МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П.Е. Троян
«19» 12 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.01 Информатика и вычислительная техника**
Направленность (профиль) / специализация: **Системы автоматизированного проектирования**
Форма обучения: **заочная (в том числе с применением дистанционных образовательных технологий)**
Факультет: **Факультет дистанционного обучения (ФДО)**
Кафедра: **Кафедра компьютерных систем в управлении и проектировании (КСУП)**
Курс: **4**
Семестр: **8**
Учебный план набора 2019 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	8 семестр	Всего	Единицы
Лабораторные занятия	12	12	часов
Самостоятельная работа	84	84	часов
Самостоятельная работа под руководством преподавателя	6	6	часов
Контрольные работы	2	2	часов
Подготовка и сдача зачета	4	4	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
		3	з.е.

Формы промежуточной аттестация	Семестр	Количество
Зачет	8	
Контрольные работы	8	1

Томск

Согласована на портале № 68168

1. Общие положения

1.1. Цели дисциплины

1. 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

1. Ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности.
2. Обучение студентов работе с основными средствами защиты.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Индекс дисциплины: Б1.О.25.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 68168

ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.1. Знает основы информационных технологий и программирования и основные компоненты программных средств, а также их назначение и состав	Знает 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.
	ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности, а также обосновывать их выбор	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.
	ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	Владеет навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.

Согласована на портале № 68168

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности, основы информационной и библиографической культуры, современные информационно-коммуникационные технологии для поиска и анализа информации, основные требования информационной безопасности в профессиональной деятельности	Знает методы и средства защиты информационной безопасности направления и методы ведения аналитической работы по выявлению угроз технические процедуры по действиям в нештатной ситуации.
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Умеет оценивать и выбирать необходимые средства защиты осуществлять мониторинг состояния информационной безопасности объекта.
	ОПК-3.3. Владеет навыками подготовки и оформления информационных ресурсов, например, в виде обзоров, рефератов, докладов по вопросам профессиональной деятельности, с применением современных технологий и с учетом основных требований информационной безопасности	Владеет навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.
Профессиональные компетенции		

Согласована на портале № 68168

ПКР-1. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПКР-1.1. Знает : основные принципы построения ИС, автоматизирующих задачи организационного управления и бизнес-процессы; современные программные средства для построения, модификации и сопровождения АИС	Знает методологии оценки рисков и угроз информационной безопасности.
	ПКР-1.2. Умеет: выполнять и управлять работами по созданию (модификации) и сопровождению АИС, автоматизирующих задачи организационного управления и бизнес-процессы	Умеет обеспечивать противодействие атакам на информационную систему; выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности.
	ПКР-1.3. Владеет: навыками по созданию, модификации и сопровождению АИС	Владеет навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	20	20
Лабораторные занятия	12	12
Самостоятельная работа под руководством преподавателя	6	6
Контрольные работы	2	2
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	84	84
Самостоятельное изучение тем (вопросов) теоретической части дисциплины	36	36
Подготовка к контрольной работе	24	24
Подготовка к лабораторной работе	20	20
Написание отчета по лабораторной работе	4	4
Подготовка и сдача зачета	4	4
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Согласована на портале № 68168

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лаб. раб.	Контр. раб.	СРП, ч.	Сам. раб., ч	Всего часов (без промежуточной аттестации)	Формируемые компетенции
8 семестр						
1 Правовое обеспечение информационной безопасности	-	2	1	10	13	ОПК-2, ОПК-3, ПКР-1
2 Организационное обеспечение информационной безопасности	-		1	10	11	ОПК-2, ОПК-3, ПКР-1
3 Безопасность операционных систем.	12		1	34	47	ОПК-2, ОПК-3, ПКР-1
4 Безопасность систем баз данных.	-		1	10	11	ОПК-2, ОПК-3, ПКР-1
5 Безопасность вычислительных сетей.	-		1	10	11	ОПК-2, ОПК-3, ПКР-1
6 Криптографические методы защиты информации. Технические каналы утечки информации.	-		1	10	11	ОПК-2, ОПК-3, ПКР-1
Итого за семестр	12	2	6	84	104	
Итого	12	2	6	84	104	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины	СРП, ч	Формируемые компетенции
8 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 использования организационных и технических средств защиты информации. Лицензирование деятельности в области защиты информации. Сертификация, стандартизация, аккредитация в информационной сфере.	1	ОПК-2, ОПК-3
	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	ОПК-2, ПКР-1
	Итого	1	

Согласована на портале № 68168

3 Безопасность операционных систем.	Ресурсы операционной системы. Методы обеспечения информационной безопасности в операционных системах. Аутентификация. Разграничение доступа. Аудит событий.	1	ОПК-2, ОПК-3, ПКР-1
	Итого	1	
4 Безопасность систем баз данных.	Введение в базы данных. Обеспечение безопасности систем баз данных.	1	ОПК-2, ОПК-3, ПКР-1
	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	ОПК-2, ОПК-3, ПКР-1
	Итого	1	
6 Криптографические методы защиты информации. Технические каналы утечки информации.	Требования к криптосистемам. Основные алгоритмы шифрования. Управление ключами. Технические каналы утечки информации.	1	ОПК-2, ОПК-3, ПКР-1
	Итого	1	
Итого за семестр		6	
Итого		6	

5.3. Контрольные работы

Виды контрольных работ и часы на контрольные работы приведены в таблице 5.3.

Таблица 5.3 – Контрольные работы

№ п.п.	Виды контрольных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1	Контрольная работа с автоматизированной проверкой	2	ОПК-2, ОПК-3, ПКР-1
Итого за семестр		2	
Итого		2	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
3 Безопасность операционных систем.	Администрирование учетных записей пользователей	4	ОПК-2, ОПК-3
	Управление параметрами операционной системы	4	ОПК-2, ОПК-3, ПКР-1
	Политика ограниченного использования программ	4	ОПК-2, ОПК-3, ПКР-1
	Итого	12	
Итого за семестр		12	
Итого		12	

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

Согласована на портале № 68168

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Правовое обеспечение информационной безопасности	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	10		
2 Организационное обеспечение информационной безопасности	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	10		
3 Безопасность операционных систем.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к лабораторной работе	20	ОПК-2, ОПК-3, ПКР-1	Лабораторная работа
	Написание отчета по лабораторной работе	4	ОПК-2, ОПК-3, ПКР-1	Отчет по лабораторной работе
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	34		
4 Безопасность систем баз данных.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	10		

Согласована на портале № 68168

5 Безопасность вычислительных сетей.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	10		
6 Криптографические методы защиты информации. Технические каналы утечки информации.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-2, ОПК-3, ПКР-1	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-2, ОПК-3, ПКР-1	Контрольная работа
	Итого	10		
Итого за семестр		84		
	Подготовка и сдача зачета	4		Зачет
Итого		88		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лаб. раб.	Конт.Раб.	СРП	Сам. раб.	
ОПК-2	+	+	+	+	Зачёт, Контрольная работа, Лабораторная работа, Отчет по лабораторной работе, Тестирование
ОПК-3	+	+	+	+	Зачёт, Контрольная работа, Лабораторная работа, Отчет по лабораторной работе, Тестирование
ПКР-1	+	+	+	+	Зачёт, Контрольная работа, Лабораторная работа, Отчет по лабораторной работе, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. 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 Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf .

7.2. Дополнительная литература

Согласована на портале № 68168

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 Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: 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 Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.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 Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Якимук А. Ю. Защита информации. Методические указания по выполнению лабораторной работы: Методические указания / Якимук А. Ю., Конев А. А. - Томск : ФДО, ТУСУР, 2017. – 81 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://study.tusur.ru/study/library.

2. Костюченко Е. Ю. Основы информационной безопасности. Методические указания по организации самостоятельной работы: Методические указания / Костюченко Е. Ю., Шелупанов А. А. - Томск : ФДО, ТУСУР, 2018. – 22 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://study.tusur.ru/study/library.

7.3.2. 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.

7.4. Иное учебно-методическое обеспечение

1. Конев А.А. Основы защиты информации [Электронный ресурс]: электронный курс / А. А. Конев. - Томск : ФДО, ТУСУР, 2018. (доступ из личного кабинета студента) .

7.5. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

2. КонсультантПлюс: справочная правовая система (www.consultant.ru). Доступ из личного кабинета студента по ссылке https://study.tusur.ru/study/download/.

3. ЭБС «Юрайт»: виртуальный читальный зал учебников и учебных пособий от авторов из ведущих вузов России (https://urait.ru/). Доступ из личного кабинета студента.

Согласована на портале № 68168

4. ЭБС «Лань»: электронно-библиотечная система издательства «Лань» (https://e.lanbook.com/). Доступ из личного кабинета студента.

8. Материально-техническое и программное обеспечение дисциплины

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

Учебные аудитории для проведения занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, для самостоятельной работы студентов

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;
- LibreOffice;
- Microsoft Windows;

8.2. 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, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

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

8.3. 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 зрения** 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.

Согласована на портале № 68168

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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Правовое обеспечение информационной безопасности	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
2 Организационное обеспечение информационной безопасности	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
3 Безопасность операционных систем.	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
4 Безопасность систем баз данных.	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий

Согласована на портале № 68168

5 Безопасность вычислительных сетей.	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
6 Криптографические методы защиты информации. Технические каналы утечки информации.	ОПК-2, ОПК-3, ПКР-1	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции

Согласована на портале № 68168

2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

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

Согласована на портале № 68168

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 (ubi.fstec.ru);
   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

Согласована на портале № 68168

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,

Согласована на портале № 68168

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.

9.1.2. Перечень вопросов для зачета

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

Согласована на портале № 68168

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.

9.1.3. Примерный перечень тем и тестовых заданий на контрольные работы

Дисциплина “Защита информации”

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;

Согласована на портале № 68168

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 оперативнорозыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
    a) Конфиденциальная информация;
    b) Секретная информация;
    c) Военная тайна;
    d) Государственная тайна.

9.1.4. Темы лабораторных работ

1. Администрирование учетных записей пользователей
2. Управление параметрами операционной системы
3. Политика ограниченного использования программ

9.2. Методические рекомендации

Согласована на портале № 68168

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 осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – 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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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;

Согласована на портале № 68168

– 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.

Согласована на портале № 68168

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 13 от «18» 12 2018 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КСУП	Ю.А. Шурыгин	Согласовано, 86bee96a-108e-4833-aead-5229de651610
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Декан ФДО	И.П. Черкашина	Согласовано, 4580bdea-d7a1-4d22-bda1-21376d739cfc

ЭКСПЕРТЫ:

Доцент, каф. КСУП	Т.Е. Григорьева	Согласовано, d848614c-1d2f-4e32-b86c-1029abc0b2d5
Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc

Согласована на портале № 68168