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
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теоретические основы компьютерной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **8**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	30	30	часов
2	Практические занятия	30	30	часов
3	Всего аудиторных занятий	60	60	часов
4	Самостоятельная работа	48	48	часов
5	Всего (без экзамена)	108	108	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 8 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 18.12.2019
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 51167

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) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

и.о. зав. каф. каф. БИС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 51167

1. Цели и задачи дисциплины

1.1. Цели дисциплины

обучение студентов комплексному подходу к обеспечению информационной безопасности;

формирование у них представлений об использовании специального математического аппарата для анализа защищенности автоматизированных систем.

1.2. Задачи дисциплины

– получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;

– изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;

– изучить методологию проектирования и построения защищенных автоматизированных систем.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Теоретические основы компьютерной безопасности» (Б1.Б.03.12) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Дискретная математика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-2 способностью создавать и исследовать модели автоматизированных систем;

В результате изучения дисциплины обучающийся должен:

– **знать** Методологические и технологические основы комплексного обеспечения безопасности автоматизированных систем и их элементов; угрозы и методы нарушения безопасности автоматизированных систем

– **уметь** создавать и исследовать модели автоматизированных систем; проектировать защищённые автоматизированные системы и их элементы

– **владеть** опытом применения формальных моделей обеспечения безопасности автоматизированных систем, методами и средствами реализации защищенных автоматизированных систем

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	60	60
Лекции	30	30
Практические занятия	30	30
Самостоятельная работа (всего)	48	48
Выполнение индивидуальных заданий	10	10
Проработка лекционного материала	10	10
Подготовка к практическим занятиям, семинарам	28	28
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144

Согласована на портале № 51167

Зачетные Единицы	4.0	4.0

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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Основные положения теории защиты информации	2	2	3	7	ПК-2
2 Математическое моделирование в проектировании защищённых телекоммуникационных систем	4	4	5	13	ПК-2
3 Классификация угроз безопасности информации в телекоммуникационных системах и их элементах	2	4	7	13	ПК-2
4 Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	4	4	1	9	ПК-2
5 Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	4	6	16	ПК-2
6 Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	6	4	6	16	ПК-2
7 Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов	6	2	4	12	ПК-2
8 Защита индивидуальных заданий	0	6	16	22	ПК-2
Итого за семестр	30	30	48	108	
Итого	30	30	48	108	

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
8 семестр			
1 Основные положения теории защиты информации	Субъектно-объектное представление автоматизированной системы. Понятие доступа. Информационная безопасность автоматизированных систем.	2	ПК-2
	Итого	2	
2 Математическое	Математические модели в информацион-	4	ПК-2

Согласована на портале № 51167

моделирование в проектировании защищённых телекоммуникационных систем	ной безопасности. Применение моделей при проектировании систем безопасности.		
	Итого	4	
3 Классификация угроз безопасности информации в телекоммуникационных системах и их элементах	Угрозы конфиденциальности, целостности и доступности информации. Угроза раскрытия параметров автоматизированной системы. Классификационные признаки угроз безопасности информации.	2	ПК-2
	Итого	2	
4 Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	Матрица доступов. Классическая модель Take-Grant. Расширенная модель Take-Grant.	4	ПК-2
	Итого	4	
5 Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем	Модель Белла-ЛаПадула. Модель Биба. Модель систем военных сообщений.	6	ПК-2
	Итого	6	
6 Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	Понятие роли. Модель ролевого разграничения доступа.	6	ПК-2
	Итого	6	
7 Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов	Монитор безопасности объектов. Монитор безопасности. Изолированная программная среда.	6	ПК-2
	Итого	6	
Итого за семестр		30	

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 представлены 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								

Согласована на портале № 51167

1 Безопасность операционных систем	+	+	+	+	+	+	+	+
2 Дискретная математика	+	+	+	+	+	+	+	+

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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПК-2	+	+	+	Отчет по индивидуальному заданию, Экзамен, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Основные положения теории защиты информации	Субъектно-объектное представление автоматизированной системы.	2	ПК-2
	Итого	2	
2 Математическое моделирование в проектировании защищённых телекоммуникационных систем	Функциональные модели автоматизированных систем. Математические модели автоматизированных систем	4	ПК-2
	Итого	4	
3 Классификация угроз безопасности информации в телекоммуникационных системах и их элементах	Противодействие угрозам конфиденциальности, целостности и доступности информации в автоматизированных системах	4	ПК-2
	Итого	4	
4 Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	Работа с матрицей доступов Модель Take-Grant	4	ПК-2
	Итого	4	
5 Мандатное разграничение доступа для	Мандатное разграничение прав доступа пользователей Модель Белла-ЛаПадула	4	ПК-2
	Итого	4	

Согласована на портале № 51167

обеспечения безопасности телекоммуникационных систем			
6 Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	Ролевое разграничение прав доступа пользователей	4	ПК-2
	Итого	4	
7 Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов	Построение изолированной программной среды	2	ПК-2
	Итого	2	
8 Защита индивидуальных заданий	Защита индивидуальных заданий	6	ПК-2
	Итого	6	
Итого за семестр		30	

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
8 семестр				
1 Основные положения теории защиты информации	Подготовка к практическим занятиям, семинарам	2	ПК-2	Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
2 Математическое моделирование в проектировании защищённых телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-2	Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	5		
3 Классификация угроз безопасности информации в телекоммуникационных системах и их элементах	Подготовка к практическим занятиям, семинарам	6	ПК-2	Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	7		

Согласована на портале № 51167

4 Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем	Проработка лекционного материала	1	ПК-2	Тест, Экзамен
	Итого	1		
5 Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-2	Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
6 Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-2	Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
7 Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов	Подготовка к практическим занятиям, семинарам	2	ПК-2	Отчет по индивидуальному заданию, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
8 Защита индивидуальных заданий	Подготовка к практическим занятиям, семинарам	6	ПК-2	Отчет по индивидуальному заданию, Тест, Экзамен
	Выполнение индивидуальных заданий	10		
	Итого	16		
Итого за семестр		48		
	Подготовка и сдача экзамена	36		Экзамен
Итого		84		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
8 семестр				

Согласована на портале № 51167

Отчет по индивидуальному заданию	20	20	20	60
Тест			10	10
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	70	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. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] [Электронный ресурс]: учебное пособие для вузов. — 2-е изд., испр. и доп. — М.: Горячая линия – Телеком, 2013. — 338 с. — Режим доступа: https://e.lanbook.com/book/63235 (дата обращения: 05.06.2021).

12.2. Дополнительная литература

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: учебное пособие для студентов специальности 075500 / Р. В. Мещеряков, Г. А. Праскурин. — 2-е изд., перераб. и доп. — Томск: В-Спектр, 2007. — 343 с. (наличие в библиотеке ТУСУР - 53 экз.)

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах.— М.: Радио и связь, 2006. — 175 с. (наличие в библиотеке ТУСУР - 60 экз.)

Согласована на портале № 51167

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности [Электронный ресурс] [Электронный ресурс]: методические указания по выполнению практических работ и самостоятельной работе для студентов специальностей 10.05.02 «Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности» // Р.В. Мещеряков, Г.А. Праскурин, А.А. Шелупанов — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/praskurin_tokb_lab_srs.pdf (дата обращения: 05.06.2021).

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. http://www.iqlib.ru - электронная интернет библиотека;
2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. http://www.elibrary.ru - научная электронная библиотека;
4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. http://www.sec.ru – каталог организаций в сфере информационной безопасности
6. https://fstec.ru/ - сайт Федеральной службы по техническому и экспортному контролю

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 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.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиату-

Согласована на портале № 51167

ра/ монитор;

- Аппаратные средства аутентификации пользователя «eToken Pro»;
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;
- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap;
- системы защиты от утечки данных: Контур информационной безопасности SearchInform;
- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;
- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education.

Устройства чтения смарт-карт и радиометок: Адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– VirtualBox

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.

Согласована на портале № 51167

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. Какова роль монитора безопасности объектов и монитора безопасности субъектов в субъектно-объектной модели при проектировании защищённых автоматизированных систем?

a) Разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов;

b) Разрешает поток, принадлежащий только множеству легального доступа;

c) Активизируется при порождении субъектов;

d) Сокращает множество возможных объектов до некоторого множества фиксированной мощности.

2. К общим принципам создания и эксплуатации защищенных автоматизированных систем не относится …

a) Принцип системности;

b) Принцип непрерывности;

c) Принцип разумной достаточности;

d) Принцип минимизации стоимости.

3. К методам и механизмам обеспечения информационной безопасности безопасности автоматизированных систем непосредственного действия относится …

a) Управление сетевыми соединениями;

b) Разграничение доступа к данным;

c) Нормативно-организационная регламентация;

d) Управление сеансами.

4. К задачам аудита информационной безопасности не относится…

a) Прогноз рисков;

b) Оценка текущего уровня безопасности;

c) Разработка рекомендаций по повышению уровня безопасности;

d) Разработка новых средств защиты информации.

5. Мощность пространства паролей …

a) Прямо пропорциональна вероятности подбора пароля;

b) Зависит от срока действия пароля;

c) Прямо пропорциональна мощности алфавита пароля;

d) Влияет на длину пароля.

6. Использование защитных механизмов различной и наиболее целесообразной в конкретных условиях природы на всех этапах функционирования автоматизированной системы и ее элементов обеспечивается …

a) Принципом комплексности;

Согласована на портале № 51167

b) Принципом целенаправленности;
c) Принципом управляемости;
d) Принципом разумной достаточности.
7. К утечкам информации не относится:
a) Разглашение;
b) Несанкционированный доступ к информации;
c) Получение защищаемой информации разведками;
d) Недобросовестная конкуренция.
8. В модели целостности Кларка-Вилсона все содержащиеся в системе данные подразделяются на:
a) Субъекты и объекты;
b) Секретные и общедоступные данные;
c) Контролируемые и неконтролируемые элементы;
d) Доступные и недоступные элементы.
9. К моделям, реализующим дискреционную политику безопасности, не относится …
a) Модель Take-Grant;
b) Расширенная модель Take-Grant;
c) Модель Харисона-Руззо-Ульмана (HRU-модель);
d) Модель Белла-ЛаПадула.
10. Задача модели безопасности при проектировании защищенных автоматизированных систем – ?
a) Защита от взлома методом грубой силы;
b) Авторизация субъектов доступа;
c) Обеспечение заданного уровня конфиденциальности;
d) Формальное доказательство соблюдения политики безопасности.
11. Произвольная операция над объектом O, реализуемая в субъекте S и зависящая от
a) Потоком информации;
b) Доступом;
c) Политикой безопасности;
d) Активностью субъекта.
12. Для добавления нового объекта в систему в модели безопасности Take-Grant используется команда:
a) Grant;
b) Append;
c) Create;
d) Make.
13. Модель, в которой безопасность автоматизированной системы рассматривается с точки зрения возможности получения субъектом определённых прав к некоторому объекту – это …
a) Модель целостности;
b) Субъект-объектная модель;
c) Дискреционная модель;
d) Модель распределения прав доступа.
14. Для какой из моделей безопасности характерны правила post, spy, find и pass?
a) Модель Take-Grant;
b) Расширенная модель Take-Grant;
c) Модель Харисона-Руззо-Ульмана (HRU-модель);
d) Модель Белла-ЛаПадула.
15. Модель Биба часто называют инверсией модели Белла-ЛаПадулла, потому что …
a) Модели описывают различные политики безопасности;
b) Данные модели противоречат друг другу;
c) Основные правила моделей являются инверсными, но описывают разные уровни безопасности;
d) Исследователь не может применить данные модели одновременно.

Согласована на портале № 51167

16. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации в автоматизированной системе называется …
a) Компьютерной безопасностью;
b) Угрозой безопасности;
c) Анализом угроз;
d) Атакой на информационную систему.
17. Под оцениванием угроз понимается …
a) Определение множества угроз, характерных, актуальных для конкретной компьютерной системы;
b) Присвоение угрозам уникальных идентификаторов и описания;
c) Формирование оценок угроз с точки зрения потерь, ущерба, возможных от их реализации
d) Составление требований к обеспечению информационной безопасности компьютерной системы.
18. По степени преднамеренности проявления угрозы делятся на …
a) Преднамеренного действия и случайного действия;
b) Естественной природы и искусственной природы;
c) Субъективного проявления и объективного проявления;
d) Пассивного действия и активного действия.
19. Основным (-и) фактором (-ами) оценки угрозы являются:
a) Возможность реализации угрозы и оценка возможного ущерба;
b) Оценка ценности объекта и стоимость средств защиты;
c) Идентификация воздействия угрозы на объект защиты;
d) Субъективная оценка возможности реализации угрозы.
20. Угроза применения «троянских» программ актуальна для систем с …
a) Мандатной политикой безопасности;
b) Контролем порождения субъектов и объектов;
c) Дискреционной политикой безопасности;
d) Внедренным контролем целостности.
21. Активные угрозы …
a) Проявляются после разрешения доступа к ресурсам;
b) Проявляются независимо от активности компьютерной системы;
c) Вызваны воздействиями на компьютерную систему объективных физических процессов или стихийных природных явлений, не зависящих от человека;
d) При воздействии вносят изменения в структуру и содержание компьютерной системы.
22. Существование информации в неизменном виде по отношению к некоторому фиксированному ее состоянию обозначается свойством …
a) Конфиденциальности информации;
b) Целостности информации;
c) Доступности информации;
d) Актуальности информации.
23. Недостаток системы, используя который можно нарушить её безопасность, называется
a) Угроза;
b) Ошибка;
c) Недекларированные возможности;
d) Уязвимость.
24. 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.
25. Какая из мер не способна влиять на уровень безопасности парольной системы защиты?
a) Проверка и отбраковка пароля по словарю;

Согласована на портале № 51167

b) Введение двухфакторной аутентификации;
c) Ограничение числа попыток ввода пароля;
d) Установление минимального срока действия пароля.
26. Территория вокруг помещений автоматизированной системы, которая непрерывно контролируется персоналом или средствами компьютерной системы называется …
a) Внешняя неконтролируемая зона;
b) Зона контролируемой территории;
c) Зона помещений компьютерной системы;
d) зона ресурсов компьютерной системы.
27. Для какой политики безопасности характерно использование грифов секретности?
a) Для мандатной политики безопасности;
b) Для дискреционной политики безопасности;
c) И для мандатной, и для дискреционной политик безопасности;
d) Ни для одной из политик безопасности.
28. Процедура распознавания субъекта по его идентификатору называется …
a) Идентфикацией;
b) Аутентификацией;
c) Авторизацией;
d) Регистрацией.
29. Принцип непрерывности в эксплуатации защищенных автоматизированных систем заключается в том, что …
a) Защитные механизмы системы должны функционировать в любых ситуациях, в том числе и внештатных;
b) Меры защиты должны быть направлены против перечня угроз, характерных для конкретной системы в конкретных условиях ее эксплуатации;
c) Подсистема безопасности системы должна строиться как система управления;
d) Необходимо использовать защитные механизмы различной и наиболее целесообразной в конкретных условиях природы.
30. Совокупность объектов, к которым разрешен доступ конкретному субъекту называется …
a) Политикой безопасности;
b) Доменом безопасности;
c) Принципом управляемости;
d) Субъект-объектной моделью.
31. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...
a) Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
b) Реализацию права на доступ к информации;
c) Разработку методов и усовершенствование средств информационной безопасности;
d) Выявление нарушителей и привлечение их к ответственности.
32. К мерам защиты информации в информационной системе не относится:
a) Идентификация и аутентификация субъектов доступа и объектов доступа;
b) Управление доступом субъектов доступа к объектам доступа;
c) Повышение эффективности работы вычислительной техники системы;
d) Защита информационной системы, ее средств и систем связи и передачи данных.
33. Меры защиты информации, выбираемые для реализации в автоматизированной системе, должны обеспечивать…
a) Блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации;
b) Формирование модели угроз и модели нарушителя информационной системы;

Согласована на портале № 51167

c) Анализ рисков информационной безопасности информационной системы;
d) Минимизацию затрат для поддержания уровня безопасности.
34. К методам повышения достоверности входных данных относится:
a) Замена процесса ввода значения процессом выбора значения из предлагаемого множества;
b) Отказ от использования данных;
c) Проведение комплекса регламентных работ;
d) Многократный ввод данных и сличение введенных значений.
35. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
a) Несанкционированного управления удаленным компьютером;
b) Внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
c) Перехвата или подмены данных на путях транспортировки;
d) Вмешательства в личную жизнь.
36. Утечка информации – это …
a) Несанкционированный процесс переноса информации от источника к злоумышленнику;
b) Процесс раскрытия секретной информации;
c) Процесс уничтожения информации;
d) Непреднамеренная утрата носителя информации.
37. Концепция системы защиты от информационного оружия не должна включать…
a) Механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры;
b) Признаки, сигнализирующие о возможном нападении;
c) Средства нанесения контратаки;
d) Процедуры оценки атаки против национальной инфраструктуры в целом и отдельных пользователей.
38. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на функционирование системы:
a) Активная;
b) Пассивная;
c) Непреднамеренная;
d) Естественная.

14.1.2. Экзаменационные вопросы

1. Что является важнейшими особенностями информации?
2. Что входит в автоматизированные системы обработки информации?
3. Дайте определение информационной безопасности автоматизированной системы.
4. Дайте определение субъекта доступа.
5. Сформулируйте основную теорему безопасности информации в АС.
6. На каком уровне иерархии модели OSI/ISO нельзя использовать модели безопасности информации?
7. На основе чего строится ценность информации в аддитивной модели?
8. Как определяется ценность информации в модель анализа риска?
9. На чем основывается порядковая шкала ценностей?
10. В каких случаях применяется модель решетки ценностей?
11. MLS-решетка.
12. Дайте определение конфиденциальности информации.
13. Дайте определение целостности информации.
14. Дайте определение доступности информации.
15. На какие уровни разделяется доступ к информации применительно к автоматизированным системам?
16. Перечислите основные принципы обеспечения информационной безопасности в АС.
17. Чем, согласно основным принципам, должна обеспечиваться информационная безопасность в АС?

Согласована на портале № 51167

18. Чем, согласно основным принципам, является оценка эффективности обеспечения информационной безопасности в АС?
19. Приведите примеры несанкционированного копирования носителей информации.
20. Приведите примеры не информационных каналов утечки информации.
21. Какого доступа к данным машинных носителей информации не существует?
22. Дайте определение идентификации и аутентификации.
23. На чем основаны парольные системы защиты?
24. Приведите примеры угроз нарушения конфиденциальности.
25. Приведите примеры угроз нарушения целостности.
26. Приведите примеры угроз отказа служб.
27. Зачем необходим принцип системности.
28. Для чего в системе защиты информации используется принцип комплексности?
29. Приведите пример идентификации.
30. Приведите пример аутентификации.
31. Как называют процедуру аутентификации, если в ней (помимо основных сторон) участвует сервер аутентификации (арбитр)?
32. С помощью какого вредоносного программного обеспечения может быть создана атака на систему аутентификации?
33. Дайте определение пароля пользователя.
34. Каких атак на пароли не существует?
35. Перечислите компоненты парольной системы защиты.
36. Какие элементы затрудняют появление угроз парольным системам?
37. Какова зависимость между мощностью алфавита паролей и скоростью перебора паролей?
38. Какова зависимость параметров парольной системы защиты от длины пароля?
39. Как расшифровывается аббревиатура СКЗИ?
40. Какие существуют системы шифрования?
41. Для чего необходимо шифрование?
42. Для чего необходима электронно-цифровая подпись?
43. Дайте определение стеганографии.
44. Приведите примеры стеганографических приемов защиты информации.
45. В чем заключается сертификация средств СКЗИ?
46. Какие стандарты защиты информации на данный момент действуют в Российской Федерации?
47. В чем заключается требование корректности транзакций?
48. В чем заключается принцип минимизации привилегий?
49. Что подразумевает разграничение функциональных обязанностей в АС?
50. Для чего необходим аудит произошедших событий в АС?
51. В каких случаях требуется обеспечение непрерывной работы защитных механизмов АС?
52. В чем заключается требование простоты использования защитных механизмов?
53. Каково назначение модели Кларка – Вилсона?
54. Перечислите правила модели Кларка-Вилсона.
55. Для чего используются барьерные адреса? Варианты назначения барьерных адресов.
56. Позволяет ли использование сегментов оперативной памяти защитить код программ друг от друга?
57. Позволяет ли использование сегментов оперативной памяти обеспечить доступ нескольких программ к одному участку оперативной памяти?
58. Чем обеспечивается отказоустойчивость программного обеспечения (ПО) АС?
59. Дайте определение политики безопасности.
60. Между какими элементами системы существуют потоки информации?
61. При каком условии возможно порождение субъекта?
62. Какое действие называется доступом субъекта S к объекту O?
63. Какой из специальных субъектов системы является механизмом реализации заданной политики безопасности системы?

Согласована на портале № 51167

64. Перечислите типы политик безопасности.
65. Какой тип политик безопасности может противостоять атакам типа «Троянский конь» ?
66. Какими свойствами определяется дискреционное управление доступом?
67. Какими свойствами определяется мандатное управление доступом?
68. Как определяется корректность субъектов друг относительно друга?
69. Каково назначение Монитора безопасности субъектов и Монитора безопасности объектов?
70. Какие специальные субъекты обязательно входят в состав Изолированной программной среды?
71. Для чего используются модели политик безопасности?
72. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих дискреционное управление доступом?
73. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих мандатное управление доступом?
74. В чем состоит основная задача дискреционных политик безопасности?
75. В чем состоит основная задача мандатных политик безопасности?
76. Какие операции преобразования матрицы доступов используются в модели HRU?
77. Возможна ли проверка безопасности произвольной системы, представленной моделью матрицы доступов HRU?
78. Какая система в модели HRU называется монооперационной?
79. Что является основой политики MLS?
80. При каком условии согласно политике MLS разрешен доступ субъекта S к объекту O?
81. При помощи чего в модели Take-Grant описывается функционирование системы?
82. Какие команды преобразования графа доступов используются в модели Take-Grant?
83. В каком случае возможно похищение прав доступа согласно модели Take-Grant?
84. Каково назначение расширенной модели Take-Grant?
85. Можно ли применять правила де-юре к мнимым дугам в расширенной модели TakeGrant?
86. С помощью каких свойств определяется безопасность системы в модели БеллаЛападула?
87. Что является основной задачей стандартов информационной безопасности?
88. Укажите назначение профиля защиты.
89. Перечислите виды оценок согласно РД «Общие критерии».

14.1.3. Темы индивидуальных заданий

Парольные системы защиты.
Целостность данных. Модель Кларка-Вилсона.
Стеганография.
Криптография. Шифрование.
Криптография. Электронно-цифровая подпись и хеширование.
Субъект-объектная модель. Изолированная программная среда.
Работа с матрицей доступов. Домены безопасности.
Модель Take-Grant.
Нарушение дискреционной политики безопасности программой «Троянский конь».
Мандатные политики безопасности.
Стандарты в области защиты информации в компьютерных системах.

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

Согласована на портале № 51167

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.

Согласована на портале № 51167