МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **40.03.01 Юриспруденция**
Направленность (профиль) / специализация: **Юриспруденция**
Форма обучения: **очно-заочная (в том числе с применением дистанционных образовательных технологий)**
Факультет: **ФДО, Факультет дистанционного обучения**
Кафедра: **ИП, Кафедра информационного права**
Курс: **2**
Семестр: **4**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	8	8	часов
2	Самостоятельная работа под руководством преподавателя	6	6	часов
3	Часы на контрольные работы	2	2	часов
4	Самостоятельная работа	56	56	часов
5	Всего (без экзамена)	72	72	часов
6	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Контрольные работы: 4 семестр - 1
Зачёт: 4 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 40.03.01 Юриспруденция, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. КИБЭВС	_____	А. Ю. Якимук
Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФДО	_____	И. П. Черкашина
Заведующий выпускающей каф. ИП	_____	В. Г. Мельникова

Эксперты:

Старший преподаватель кафедры технологий электронного обучения (ТЭО)	_____	А. В. Гураков
Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

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.

1.2. Задачи дисциплины

– Ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности.

– Обучение студентов работе с основными средствами защиты.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» (Б1.В.02.12) относится к блоку 1 (вариативная часть).

Последующими дисциплинами являются: Информационное право, Проблемы доказывания при расследовании преступлений в сфере защиты компьютерной информации, Телекоммуникационное право.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-3 владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

– ОК-4 способностью работать с информацией в глобальных компьютерных сетях;

– ПК-2 способностью осуществлять профессиональную деятельность на основе развитого правосознания, правового мышления и правовой культуры;

В результате изучения дисциплины обучающийся должен:

– **знать** базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем и задачи информационной безопасности; законодательство по обеспечению информационной безопасности и стандарты в области 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.

– **владеть** навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.

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
		4 семестр
Контактная работа (всего)	14	14
Лекции	8	8
Самостоятельная работа под руководством преподавателя (СРП)	6	6
Часы на контрольные работы (всего)	2	2
Самостоятельная работа (всего)	56	56

Подготовка к контрольным работам	7	7
Проработка лекционного материала	7	7
Самостоятельное изучение тем (вопросов) теоретической части курса	42	42
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72
Зачетные Единицы	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	Лек., ч	СРП, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр					
1 Правовое обеспечение информационной безопасности	2	1	8	11	ОК-3, ОК-4, ПК-2
2 Организационное обеспечение информационной безопасности	1	1	8	10	ОК-3, ОК-4, ПК-2
3 Безопасность операционных систем	1	1	8	10	ОК-3, ОК-4, ПК-2
4 Безопасность систем баз данных	1	1	8	10	ОК-3, ОК-4, ПК-2
5 Безопасность вычислительных сетей	1	1	8	10	ОК-3, ОК-4, ПК-2
6 Криптографические методы защиты информации	1	1	8	10	ОК-3, ОК-4, ПК-2
7 Технические каналы утечки информации	1	0	8	9	ОК-3, ОК-4, ПК-2
Итого за семестр	8	6	56	72	
Итого	8	6	56	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
4 семестр			
1 Правовое обеспечение информационной безопасности	Понятие информационной безопасности. Информационное право в теории государства и права. Информация как объект правового регулирования. Защита информации. Информация ограниченного доступа. Правовые основы использованияорганизационных и	2	ОК-3, ОК-4

	технических средств защиты информации. Лицензирование деятельности в области защиты информации. Сертификация, стандартизация, аккредитация в информационной сфере.		
	Итого	2	
2 Организационное обеспечение информационной безопасности	Функции организационной составляющей системы защиты информации. Регламентация работы с информацией и ее носителями. Регламентация действий при осуществлении информационных процессов. Регламентация работы с элементами системы защиты информации.	1	ОК-3, ОК-4, ПК-2
	Итого	1	
3 Безопасность операционных систем	Ресурсы операционной системы. Методы обеспечения информационной безопасности в операционных системах. Аутентификация. Разграничение доступа. Аудит событий.	1	ОК-4, ПК-2
	Итого	1	
4 Безопасность систем баз данных	Введение в базы данных. Обеспечение безопасности систем баз данных	1	ОК-3, ОК-4, ПК-2
	Итого	1	
5 Безопасность вычислительных сетей	Классификация сетей. Типовая сеть крупной организации. Уровни информационной инфраструктуры корпоративной сети.Классификация угроз, уязвимостей, атак. Защитные механизмы и контрмеры.	1	ОК-4, ПК-2
	Итого	1	
6 Криптографические методы защиты информации	Требования к криптосистемам. Основные алгоритмы шифрования. Управление ключами.	1	ОК-3, ПК-2
	Итого	1	
7 Технические каналы утечки информации	Технические каналы утечки информации. Методы и средства защиты информации от утечки по техническим каналам.	1	ОК-3, ОК-4, ПК-2
	Итого	1	
Итого за семестр		8	

5.3. Содержание разделов дисциплины (самостоятельная работа под руководством преподавателя)

Содержание разделов дисциплин (самостоятельная работа под руководством преподавателя) приведено в таблице 5.3.

Таблица 5.3 – Содержание разделов дисциплин (самостоятельная работа под руководством преподавателя)

Названия разделов	Содержание разделов дисциплины (самостоятельная работа под руководством преподавателя)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Правовое обеспечение информационной безопасности	Понятие информационной безопасности. Информационное право в теории государства и права. Информация как объект правового регулирования. Защита информации. Информация ограниченного доступа. Правовые основы использованияорганизационных и технических средств защиты информации. Лицензирование деятельности в области защиты информации. Сертификация, стандартизация, аккредитация в информационной сфере.	1	ОК-3, ОК-4
	Итого	1	
2 Организационное обеспечение информационной безопасности	Функции организационной составляющей системы защиты информации. Регламентация работы с информацией и ее носителями. Регламентация действий при осуществлении информационных процессов. Регламентация работы с элементами системы защиты информации.	1	ОК-3, ОК-4, ПК-2
	Итого	1	
3 Безопасность операционных систем	Ресурсы операционной системы. Методы обеспечения информационной безопасности в операционных системах. Аутентификация. Разграничение доступа. Аудит событий.	1	ОК-4, ПК-2
	Итого	1	
4 Безопасность систем баз данных	Введение в базы данных. Обеспечение безопасности систем баз данных	1	ОК-3, ОК-4, ПК-2
	Итого	1	
5 Безопасность вычислительных сетей	Классификация сетей. Типовая сеть крупной организации. Уровни информационной инфраструктуры корпоративной сети.Классификация угроз, уязвимостей, атак. Защитные механизмы и контрмеры.	1	ОК-4, ПК-2
	Итого	1	

6 Криптографические методы защиты информации	Требования к криптосистемам. Основные алгоритмы шифрования. Управление ключами.	1	ОК-3, ПК-2
	Итого	1	
Итого за семестр		6	

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

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.4.

Таблица 5.4 – 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
Последующие дисциплины							
1 Информационное право	+	+					
2 Проблемы доказывания при расследовании преступлений в сфере защиты компьютерной информации			+	+	+	+	+
3 Телекоммуникационное право					+		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.5.

Таблица 5.5 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	СРП	Лек.	Сам. раб.	
ОК-3	+	+	+	Контрольная работа, Тест, Опрос на занятиях, Зачёт
ОК-4	+	+	+	Контрольная работа, Тест, Опрос на занятиях, Зачёт
ПК-2	+	+	+	Контрольная работа, Тест, Опрос на занятиях, Зачёт

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Часы на контрольные работы

Часы на контрольные работы приведены в таблице 8.1.

Таблица 8.1 – Часы на контрольные работы

№	Вид контрольной работы	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1	Контрольная работа с автоматизированной проверкой	2	ОК-3, ОК-4, ПК-2

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
4 семестр				
1 Правовое обеспечение информационной безопасности	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-4, ПК-2, ОК-3	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
2 Организационное обеспечение информационной безопасности	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-4, ПК-2, ОК-3	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
3 Безопасность операционных систем	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-4, ПК-2, ОК-3	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
4 Безопасность систем баз данных	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-4, ПК-2, ОК-3	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		

5 Безопасность вычислительных сетей	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-3, ОК-4, ПК-2	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
6 Криптографические методы защиты информации	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-4, ПК-2, ОК-3	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
7 Технические каналы утечки информации	Самостоятельное изучение тем (вопросов) теоретической части курса	6	ОК-3, ПК-2, ОК-4	Зачёт, Контрольная работа, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Подготовка к контрольным работам	1		
	Итого	8		
	Выполнение контрольной работы	2	ОК-3, ОК-4, ПК-2	Контрольная работа
Итого за семестр		56		
Итого		56		

10. Контроль самостоятельной работы (курсовой проект / курсовая работа)

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Основы защиты информации [Электронный ресурс]: учебное пособие. Изд. 5-е, перераб. И доп. / Шелупанов А.А [и др.]. – Томск: В-Спектр, 2011. – 244 с. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/.

12.2. Дополнительная литература

1. Шелупанов А. А. Нормативно-правовые акты информационной безопасности - 1 [Электронный ресурс]: Дополнительные материалы / Шелупанов А. А., Сопов М. А. - Томск: В-

Спектр, 2013. – 244 с. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/.

2. Шелупанов А. А. Нормативно-правовые акты информационной безопасности - 2 [Электронный ресурс]: Дополнительные материалы / Шелупанов А. А., Сопов М. А. - Томск: В-Спектр, 2013. – 222 с. Доступ из личного кабинета студента — Режим доступа: https://study.tusur.ru/study/library/.

3. Шелупанов А. А. Нормативно-правовые акты информационной безопасности - 3 [Электронный ресурс]: Дополнительные материалы / Шелупанов А. А., Сопов М. А. - Томск: В-Спектр, 2013. – 264 с. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/.

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Е. Ю. Костюченко. Основы информационной безопасности [Электронный ресурс]: методические указания по организации самостоятельной работы для студентов очно-заочной формы обучения направления подготовки 40.03.01 – Юриспруденция, обучающихся с применением дистанционных образовательных технологий/ Костюченко Е. Ю., Шелупанов А. А. – Томск: ФДО, ТУСУР, 2018. – 23 с. — Режим доступа: https://study.tusur.ru/study/library/.

2. Костюченко Е.Ю. Основы защиты информации: электронный курс / Е.Ю. Костюченко – Томск : ФДО, ТУСУР, 2018. Доступ из личного кабинета студента

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. eLIBRARY.RU: крупнейший российский информационный портал в области науки, технологии, медицины и образования (https://www.elibrary.ru);
2. веб-сайт системы федеральных образовательных порталов (http://www.edu.ru);
3. образовательный портал факультета безопасности (http://edu.fb.tusur.ru);
4. Федеральная служба по техническому и экспортному контролю (https://fstec.ru).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение дисциплины

Кабинет для самостоятельной работы студентов
помещение для самостоятельной работы
634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.
Описание имеющегося оборудования:
- Веб-камера - 6 шт.;
- Наушники с микрофоном - 6 шт.;
- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Google Chrome
- Kaspersky Endpoint Security для Windows
- Microsoft Windows
- OpenOffice (с возможностью удаленного доступа)

13.1.2. Материально-техническое и программное обеспечение для лекционных занятий

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

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какая из нижеперечисленных задач, изложенных в Доктрине информационной безопасности Российской Федерации, не относится к задачам государственных органов в рамках деятельности по обеспечению информационной безопасности:

a) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

b) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

c) планирование и разработка мер по проведению киберразведовательных операций;

d) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения.

2. В стандарте США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" в зависимости от конкретных значений,

которым отвечают автоматизированные системы, они разделены на…

a) 5 классов;

b) 4 группы;

c) 3 множества;

d) 2 подгруппы.

3. Что из нижеперечисленного не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?

a) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

b) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

c) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

4. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США» называют …

a) «Желтой книгой»;

b) «Оранжевым документом»;

c) «Оранжевой книгой»;

d) «Красным списком».

5. Модель угроз безопасности информации не включает в себя:

a) Описание информационной системы и ее структурно-функциональных характеристик;

b) Описание угроз безопасности информации;

c) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;

d) Стадии (этапы работ) создания системы защиты информационной системы.

6. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

a) Проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

b) Установка средств мониторинга сетевой инфраструктуры;

c) Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;

d) Внедрение документов, регламентирующих организационные меры по защите информации.

7. Методический документ ФСТЭК России «Методика определения безопасности информации в информационных системах» применяется совместно с:

a) Базой данных уязвимостей, разработанной Федеральной службой безопасности Российской Федерации;

b) Банком данных угроз безопасности информации, сформированным ФСТЭК России;

c) Общедоступной базой данных компьютерных угроз;

d) Перечнем сведений конфиденциального характера.

8. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…

a) Несанкционированный доступ;

b) Злоумышленный доступ;

c) Неразрешенный доступ;

d) Запретный доступ.

9. Какой вид информации не относится к категории конфиденциальной информации?

a) Коммерческая тайна;

b) Тайна судопроизводства;

c) Персональные данные;

d) Государственная тайна.

10. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?

a) Конфиденциальная информация;

b) Персональные данные;

c) Информация про личность;

d) Информация с ограниченным доступом.

11. Каналы несанкционированного получения информации сгруппированы в…

a) 3 класса;

b) 4 класса;

c) 7 классов;

d) 9 классов.

12. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …

a) Моделью безопасности;

b) Методом шифрования;

c) Компьютерной безопасностью;

d) Политикой безопасности.

13. Общая, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов – это …

a) Миссия;

b) Стратегия;

c) Функция;

d) Процесс.

14. Что из перечисленного не является целью проведения аудита безопасности?

a) Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы;

b) Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы;

c) Оценка будущего уровня защищенности системы;

d) Оценка соответствия системы существующим стандартам в области информационной

безопасности

15. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:

a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;

b) Способностью обнаруживать ранее неизвестные атаки;

c) Простотой в настройке и эксплуатации для конечного пользователя системы;

d) Популярностью использования в системах антивирусной защиты.

16. Модель системы с полным перекрытием характеризуется следующим положением:

a) В автоматизированной системе средствами защиты «перекрыто» большинство каналов утечки;

b) В механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации;

c) В системе защиты присутствует только одно средство для перекрытия всех угроз безопасности;

d) Автоматизированная система является системой множественного доступа.

17. Инструментальная комплексность в сфере информационной безопасности подразумевает:

a) Непрерывность осуществления мероприятий по защите информации;

b) Защиту информации от внешних и внутренних угроз;

c) Интеграцию всех видов и направлений ИБ для достижения поставленных целей;

d) Обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

18. Какой документ устанавливает цель, задачи и структуру стандартов по защите информации, объединяющий аспекты стандартизации в данной области и являющийся основополагающим стандартом в области защиты информации:

a) ГОСТ Р 52069.0-2013;

b) ФЗ №152 от 27.07.2006;

c) Постановление Правительства РФ №119 от 01.11.2012;

d) Конституция РФ.

19. Деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России) называется

a) Аттестация средств защиты информации;

b) Сертификация средств защиты информации;

c) Комплексное тестирование средств защиты информации;

d) Выборка средств защиты информации.

20. Положения Федерального закона №149 от 27.06.2006 не распространяются на:

a) Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;

b) Отношения, возникающие при применении информационных технологий;

c) Отношения, возникающие при обеспечении защиты информации;

d) Отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

14.1.2. Темы контрольных работ

Дисциплина “Основы информационной безопасности”

1. Риск информационной безопасности это

a) Число уязвимостей в системе;

b) Отношение стоимости системы защиты к вероятности её «простоя»;

c) Сочетание вероятности угрозы информационной безопасности и последствий её наступления;

d) Оценка стоимости защитных средств.

2. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …

a) Угрозой безопасности;
b) Компьютерной безопасностью;
c) Анализом угроз;
d) Атакой на информационную систему.
3. Что из перечисленного происходит при использовании RAID-массивов?
a) Производится полное шифрование данных;
b) Обеспечивается более высокий уровень защиты от вирусов;
c) Повышается надёжность хранения данных;
d) Увеличивается максимальная пропускная способность сети.
4. Заключительным этапом построения системы защиты является …
a) Анализ уязвимых мест;
b) Планирование;
c) Обследование;
d) Сопровождение.
5. Что из перечисленного не используется в биометрической аутентификации?
a) Рисунок папиллярного узора;
b) Клавиатурный почерк;
c) Пластиковая карта с магнитной полосой;
d) Радужная оболочка глаза.
6. К какой подсистеме не предъявляются требования в Руководящем документе «Классификация автоматизированных систем и требований по защите информации»?
a) управления доступом;
b) регистрации и учета;
c) технической защиты информации;
d) обеспечения целостности.
7. Защита информации это:
a) Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;
b) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
c) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
d) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
8. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
a) Отсутствием управления доступом;
b) Произвольным управлением доступом;
c) Принудительным управлением доступом;
d) Верифицируемой безопасностью.
9. Свойство доступности достигается за счет применения мер, направленных на повышение:
a) Аутентичности;
b) Непротиворечивости;
c) Отказоустойчивости;
d) Неотказуемости.
10. Каким термином называется защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
a) Конфиденциальная информация;
b) Секретная информация;
c) Военная тайна;
d) Государственная тайна

14.1.3. Темы опросов на занятиях

1. Правовое обеспечение информационной безопасности. Основные методы.
2. Организационное обеспечение информационной безопасности. Основные методы.

3. Безопасность операционных систем. Основные методы.

4. Безопасность систем баз данных. Основные методы.

5. Безопасность вычислительных сетей. Основные методы.

6. Криптографические методы защиты информации. Основные методы.

7. Технические каналы утечки информации. Основные методы.

14.1.4. Зачёт

Приведены примеры типовых заданий из банка контрольных тестов, составленных по пройденным разделам дисциплины

1. Анализ уязвимостей информационной системы проводится в целях:

a) Оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации;

b) Оценки эффективности использования политик разграничения доступа;

c) Оптимизации производительности программно-аппаратных средств защиты информации;

d) Сегментации информационной системы.

2. Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности называется:

a) Аттестация;

b) Аудит;

c) Сертификация;

d) Пентест.

3. Что из нижеперечисленного не относится к международным методикам проведения тестирования на проникновение, ориентированных на моделирование атак, направленных

на сетевую инфраструктуру организации:

a) Trusted Computer System Evaluation Criteria;

b) PCI DSS;

c) NIST SP800-115;

d) Open Source Security Testing Methodology Manual.

4. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:

a) Характеристика нарушителя;

b) Модель нарушителя;

c) Сценарий нарушителя;

d) Модель источников угроз.

5. Какое из нижеперечисленных направлений не относится к аттестации объектов информатизации по требованиям безопасности информации:

a) Аттестация автоматизированных систем, средств связи, обработки и передачи информации;

b) Аттестация помещений, предназначенных для ведения конфиденциальных переговоров;

c) Аттестация рабочих мест с целью оценки условий труда;

d) Аттестация технических средств, установленных в выделенных помещениях и защищаемых помещениях.

6. Стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта

a) Тестировение черного ящика;

b) Тестирование белого ящика;

c) Тестирование красного ящика;

d) Тестирование неизвестного ящика.

7. Методика тестирования на проникновение называется:

a) Аудит;

b) Пентест;

c) Honeypot;

d) Metasploit

8. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности:

a) Построение модели нарушителя;

b) Идентификация ресурсов;

c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам; d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.

9. Какая угроза безопасности информации является преднамеренной ?

a) Ошибки персонала;

b) Сбой программного обеспечения;

c) Фальсификация, подделка документов;

d) Открытие электронного письма, содержащего вирус.

10. Территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных называется …

a) Неконтролируемой зоной;

b) Зоной помещений автоматизированной системы;

c) Зоной баз данных защищаемой системы;

d) Зоной контролируемой территории.

11. Угроза диверсии относится к …

a) Субъективной преднамеренной причине нарушения целостности информации;

b) Субъективной непреднамеренной причине нарушения целостности информации;

c) Объективной непреднамеренной причине нарушения целостности информации;

d) Объективной преднамеренной причине нарушения целостности информации.

12. Перехват данных является угрозой:

a) Доступности;

b) Конфиденциальности;

c) Целостности;

d) Достоверности.

13. Продолжите тезис верно: Класс задач «Легендирование» по защите информации…

a) Не существует;

b) Потерял актуальность в связи с переходом на новые стандарты симметричных криптосистем;

c) Предполагает включение в состав элементов системы обработки информации дополнительных компонентов;

d) Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта.

14. Задачи по резервированию системы защиты делятся на:

a) Теплое и холодное резервирование;

b) Холодное и горячее резервирование;

c) Белое и серое резервирование;

d) Толстое и тонкое резервирование.

15. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…

a) Несанкционированный доступ;

b) Злоумышленный доступ;

c) Неразрешенный доступ;

d) Запретный доступ.

16. Какой вид информации не относится к категории конфиденциальной информации?

a) Коммерческая тайна;

b) Тайна судопроизводства;

c) Персональные данные;

d) Государственная тайна.

17. Положения Федерального закона №149 от 27.06.2006 не распространяются на:

a) Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;

b) Отношения, возникающие при применении информационных технологий;

c) Отношения, возникающие при обеспечении защиты информации;

d) Отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

18. К какой подсистеме не предъявляются требования в Руководящем документе «Классификация автоматизированных систем и требований по защите информации»?

a) управления доступом;

b) регистрации и учета;

c) технической защиты информации;

d) обеспечения целостности.

19. Что из перечисленного не используется в биометрической аутентификации?

a) Рисунок папиллярного узора;

b) Клавиатурный почерк;

c) Пластиковая карта с магнитной полосой;

d) Радужная оболочка глаза.

20. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …

a) Угрозой безопасности;

b) Компьютерной безопасностью;

c) Анализом угроз;

d) Атакой на информационную систему.

14.1.5. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

- чтение или просмотр материала необходимо осуществлять медленно, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

- если в тексте встречаются термины, следует выяснить их значение для понимания дальнейшего материала;

- необходимо осмысливать прочитанное и изученное, отвечать на предложенные вопросы.

Студенты могут получать индивидуальные консультации с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия в форме вебинаров. Расписание вебинаров публикуется в кабинете студента на сайте Университета. Запись вебинара публикуется в электронном курсе по дисциплине.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.