+	+				
5	Теоретические основы информатики		+						
6	Электронный бизнес	+	+	+	+	+	+	+	+

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	
ОК-4	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные лабораторные занятия	Всего
7 семестр		
IT-методы	2	2
Работа в команде	4	4
Итого за семестр:	6	6
Итого	6	6

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			
5 Модель угроз, модель нарушителя	Защита персональных данных.	4	ОК-4
	Защита от компьютерных вирусов.	4	
	Итого	8	
6 Модели оценки угроз конфиденциальности, целостности, доступности	Защита компьютерной информации на уровне доступ в систему.	6	ОК-4
	Итого	6	
7 Функции и задачи защиты информации	Защита от атак по локальным и глобальным сетям.	4	ОК-4
	Итого	4	
Итого за семестр		18	

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 Понятие	Проработка лекционного	2	ОК-4	Опрос на занятиях

информационной безопасности, ее роль в национальной безопасности	материала			
	Итого	2		
2 Терминологические основы информационной безопасности	Подготовка к контрольным работам	2	ОК-4	Контрольная работа
	Итого	2		
3 Угрозы	Проработка лекционного материала	1	ОК-4	Опрос на занятиях
	Итого	1		
4 Классификация и анализ угроз информационной безопасности	Проработка лекционного материала	1	ОК-4	Опрос на занятиях
	Итого	1		
5 Модель угроз, модель нарушителя	Оформление отчетов по лабораторным работам	4	ОК-4	Домашнее задание, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	4		
	Выполнение домашних заданий	2		
	Итого	10		
6 Модели оценки угроз конфиденциальности, целостности, доступности	Оформление отчетов по лабораторным работам	4	ОК-4	Домашнее задание, Отчет по лабораторной работе
	Выполнение домашних заданий	4		
	Итого	8		
7 Функции и задачи защиты информации	Оформление отчетов по лабораторным работам	4	ОК-4	Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Выполнение индивидуальных заданий	4		
	Итого	8		
8 Проблемы региональной информационной безопасности	Выполнение индивидуальных заданий	4	ОК-4	Отчет по индивидуальному заданию
	Итого	4		
Итого за семестр		36		
Итого		36		

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	Максимальный балл за период	Максимальный балл за период	Всего за семестр

	начала семестра	между 1КТ и 2КТ	между 2КТ и на конец семестра	
7 семестр				
Домашнее задание		15	10	25
Контрольная работа	5			5
Опрос на занятиях	15			15
Отчет по индивидуальному заданию			15	15
Отчет по лабораторной работе		30	10	40
Итого максимум за период	20	45	35	100
Нарастающим итогом	20	65	100	100

11.2. Пересчет баллов в оценки за контрольные точки

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

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

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

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

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
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. Шелупанов А.А., Сопов М.А. и др. Основы защиты информации. Учебное пособие. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты

информационной безопасности. Учебное пособие. 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]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

12.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

12.3. Учебно-методическое пособие и программное обеспечение

1. 1. Конев А. А., Костюченко Е.Ю., Сопов М.А. Методические указания по проведению лабораторных работ для специальности 040101 «Социальная работа», 2012. – 39 с. [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf

2. Парошин А.А. Информационная безопасность: стандартизированные термины и понятия. Методическое пособие, 2010 – 216 с. [Электронный ресурс]. Режим доступа (локальная сеть кафедры КИБЭВС): \\cesir\aos\Парошин – Стандаритзированные термины и понятия [2010].pdf [Электронный ресурс]. -

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

12.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрены

13. Материально-техническое обеспечение дисциплины

Мультимедийная лекционная аудитория.
Компьютерный класс с выходом в Интернет.

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): **38.03.05 Бизнес-информатика**
Направленность (профиль): **Бизнес-информатика**
Форма обучения: **очная**
Факультет: **ФСУ, Факультет систем управления**
Кафедра: **АОИ, Кафедра автоматизации обработки информации**
Курс: **4**
Семестр: **7**

Учебный план набора 2013 года

Разработчики:

- ассистент преподавателя каф. КИБЭВС Ганюшкин И. Г.

Зачет: 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
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	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. ; Должен уметь классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. ; Должен владеть профессиональной терминологией в области информационной безопасности;

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-4

ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности.

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	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	• Интерактивные лабораторные занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Интерактивные лабораторные занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Интерактивные лабораторные занятия; • Лабораторные занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Отчет по лабораторной работе; • Домашнее задание; • Отчет по	• Контрольная работа; • Отчет по лабораторной работе; • Домашнее задание; • Отчет по	• Отчет по лабораторной работе; • Домашнее задание; • Отчет по индивидуальному

	индивидуальному заданию; • Опрос на занятиях; • Зачет;	индивидуальному заданию; • Опрос на занятиях; • Зачет;	заданию; • 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)	• 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;

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 домашних заданий

– Проработка модели угроз и модели нарушителя для исследуемого объекта защиты

– Оценка угроз конфиденциальности, целостности, доступности информации на исследуемом объекте защиты

3.2 Темы индивидуальных заданий

– Построение модели с полным перекрытием

3.3 Темы опросов на занятиях

– Понятие информационной безопасности. Информационное право в теории государства и права. Информация как объект правового регулирования. Национальные интересы Российской Федерации в информационной сфере. Правовое обеспечение защиты информации.

– Угрозы. Уязвимости. Факторы. Характер происхождения угроз.

– Виды угроз. Источники угроз. Предпосылки появления угроз.

3.4 Темы контрольных работ

– Понятие информационной безопасности, основные термины и определения

3.5 Темы лабораторных работ

– Защита персональных данных.

– Защита компьютерной информации на уровне доступ в систему.

– Защита от компьютерных вирусов.
– Защита от атак по локальным и глобальным сетям.

3.6 Зачёт

– 1. Теория защиты информации. Основные направления. 2. Обеспечение информационной безопасности и направления защиты. 3. Комплексность (целевая, инструментальная, структурная, функциональная, временная). 4. Требования к системе защиты информации. 5. Угрозы информации. 6. Виды угроз. Основные нарушения. 7. Характер происхождения угроз. 8. Источники угроз. Предпосылки появления угроз. 9. Система защиты информации. 10. Классы каналов несанкционированного получения информации. 11. Причины нарушения целостности информации:. 12. Методы и модели оценки уязвимости информации. 13. Общая модель воздействия на информацию. 14. Общая модель процесса нарушения физической целостности информации. 15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. 16. Методологические подходы к оценке уязвимости информации. 17. Модель защиты системы с полным перекрытием. 18. Рекомендации по использованию моделей оценки уязвимости информации. 19. Допущения в моделях оценки уязвимости информации. 20. Методы определения требований к защите информации. 21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации. 22. Классификация требований к средствам защиты информации. 23. Требования к защите, определяемые структурой автоматизированной системы обработки данных. 24. Требования к защите, обуславливаемые видом защищаемой информации. 25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации. 26. Анализ существующих методик определения требований к защите информации. 27. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения. 28. Руководящем документе Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. Часть 1. 29. Классы защищенности средств вычислительной техники от несанкционированного доступа. 30. Факторы, влияющие на требуемый уровень защиты информации. 31. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты. 32. Методы формирования функций защиты. 33. События, возникающие при формировании функций защиты. 34. Классы задач функций защиты. 35. Класс задач функций защиты 1 — уменьшение степени распознавания объектов 36. Класс задач функций защиты 2 — защита содержания обрабатываемой, хранимой и передаваемой информации. 37. Класс задач функций защиты 3 — защита информации от информационного воздействия. 38. Функции защиты информации. 39. Стратегии защиты информации. 40. Способы и средства защиты информации. 41. Способы "абсолютной системы защиты". 42. Архитектура систем защиты информации. Требования. 43. Общеметодологических принципов архитектуры системы защиты информации. 44. Построение средств защиты информации. 45. Ядро системы защиты. 46. Семирубежная модель защиты.

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

2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. 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]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

4.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

4.3. Учебно-методическое пособие и программное обеспечение

1. 1. Конев А. А., Костюченко Е.Ю., Сопов М.А. Методические указания по проведению лабораторных работ для специальности 040101 «Социальная работа», 2012. – 39 с. [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf

2. Парошин А.А. Информационная безопасность: стандартизированные термины и понятия. Методическое пособие, 2010 – 216 с. [Электронный ресурс]. Режим доступа (локальная сеть кафедры КИБЭВС): \\cesir\aos\Парошин – Стандаритзированные термины и понятия [2010].pdf [Электронный ресурс]. -

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

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрены