МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	28	28	часов
4	Всего аудиторных занятий	74	74	часов
5	Из них в интерактивной форме	20	20	часов
6	Самостоятельная работа	70	70	часов
7	Всего (без экзамена)	144	144	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е

Экзамен: 7 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «12» 2 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 2016-12-01 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Ассистент каф. БИС _____ Рахманенко И. А.

Заведующий обеспечивающей каф.
КИБЭВС _____ Шелупанов А. А.

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

Декан ФБ _____ Давыдова Е. М.

Заведующий выпускающей каф.
КИБЭВС _____ Шелупанов А. А.

Эксперты:

доцент каф. КИБЭВС _____ Конев А. А.

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, а также навыков и умения в применении знаний для конкретных условий.

Развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

1.2. Задачи дисциплины

- Дать знания по концепции обеспечения информационной безопасности компьютерных систем;
- программно-аппаратным средствам, реализующим отдельные функциональные требования по защите;
- методам и средствам хранения ключевой информации;
- методам и средствам ограничения доступа к компонентам вычислительных систем;
- защите программ от изменения и контролю целостности;
- задачам и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» (Б1.Б.6) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность операционных систем, Безопасность систем баз данных, Дискретная математика, Моделирование автоматизированных информационных систем.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

В результате изучения дисциплины студент должен:

- **знать** программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах управления базами данных, компьютерных сетях; основные информационные технологии, используемые в автоматизированных системах.
- **уметь** проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
- **владеть** профессиональной терминологией в области информационной безопасности; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками анализа основных узлов и устройств современных автоматизированных систем.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	74	74
Лекции	28	28

Практические занятия	18	18
Лабораторные работы	28	28
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	70	70
Выполнение домашних заданий	32	32
Оформление отчетов по лабораторным работам	19	19
Проработка лекционного материала	10	10
Подготовка к практическим занятиям, семинарам	9	9
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	180	180
Зачетные Единицы	5.0	5.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Программно-аппаратные средства обеспечения информационной безопасности.	8	6	10	21	45	ПК-1
2 Методы и средства защиты программного обеспечения.	6	6	6	18	36	ПК-1
3 Построение изолированной программной среды.	6	2	8	19	35	ПК-1
4 Обеспечение информационной безопасности компьютерных сетей.	4	2	4	9	19	ПК-1
5 Стандарты информационной безопасности.	4	2	0	3	9	ПК-1
Итого за семестр	28	18	28	70	144	
Итого	28	18	28	70	144	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Программно-аппаратные средства обеспечения информационной безопасности.	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем	8	ПК-1
	Итого	8	
2 Методы и средства защиты программного обеспечения.	Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель политики безопасности на основе дискретных компонент АДЕПТ-50. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности	6	ПК-1
	Итого	6	
3 Построение изолированной программной среды.	Модель компьютерной системы. Понятие монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели	6	ПК-1

	безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.		
	Итого	6	
4 Обеспечение информационной безопасности компьютерных сетей.	Программно-аппаратные средства защиты информации в сетях передачи данных. Межсетевые экраны. Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов	4	ПК-1
	Итого	4	
5 Стандарты информационной безопасности.	Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий	4	ПК-1
	Итого	4	
Итого за семестр		28	

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
Предшествующие дисциплины					
1 Безопасность операционных систем	+	+	+		
2 Безопасность систем баз данных		+	+		+
3 Дискретная математика			+		
4 Моделирование автоматизированных	+		+		

информационных систем					
Последующие дисциплины					
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий				Формы контроля
	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПК-1	+	+	+	+	Домашнее задание, Экзамен, Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

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

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

Методы	Интерактивные практические занятия	Интерактивные лабораторные занятия	Интерактивные лекции	Всего
7 семестр				
Презентации с использованием слайдов с обсуждением			8	8
Решение ситуационных задач	4	4		8
Case-study (метод конкретных ситуаций)		4		4
Итого за семестр:	4	8	8	20
Итого	4	8	8	20

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Программно-аппаратные средства обеспечения информационной безопасности.	Разработка защищенного ПО с применением аппаратных ключей eToken	10	ПК-1
	Итого	10	
2 Методы и средства защиты программного обеспечения.	Программно-аппаратное устройство защиты информации "Аккорд"Привязка программного к аппаратному окружению	6	ПК-1
	Итого	6	
3 Построение изолированной программной среды.	Программно-аппаратное устройство защиты информации SecretNetЗащита программ от изменения и разрушающих программных воздействийЗащита программ от изменения и контроль целостности	8	ПК-1
	Итого	8	
4 Обеспечение информационной безопасности компьютерных сетей.	Защита информации в компьютерной сетях передачи данных	4	ПК-1
	Итого	4	
Итого за семестр		28	

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
7 семестр			
1 Программно-аппаратные средства обеспечения информационной безопасности.	Программно-аппаратные средства обеспечения информационной безопасности.	6	ПК-1
	Итого	6	
2 Методы и средства защиты программного обеспечения.	Методы и средства защиты программного обеспечения.	6	ПК-1
	Итого	6	
3 Построение изолированной программной среды.	Построение изолированной программной среды.	2	ПК-1

	Итого	2	
4 Обеспечение информационной безопасности компьютерных сетей.	Обеспечение информационной безопасности компьютерных сетей.	2	ПК-1
	Итого	2	
5 Стандарты информационной безопасности.	Стандарты информационной безопасности.	2	ПК-1
	Итого	2	
Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Программно-аппаратные средства обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	3		
	Оформление отчетов по лабораторным работам	6		
	Выполнение домашних заданий	10		
	Итого	21		
2 Методы и средства защиты программного обеспечения.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	3		
	Оформление отчетов по лабораторным работам	3		
	Выполнение домашних заданий	10		
	Итого	18		
3 Построение изолированной программной среды.	Подготовка к практическим занятиям, семинарам	1	ПК-1	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	6		
	Выполнение домашних заданий	6		

	Выполнение домашних заданий	6		
	Итого	19		
4 Обеспечение информационной безопасности компьютерных сетей.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	3		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
5 Стандарты информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		70		
	Подготовка и сдача экзамена	36		Экзамен
Итого		106		

9.1. Темы домашних заданий

1. Состав комплекса «Аккорд»
2. Принцип работы комплекса «Аккорд»
3. Механизм замкнутой программной среды Secret Net

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
7 семестр				
Домашнее задание	10	5	5	20
Защита отчета		10	10	20
Конспект самоподготовки			5	5
Опрос на занятиях		5		5
Отчет по лабораторной работе		10	10	20
Итого максимум за период	10	30	30	70

Экзамен				30
Нарастающим итогом	10	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. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В-Спектр, 2007 - . Раздел 1. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 143[1] с. : ил. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.)

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев ; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В-Спектр, 2007 - . Раздел 2. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 118[2] с. : ил. - Библиогр.: с. 37. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.)

12.2. Дополнительная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). (наличие в библиотеке ТУСУР - 20 экз.)

2. Защита информации с использованием смарт-карт и электронных брелоков / Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 30 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Рахманенко И.А. Методические указания по выполнению практических работ по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_pract.pdf
2. Рахманенко И.А. Лабораторный практикум по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_lab.pdf
3. Рахманенко И.А. Методические указания по самостоятельной и индивидуальной работе студентов по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_sam.pdf

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Система подготовки документов Open Office; Система для использования виртуальных машин VMware Player; Google; Wikipedia.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 404. Состав оборудования: Учебная мебель; TraceBoard TS-408L - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже Celeron 2.4 GHz/256Mb/40Gb с широкополосным доступом в Internet, – 4 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская

вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Электронные ключи eToken. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для проведения самостоятельной работы используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями	Собеседование по вопросам к зачету,	Преимущественно устная проверка

зрения	опрос по терминам	(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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Программно-аппаратные средства защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**

Учебный план набора 2016 года

Разработчики:

- Ассистент каф. БИС Рахманенко И. А.

Экзамен: 7 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Должен знать программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах управления базами данных, компьютерных сетях; основные информационные технологии, используемые в автоматизированных системах.; Должен уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.; Должен владеть профессиональной терминологией в области информационной безопасности; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками анализа основных узлов и устройств современных автоматизированных систем.;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к

			обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-1

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Знать как выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Уметь выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Владеть способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Домашнее задание; • Опрос на занятиях; • Конспект самоподготовки; • Экзамен;	• Отчет по лабораторной работе; • Домашнее задание; • Опрос на занятиях; • Конспект самоподготовки; • Экзамен;	• Отчет по лабораторной работе; • Домашнее задание; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть

Отлично (высокий уровень)	• Знать в полном объеме как выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Уметь в полном объеме выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Владеть в полном объеме способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
Хорошо (базовый уровень)	• Знать на продвинутом уровне как выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Уметь на продвинутом уровне выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Владеть на продвинутом уровне способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
Удовлетворительно (пороговый уровень)	• Знать на базовом уровне как выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Уметь на базовом уровне выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	• Владеть на базовом уровне способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

3 Типовые контрольные задания

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

3.1 Вопросы на самоподготовку

– 1. Подсистема безопасности операционной системы Windows 8 2. Аудит событий безопасности в операционной системе Windows 8 3. Поставщик служб криптографии ОС Windows 2012 4. Поставщик служб криптографии КриптоПро и его интеграции в ОС Windows 2012 5. Электронные платежные системы – принципы функционирования и защиты информации 6. Управление криптографическими ключами. Генерация ключей 7. Управление криптографическими ключами. Хранение ключей 8. Управление криптографическими ключами. Распределение ключей 9. Методы защиты программ от изучения 10. Методы и средства исследования программ 11. Методы и средства ограничения доступа к компонентам ЭВМ 12. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям 13. Защита от

разрушающих программных воздействий 14. Защита от изменения и контроль целостности 15. Классификация компьютерных вирусов 16. Проблемы обеспечения безопасности при удалённом доступе 17. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях 18. Понятие межсетевых экранов, их классификация

3.2 Темы домашних заданий

– Архитектура ПАК “Соболь”. Функциональные возможности ПАК “Соболь”. Установка ПАК “Соболь”. Состав ПАК “Аккорд АМДЗ”. Функции ПАК “Аккорд АМДЗ”. КСЗИ “Панцирь-К”. Серверная и клиентские части. КСЗИ “Панцирь-К”. Идентификация и аутентификация пользовате-лей. КСЗИ “Панцирь-К”. Контроль и разграничение доступа. КСЗИ “Панцирь-К”. Аудит. КСЗИ “Панцирь-К”. Дополнительные возможности.

3.3 Темы опросов на занятиях

– Угрозы безопасности компьютерных систем Противодействие угрозам безопасности Защита компьютерной системы от взлома Модель КС Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности Реализация механизмов безопасности на аппаратном уровне Безопасность компьютерной сети Защита от анализаторов протоколов Технология защиты информации на основе смарт-карт Состав комплекса «Аккорд» Принцип работы комплекса «Аккорд» Механизм замкнутой программной среды Secret Net

3.4 Экзаменационные вопросы

– Методы обеспечения информационной безопасности автоматизированных систем (основные понятия, угрозы). Методы обеспечения информационной безопасности автоматизированных систем (методы взлома, защита от взлома). Методы обеспечения информационной безопасности автоматизированных систем (защита от программных закладок). Политика безопасности. Модель КС. Замкнутая программная среда. Формирование и поддержка изолированной программной среды. Реализация ИПС с использованием механизма расширения BIOS UEFI. Принципы работы Персональное средство аутентификации eToken eToken API Безопасное взаимодействие в КС. Процедуры идентификации и аутентификации. Аутентификация до загрузки ОС Контроль и управление доступом. Диспетчер доступа. Назначение, функции, принцип работы ПАК «Аккорд». Назначение, функции, принцип работы ПАК “Соболь” Персональные идентификаторы. Виды, назначение, функции. Назначение, функции, принцип работы ключей защиты. Известные модели. Виды защиты ПО с помощью электронных ключей. Методы взлома. КСЗИ Панцирь-К. Серверная и клиентские части, идентификация и аутентификация пользователей КСЗИ Панцирь-К. Контроль и разграничение доступа КСЗИ Панцирь-К. Аудит и дополнительные возможности Управление криптографическими ключами Концепция иерархии ключей, генерация ключей. Аппаратные модули безопасности

3.5 Темы лабораторных работ

– Разработка защищенного ПО с применением аппаратных ключей eToken

– Программно-аппаратное устройство защиты информации "Аккорд" Привязка программного к аппаратному окружению

– Программно-аппаратное устройство защиты информации SecretNet Защита программ от изменения и разрушающих программных воздействий Защита программ от изменения и контроль целостности

– Защита информации в компьютерной сетях передачи данных

4 Методические материалы

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

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Программно-аппаратные средства обеспечения информационной безопасности :

учебное пособие: В 2 разделах / А. П. Зайцев; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В-Спектр, 2007 - . Раздел 1. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 143[1] с. : ил. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.)

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев ; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В-Спектр, 2007 - . Раздел 2. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 118[2] с. : ил. - Библиогр.: с. 37. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.)

4.2. Дополнительная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). (наличие в библиотеке ТУСУР - 20 экз.)

2. Защита информации с использованием смарт-карт и электронных брелоков / Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 30 экз.)

4.3. Обязательные учебно-методические пособия

1. Рахманенко И.А. Методические указания по выполнению практических работ по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_pract.pdf

2. Рахманенко И.А. Лабораторный практикум по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_lab.pdf

3. Рахманенко И.А. Методические указания по самостоятельной и индивидуальной работе студентов по дисциплине Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_sam.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Система подготовки документов Open Office; Система для использования виртуальных машин VMware Player; Google; Wikipedia.