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 УР
_____Сенченко П.В.
«13» _____12_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.01 Информатика и вычислительная техника**
Направленность (профиль) / специализация: **Информационное и программное обеспечение программно-аппаратных комплексов робототехнических систем**
Форма обучения: **очная**
Факультет: **Факультет инновационных технологий (ФИТ)**
Кафедра: **управления инновациями (УИ)**
Курс: **3**
Семестр: **6**
Учебный план набора 2024 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	6 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
Самостоятельная работа	54	54	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестации	Семестр
Зачет с оценкой	6

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 13.12.2023
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 80080

1. Общие положения

1.1. Цели дисциплины

1. Формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, навыков и умений по применению программно-аппаратных средств защиты информации в конкретных условиях.
2. Развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

1.2. Задачи дисциплины

1. Дать знания по концепции обеспечения информационной безопасности компьютерных систем с применением программно-аппаратных средств защиты информации.
2. Сформировать представление и получить навыки работы с программно-аппаратными средствами защиты информации, реализующим отдельные функциональные требования по защите.
3. Дать знания по методам и средствам хранения ключевой информации, методам и средствам ограничения доступа к компонентам вычислительных систем, задачам и технологии сертификации программно-аппаратных средств защиты информации на соответствие требованиям информационной безопасности.
4. Сформировать навыки и знания по методам защиты от сетевых атак.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: ФТД. Факультативные дисциплины.

Индекс дисциплины: ФТД.02.02.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

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

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

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		
ПК-9. Способен обеспечивать информационную безопасность уровня баз данных.	ПК-9.1. Знает основы информационной безопасности	Знает основы информационной безопасности, в том числе типы программно-аппаратных средств защиты информации
	ПК-9.2. Умеет обеспечивать безопасность на уровне баз данных	Умеет обеспечивать безопасность на различных уровнях с применением типовых программно-аппаратных средств защиты информации
	ПК-9.3. Владеет навыками использования современных системам управления базами данных	Владеет навыками обеспечения информационной безопасности, в том числе с применением систем управления базами данных

Согласована на портале № 80080

ПК-10. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения. Способен проводить регламентные работы на сетевых устройствах и программном обеспечении инфокоммуникационной системы	ПК-10.1. Знает основы работы и параметры настройки телекоммуникационных устройств	Знает основы работы и параметры настройки телекоммуникационных устройств, небходимые для обеспечения безопасности данных устройств.
	ПК-10.2. Умеет настраивать параметры работы сетевых протоколов, проводить регламентные работы на сетевых устройствах и программном обеспечении инфокоммуникационной системы	Умеет настраивать параметры работы сетевых протоколов, проводить настройку сетевого программного обеспечения инфокоммуникационной системы
	ПК-10.3. Владеет современными методами обеспечения сетевой безопасности	Владеет современными методами обеспечения сетевой безопасности, в том числе с применением программно-аппаратных средств защиты информации

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

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

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

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	54	54
Лекционные занятия	18	18
Лабораторные занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	54	54
Подготовка к зачету с оценкой	13	13
Подготовка к тестированию	5	5
Подготовка к защите отчета по лабораторной работе	18	18
Подготовка к лабораторной работе, написание отчета	18	18
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

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

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

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
6 семестр					

Согласована на портале № 80080

1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	4	-	6	10	ПК-10, ПК-9
2 Программно-аппаратные средства обеспечения информационной безопасности.	12	36	44	92	ПК-10, ПК-9
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	2	-	4	6	ПК-10, ПК-9
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.
Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
6 семестр			
1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	4	ПК-9, ПК-10
	Итого	4	
2 Программно-аппаратные средства обеспечения информационной безопасности.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Средства обеспечения информационной безопасности в операционной системе Astra Linux. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе Astra Linux. Замкнутая программная среда и контроль целостности в операционной системе Astra Linux. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Средства обеспечения безопасности сети.	12	ПК-9, ПК-10
	Итого	12	

Согласована на портале № 80080

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. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий	2	ПК-9, ПК-10
	Итого	2	
	Итого за семестр	18	
	Итого	18	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
6 семестр			

Согласована на портале № 80080

2 Программно-аппаратные средства обеспечения информационной безопасности.	Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе Astra Linux.	4	ПК-9, ПК-10
	Замкнутая программная среда и контроль целостности в операционной системе Astra Linux.	4	ПК-9, ПК-10
	Secret Net Studio. Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.	4	ПК-9, ПК-10
	Secret Net Studio. Замкнутая программная среда. Контроль целостности.	4	ПК-9, ПК-10
	Secret Net Studio. Аудит событий информационной безопасности в СЗИ от НСД Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование	4	ПК-9, ПК-10
	Администрирование безопасности сетевых устройств и сетевого программного обеспечения	8	ПК-9, ПК-10
	Изучение современных програмнно-аппаратных средств защиты информации	8	ПК-9, ПК-10
	Итого	36	
Итого за семестр		36	
Итого		36	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

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

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
6 семестр				
1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Подготовка к зачету с оценкой	4	ПК-9, ПК-10	Зачёт с оценкой
	Подготовка к тестированию	2	ПК-9, ПК-10	Тестирование
	Итого	6		

Согласована на портале № 80080

2 Программно-аппаратные средства обеспечения информационной безопасности.	Подготовка к зачету с оценкой	6	ПК-9, ПК-10	Зачёт с оценкой
	Подготовка к тестированию	2	ПК-9, ПК-10	Тестирование
	Подготовка к защите отчета по лабораторной работе	18	ПК-9, ПК-10	Защита отчета по лабораторной работе
	Подготовка к лабораторной работе, написание отчета	18	ПК-9, ПК-10	Лабораторная работа
	Итого	44		
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	Подготовка к зачету с оценкой	3	ПК-9, ПК-10	Зачёт с оценкой
	Подготовка к тестированию	1	ПК-9, ПК-10	Тестирование
	Итого	4		
Итого за семестр		54		
Итого		54		

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

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

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

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ПК-9	+	+	+	Зачёт с оценкой, Защита отчета по лабораторной работе, Лабораторная работа, Тестирование
ПК-10	+	+	+	Зачёт с оценкой, Защита отчета по лабораторной работе, Лабораторная работа, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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
6 семестр				
Зачёт с оценкой	0	0	30	30
Защита отчета по лабораторной работе	10	10	10	30

Согласована на портале № 80080

Лабораторная работа	10	10	10	30
Тестирование	0	0	10	10
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/491249.

7.2. Дополнительная литература

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/237770.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Администрирование средств защиты информации: Учебно-методическое пособие для студентов направлений подготовки 10.00.00 Информационная безопасность / И. А. Рахманенко, А. Ю. Якимук - 2022. 166 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9988.

2. Разработка компонентов средств защиты информации: Учебно-методическое пособие / И. А. Рахманенко, А. Ю. Якимук - 2022. 78 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9996.

Согласована на портале № 80080

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

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

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

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

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. 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:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Аппаратные средства аутентификации пользователя "eToken Pro";
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x;
- Устройства чтения смарт-карт и радиометок: адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security;
- Microsoft Windows 10;
- VirtualBox;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Согласована на портале № 80080

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

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

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

Перечень программного обеспечения:

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

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

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

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

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

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

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

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

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	ПК-10, ПК-9	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Тестирование	Примерный перечень тестовых заданий

Согласована на портале № 80080

2 Программно-аппаратные средства обеспечения информационной безопасности.	ПК-10, ПК-9	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	ПК-10, ПК-9	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Тестирование	Примерный перечень тестовых заданий

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

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

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

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции

Согласована на портале № 80080

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

9.1.1. Примерный перечень тестовых заданий

1. 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

Согласована на портале № 80080

выбор – защищенного или обычного – в программно-аппаратном комплексе МКTrusT:
a) Используется выбор режима в процессе загрузки компьютера
b) Используется дополнительное устройство, содержащее операционную систему для соответствующего режима работы МКTrusT
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)
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

Согласована на портале № 80080

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
    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)

Согласована на портале № 80080

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

9.1.2. Перечень вопросов для зачета с оценкой

1. Методы обеспечения информационной безопасности автоматизированных систем (основные понятия, угрозы).
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 автоматизированной системы.
5. Замкнутая программная среда. Ядро безопасности с учетом контроля порождения субъектов
6. Формирование и поддержка изолированной программной среды. Условия невозможности НСД
7. Реализация ИПС с использованием механизма расширения BIOS
8. UEFI. Принципы работы
9. Безопасное взаимодействие в КС. Процедуры идентификации и аутентификации
10. Аутентификация до загрузки ОС
11. Контроль и управление доступом
12. Персональное средство аутентификации eToken
13. eToken API
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. Защитные механизмы Astra Linux Special Edition: дискреционное и мандатное разграничение доступа.
20. Защитные механизмы Astra Linux Special Edition: замкнутая программная среда и контроль целостности
21. Управление криптографическими ключами
22. Концепция иерархии ключей, генерация ключей
23. Аппаратные модули безопасности (HSM)
24. Концепция доверенных сеансов связи. Комплекс «МАРШ!», «М!&М».
25. Защищенные микрокомпьютеры «МКТ». Назначение, функции.
26. Защищенные носители «СЕКРЕТ». Виды, назначение, функции.
27. Средства защиты виртуальной инфраструктуры. vGate.
28. Сертификация автоматизированных систем и средств вычислительной техники: виды нормативных документов, определяющих требования по сертификации СЗИ.
29. Сертификация автоматизированных систем и средств вычислительной техники: требования к средствам вычислительной техники
30. Сертификация автоматизированных систем и средств вычислительной техники:

Согласована на портале № 80080

требования по контролю отсутствия недекларированных возможностей
31. Сертификация автоматизированных систем и средств вычислительной техники: требования по уровням доверия (Приказ ФСТЭК № 76).

9.1.3. Примерный перечень вопросов для защиты лабораторных работ

1. Каким образом в Astra Linux реализуется дискреционное разграничение доступа к файлам?
2. Каким образом в Astra Linux реализуется мандатное разграничение доступа к файлам?
3. Для чего предназначен механизм контроля подключения и изменения устройств?
4. Каким образом Secret Net Studio определяет, будет ли распечатан конфиденциальный документ?
5. В каких ситуациях пользователь не сможет войти в операционную систему?
6. Для чего предназначен механизм контроля целостности (КЦ)?
7. Для чего предназначен механизм замкнутой программной среды (ЗПС)?
8. Для чего на практике применяется «мягкий» режим работы ЗПС?
9. Какие типы файлов следует ставить на контроль целостности?
10. Почему не стоит ставить текстовые документы на контроль целостности?

9.1.4. Темы лабораторных работ

1. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе Astra Linux.
2. Замкнутая программная среда и контроль целостности в операционной системе Astra Linux.
3. Secret Net Studio. Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.
4. Secret Net Studio. Замкнутая программная среда. Контроль целостности.
5. Secret Net Studio. Аудит событий информационной безопасности в СЗИ от НСД Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование
6. Администрирование безопасности сетевых устройств и сетевого программного обеспечения
7. Изучение современных програмнно-аппаратных средств защиты информации

9.2. Методические рекомендации

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

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

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

При самостоятельном изучении тем следуйте рекомендациям:

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

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

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

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

Согласована на портале № 80080

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

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

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

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

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

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

– в печатной форме;
– 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;

Согласована на портале № 80080

– в печатной форме.

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

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 10 от «21» 11 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. УИ	Г.Н. Нариманова	Согласовано, eb4e14e0-de8d-48f7-bf05-ceacb167edfe
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. УИ	М.Е. Антипин	Согласовано, c47100a1-25fd-4b1a-af65-5d736538bbd4
Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd

РАЗРАБОТАНО:

Доцент, каф. БИС	И.А. Рахманенко	Разработано, 438e5305-e83a-40ae-b333-7c84f2fc4661

Согласована на портале № 80080