МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **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 2014 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	34	34	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 7 семестр

Томск 2018

Согласована на портале № 28673

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры БИС «___» _____ 20__ года, протокол №_____.

Разработчики:

Доцент каф. БИС _____ И. А. Рахманенко

Доцент каф. КИБЭВС _____ К. С. Сарин

Заведующий обеспечивающей каф. БИС _____ Р. В. Мещеряков

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

доцент каф. КИБЭВС _____ А. А. Конев

доцент каф. БИС _____ О. О. Евсютин

Согласована на портале № 28673

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 умений по применению программно-аппаратных средств защиты информации в конкретных условиях.

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;

– методам защиты от вредоносных программ;

– 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: Безопасность операционных систем, Дискретная математика, Моделирование автоматизированных информационных систем, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Прикладная криптография, Управление средствами защиты информации.

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;

– ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации;

В результате изучения дисциплины обучающийся должен:

– **знать** программно-аппаратные средства обеспечения информационной безопасности в типовых автоматизированных системах; особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; типовые средства, методы и протоколы идентификации, аутентификации и авторизации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

– **уметь** Проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации.

– **владеть** Навыками разработки архитектуры системы защиты информации автоматизированной системы; навыками противодействия вредоносному программному обеспечению; навыками разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.

Согласована на портале № 28673

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
		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)	34	34
Оформление отчетов по лабораторным работам	16	16
Проработка лекционного материала	8	8
Подготовка к практическим занятиям, семинарам	10	10
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
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	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	8	6	0	4	18	ПК-1, ПК-12
2 Программно-аппаратные средства обеспечения информационной безопасности.	16	8	28	26	78	ПК-1, ПК-12
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	4	4	0	4	12	ПК-1, ПК-12
Итого за семестр	28	18	28	34	108	
Итого	28	18	28	34	108	

Согласована на портале № 28673

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 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. Обеспечение гарантий выполнения политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	8	ПК-1
	Итого	8	
2 Программно-аппаратные средства обеспечения информационной безопасности.	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности.	16	ПК-1
	Итого	16	
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	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. Показате-	4	ПК-1

Согласована на портале № 28673

	ли защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий		
	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
Предшествующие дисциплины			
1 Безопасность операционных систем	+	+	
2 Дискретная математика	+		
3 Моделирование автоматизированных информационных систем	+	+	
4 Организационное и правовое обеспечение информационной безопасности			+
5 Основы информационной безопасности	+		+
6 Прикладная криптография		+	
7 Управление средствами защиты информации		+	
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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-1	+	+	+	+	Экзамен, Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест

Согласована на портале № 28673

ПК-12		+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
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			
2 Программно-аппаратные средства обеспечения информационной безопасности.	Разработка защищенного ПО с применением аппаратных ключей eToken	16	ПК-1, ПК-12
	Программно-аппаратное средство защиты информации от несанкционированного доступа.Защита программ от изменения и контроль целостности.	8	
	Защита программ от разрушающих программных воздействий и защита автоматизированной системы от вредоносного программного обеспечения.	4	
	Итого	28	
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

Согласована на портале № 28673

7 семестр			
1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Разработка архитектуры системы защиты информации автоматизированной системы с применением программно-аппаратных средств защиты информации. Построение моделей защищенной автоматизированной системы. Изучение методов идентификации и аутентификации с применением программно-аппаратных средств защиты информации.	6	ПК-1, ПК-12
	Итого	6	
2 Программно-аппаратные средства обеспечения информационной безопасности.	Изучение современных программно-аппаратных средств обеспечения информационной безопасности. Назначение, функции, область применения программно-аппаратных средств защиты информации. Изучение и сравнение особенностей и аналогов программно-аппаратных средств обеспечения информационной безопасности различных категорий.	8	ПК-1, ПК-12
	Итого	8	
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	Изучение нормативной документации, в том числе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации. Поиск программно-аппаратных средств защиты информации, соответствующих требованиям руководящих документов.	4	ПК-1, ПК-12
	Итого	4	
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 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-1, ПК-12	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
2 Программно-аппаратные средства обеспечения информационной	Подготовка к практическим занятиям, семинарам	6	ПК-1, ПК-12	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Проработка лекционного	4		

Согласована на портале № 28673

безопасности.	материала			
	Оформление отчетов по лабораторным работам	16		
	Итого	26		
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	Подготовка к практическим занятиям, семинарам	2	ПК-1, ПК-12	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
Итого за семестр		34		
	Подготовка и сдача экзамена	36		Экзамен
Итого		70		

10. Курсовая работа (проект)

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
7 семестр				
Защита отчета		10	10	20
Конспект самоподготовки			5	5
Опрос на занятиях		5	10	15
Отчет по лабораторной работе		10	10	20
Тест			10	10
Итого максимум за период		25	45	70
Экзамен				30
Нарастающим итогом	0	25	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

Согласована на портале № 28673

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-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-004-7 [Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/489084, дата обращения: 04.06.2018.

2. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6 [Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/923168, дата обращения: 04.06.2018.

12.2. Дополнительная литература

1. 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 - 29 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 1. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 143[1] с. : ил. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.)

3. 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.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Методические указания к практическим занятиям по дисциплине "Программно-аппаратные средства обеспечения информационной безопасности" / Рахманенко И.А. - 2017. - 10 с.: [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_pract.pdf, дата обращения: 04.06.2018.

2. Лабораторный практикум по дисциплине “Программно-аппаратные средства обеспече-

ния информационной безопасности" / Рахманенко И.А. - 2016. - 37 с.: [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_lab.pdf, дата обращения: 04.06.2018.

3. Методические указания для выполнения самостоятельной и индивидуальной работы по дисциплине "Программно-аппаратные средства обеспечения информационной безопасности" / Рахманенко И.А. - 2017. - 6 с.: [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/pasoib_sam.pdf, дата обращения: 04.06.2018.

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. Государственный реестр сертифицированных средств защиты информации: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

2. Федеральная служба по техническому и экспортному контролю https://fstec.ru/

3. Информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

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:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);
- Комплект специализированной учебной мебели;
- 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;

Согласована на портале № 28673

- Рабочее место преподавателя.

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;

Программное обеспечение:

- Антивирусный программный комплекс: Kaspersky endpoint security ;
- Microsoft Windows 7 Pro;
- VirtualBox;
- Криптографическое средство защиты информации КриптоПро CSP;
- Аппаратно-программные средства управления доступом к данным шифрования: ПО ViPNet Administrator 4.x, ПО ViPNet Coordinator for Windows 4.x, ПО ViPNet Coordinator for Linux 4.x, ПО ViPNet Client for Windows 4.x, ПО ViPNet Crypto Service 4.x, КриптоПро CSP, DallasLock;
- Visual Studio.

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

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:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);
- Комплект специализированной учебной мебели;
- 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;
- Рабочее место преподавателя.

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;

Согласована на портале № 28673

- 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;

Программное обеспечение:

– Антивирусный программный комплекс: Kaspersky endpoint security ;
– Microsoft Windows 7 Pro;
– VirtualBox;
– Криптографическое средство защиты информации КриптоПро CSP;
– Аппаратно-программные средства управления доступом к данным шифрования: ПО ViPNet Administrator 4.x, ПО ViPNet Coordinator for Windows 4.x, ПО ViPNet Coordinator for Linux 4.x, ПО ViPNet Client for Windows 4.x, ПО ViPNet Crypto Service 4.x, КриптоПро CSP, DallasLock;
– Visual Studio.

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

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

Перечень программного обеспечения:

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

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

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

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся

Согласована на портале № 28673

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. Уберите лишнее. Применение аппаратных модулей безопасности (HSM) возможно в таких областях, как:

a) PKI, центр сертификации

b) Банковские операции

c) Экспорт криптографических ключей

d) Установление SSL соединений

2. Какая из функций не относится к аппаратным модулям безопасности (HSM):

a) Безопасная генерация ключей шифрования

b) Безопасное хранение и управление ключами

c) Работа с эллиптическими кривыми

d) Шифрование и расшифровывание конфиденциальной информации

3. Выберите верный вариант ответа. Ключи шифрования ключей (КК), используемые для пересылки ключей между двумя узлами сети, называются:

a) Ключами для шифрования МК (мастер-ключа)

b) Рабочие или сеансовые КК

c) Ключами обмена между узлами сети (cross-domain keys)

d) Ключами аутентификации сообщений

4. К особенностям программно-аппаратного комплекса MKTrusT не относится:

a) Позволяет работать в одном из двух режимов – защищенном (например, работа с ДБО или иными критичными к защищенности сервисами) и незащищенном, без ограничения возможностей

b) Защищенная ОС – Linux собственной сборки, незащищенная ОС – Android

c) В стандартной комлектации MKTrusT присутствует IP-телефон, построенный на «гарвардской» архитектуре

d) MKTrusT требует для работы только телевизор (монитор или проектор) через HDMI порт, питание от USB порта (не менее 1 Ампер), сеть – WiFi

5. Выберите верный вариант ответа. Как осуществляется выбор одного из двух режимов на выбор – защищенного или обычного – в программно-аппаратном комплексе MKTrusT:

a) Используется выбор режима в процессе загрузки компьютера

b) Используется дополнительное устройство, содержащее операционную систему для соответствующего режима работы MKTrusT

c) Используется физический переключатель

d) Используется специальное ПО, реализующее подобие «виртуальной машины»

6. Вставьте пропущенное выражение. ... – период работы компьютера, в рамках которого обеспечивается доверенная загрузка ОС, организуется защищённое сетевое соединение и поддерживаются достаточные условия для работы СКЗИ:

a) Информационно-поисковая система (ИПС)

Согласована на портале № 28673

b) Безопасный режим (БР)

c) Доверенный сеанс связи (ДСС)

d) Автоматизированный рабочий режим (АРР)

7. Что не относится к сложностям обеспечения безопасности удалённого доступа к информационным ресурсам?

a) Сложность контроля выполнения требований политики ИБ на удалённых АРМ пользователей

b) Необходимость использования сертифицированных ОС, СЗИ НСД и СКЗИ для шифрованием и работы с ЭЦП

c) Необходимость проведения аттестационных, адаптационных и инспекционных действий для допуска пользователей к АРМ

d) Ограничение функционала сертифицированных ОС и прикладного ПО (в т.ч. сложность процедуры обновлений)

8. Какие из функций не относятся к возможностям КСЗИ «Панцирь-К»

a) Идентификация и аутентификация: Console, flash, eToken USB, …

b) Разграничение и аудит действий пользователей и приложений, контроль целостности

c) Временное гарантированное удаление информации с возможностью восстановления через встроенные механизмы

d) Шифрование: 3DES, AES, DES, ГОСТ 28147-89

9. Что не относится к основным принципам разграничения доступа к файловой системе в КСЗИ «Панцирь-К»?

a) Существует две политики контроля доступа к ресурсам – разрешительная и запретительная

b) Права доступа назначаются субъектам, а не присваиваются объектам в качестве их атрибутов

c) Администратор имеет такие же права на назначение (изменение) права доступа субъекта к объекту, как и “Владелец”

d) Для любого субъекта доступа может быть реализована собственная разграничительная политика

10. Выберите верный вариант ответа. К механизмам контроля целостности КСЗИ «Панцирь-К» относится:

a) Контроль целостности каталогов и файлов данных (синхронный и асинхронный)

b) Контроль целостности исполняемых файлов (программ перед запуском)

c) Все перечисленное

d) Контроль целостности файлов КСЗИ

11. Какое утверждение не относится к одному из вариантов обхода системы защиты ПО с помощью ключей защиты злоумышленником:

a) Перехват, протоколирование и анализ обращений к ключу защиты с последующей эмуляцией ответов

b) Внесение изменений в программный модуль (взлом)

c) Создание вредоносной программы, временно блокирующей запросы к ключу защиты

d) Эмулирование наличия ключа путем перехвата вызовов библиотеки API для обмена с ключом

12. Какие утверждения не относятся к защите ПО с помощью API функций ключей защиты?

a) Самостоятельная разработка защиты ПО

b) Интегрирование самостоятельно разработанной системы защиты в приложение на уровне исходного кода

c) Отсутствие необходимости изучения и модификации исполняемого кода защищенного приложения для обхода защиты

d) Сложность в нейтрализации защиты вследствие её уникальности и «размытости» в теле программы

13. К этапу инициализации программно-аппаратного комплекса «Соболь» не относится:

a) Установка платы комплекса

b) Настройка общих параметров

Согласована на портале № 28673

c) Настройка параметров подключения к сети

d) Настройка контроля целостности

14. К переводу программно-аппаратного комплекса «Соболь» в режим эксплуатации не относится действие:

a) Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI

b) Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI

c) Вытащите кабель из порта «Настройка» и переключите его в порт «Эксплуатация»

d) Подключите к плате считыватель iButton

15. Выберите верный вариант ответа. Выставьте в правильном порядке действия при установке программно-аппаратного комплекса «Аккорд». 1. Подсоединение контактного устройства (съемника информации). 2. Установка платы контроллера в свободный слот ПЭВМ. 3. Регистрация администратора БИ, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ. 4. Назначение списка дисков, файлов, разделов реестра, контролируемых на целостность. 5. Регистрация пользователей, назначение пользователям персональных идентификаторов, паролей и времени доступа

a) 2, 1, 3, 4, 5

b) 1, 2, 3, 5, 4

c) 2, 1, 3, 5, 4

d) 1, 2, 5, 4, 3

16. Какое из перечисленных программно-аппаратных средств не используют для хранения криптографических ключей?

a) eToken

b) Смарт-карты

c) iButton

d) Аппаратный модуль безопасности (HSM)

17. Какое из высказываний не относится к преимуществам аппаратного генератора случайных чисел:

a) Запас чисел не ограничен

b) Низкие вычислительные затраты

c) Используется специальное устройство

d) Не занимается место в памяти

18. Какое из действий не относится к организации замкнутой программной среды в КСЗИ «Панцирь-К»:

a) Задание списка разрешенных процессов (системных и прикладных) с возможностью запуска только тех процессов, которые отнесены к разрешенным

b) Задание папок, откуда разрешается запускать программы (с запретом записи и модификации в них файлов)

c) Задание специального общего пользователя, от чьего лица совершается установка и запуск программ

d) Дополнительный анализ содержимого файлов (поиск признаков исполняемого файла)

19. При взломе программ, защищенных с помощью аппаратных ключей защиты не используется следующий метод:

a) Отладка

b) Дизассемблирования

c) Диверсификация

d) Дамп оперативной памяти

20. Что не входит в комплектацию программно-аппаратного комплекса «Аккорд-АМДЗ»?

a) Контроллер

b) Съемник информации с контактным устройством

c) Секретный логин и пароль, необходимый для первоначального запуска АМДЗ

d) Персональный идентификатор пользователя

14.1.2. Экзаменационные вопросы

1. Методы обеспечения информационной безопасности автоматизированных систем (основные понятия, угрозы).

Согласована на портале № 28673

2. Методы обеспечения информационной безопасности автоматизированных систем (методы взлома, защита от взлома).

3. Методы обеспечения информационной безопасности автоматизированных систем (защита от программных закладок).

4. Политика безопасности. Модель КС.

5. Замкнутая программная среда.

6. Формирование и поддержка изолированной программной среды.

7. Реализация ИПС с использованием механизма расширения BIOS

8. UEFI. Принципы работы

9. Персональное средство аутентификации eToken

10. eToken API

11. Безопасное взаимодействие в КС. Процедуры идентификации и аутентификации.

12. Аутентификация до загрузки ОС

13. Контроль и управление доступом. Диспетчер доступа.

14. Назначение, функции, принцип работы ПАК «Аккорд».

15. Назначение, функции, принцип работы ПАК «Соболь».

16. Персональные идентификаторы. Виды, назначение, функции.

17. Назначение, функции, принцип работы ключей защиты. Известные модели.

18. Виды защиты ПО с помощью электронных ключей. Методы взлома.

19. КСЗИ Панцирь-К. Серверная и клиентские части, идентификация и аутентификация пользователей

20. КСЗИ Панцирь-К. Контроль и разграничение доступа

21. КСЗИ Панцирь-К. Аудит и дополнительные возможности

22. Управление криптографическими ключами

23. Концепция иерархии ключей, генерация ключей.

24. Аппаратные модули безопасности (HSM)

25. Концепция доверенных сеансов связи.. Комплекс «МАРШ!», «М!&М».

26. Защищенные микрокомпьютеры «МКТ». Назначение, функции.

27. Защищенные носители «СЕКРЕТ». Виды, назначение, функции.

14.1.3. 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

14.1.4. Вопросы на самоподготовку

1. Подсистема безопасности операционной системы Windows

2. Аудит событий безопасности в операционной системе Windows

3. Поставщик служб криптографии ОС Windows

4. Поставщик служб криптографии КриптоПро и его интеграции в ОС Windows

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

Согласована на портале № 28673

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

14.1.5. Темы лабораторных работ

Разработка защищенного ПО с применением аппаратных ключей eToken

Программно-аппаратное средство защиты информации от несанкционированного доступа.

Защита программ от изменения и контроль целостности.

Защита программ от разрушающих программных воздействий и защита автоматизированной системы от вредоносного программного обеспечения.

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

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

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

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

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

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

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

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

- письменно на бумаге;
- набор ответов на компьютере;

Согласована на портале № 28673

– 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 № 28673