МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разработка компонентов средств защиты информации

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **2**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	2 семестр	Всего	Единицы
1	Лекции	16	16	часов
2	Практические занятия	32	32	часов
3	Всего аудиторных занятий	48	48	часов
4	Самостоятельная работа	60	60	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 2 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 13 от «24» 12 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.04.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. БИС _____ И. А. Рахманенко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

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

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

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Формирование глубокого понимания принципов функционирования компонентов средств защиты информации;

Получение практических навыков создания и тестирования компонентов средств защиты информации.

1.2. Задачи дисциплины

- Ознакомление с типовыми компонентами средств защиты информации;
- Изучение принципов функционирования компонентов средств защиты информации;
- Получение практических навыков создания компонентов средств защиты информации;
- Получение практических навыков тестирования компонентов средств защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Разработка компонентов средств защиты информации» (Б1.В.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Администрирование средств защиты информации объектов критической информационной инфраструктуры.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты, Защищенные информационные системы, Научно-исследовательская работа (рассред.), Преддипломная практика, Технологии построения защищенных каналов передачи данных, Управление компьютерными инцидентами.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-2 способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;
- ПК-4 способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности;
- ПК-16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

В результате изучения дисциплины обучающийся должен:

- **знать** Типовые компоненты средств защиты информации; Принципы функционирования компонентов средств защиты информации; Методы тестирования работоспособности компонентов средств защиты информации.
- **уметь** Создавать компоненты средств защиты информации; Тестировать работоспособность компонентов средств защиты информации.
- **владеть** Навыками разработки и анализа компонентов средств защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Аудиторные занятия (всего)	48	48
Лекции	16	16
Практические занятия	32	32
Самостоятельная работа (всего)	60	60

Проработка лекционного материала	10	10
Написание рефератов	18	18
Подготовка к практическим занятиям, семинарам	32	32
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр					
1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	6	0	22	28	ПК-2
2 Разработка компонентов средств защиты информации	8	24	29	61	ПК-16, ПК-2, ПК-4
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	2	8	9	19	ПК-16, ПК-4
Итого за семестр	16	32	60	108	
Итого	16	32	60	108	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.	2	ПК-2
	Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом; взаимодействие с аппаратными средства защиты информации; конфигурирование; аудит; мониторинг и оперативное управление; контроль печати.	2	

	Системы управления жизненным циклом средств аутентификации; Средства обеспечения безопасности компьютерной сети; Средства обеспечения мониторинга и аудита событий информационной безопасности в корпоративных сетях.	2	
	Итого	6	
2 Разработка компонентов средств защиты информации	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.	2	ПК-2
	Модели безопасного взаимодействия в АС. Процедура идентификации и аутентификации: защита на уровне аппаратных средств, защита на уровне загрузчиков операционной среды. Методы аутентификации в программных средствах защиты информации.	2	
	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.	2	
	Применение криптографических средств защиты информации в компонентах средств защиты информации. Обеспечение конфиденциальности информации криптографическими методами. Обеспечение целостности информации криптографическими методами.	2	
	Итого	8	
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	Методы тестирования при разработке программного обеспечения;Создание методики испытаний компонентов средств защиты информации.	2	ПК-4
	Итого	2	
Итого за семестр		16	

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 Администрирование средств защиты информации объектов критической информационной инфраструктуры	+		
Последующие дисциплины			
1 Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты	+	+	+
2 Защищенные информационные системы	+	+	
3 Научно-исследовательская работа (рассред.)	+	+	
4 Преддипломная практика	+	+	+
5 Технологии построения защищенных каналов передачи данных		+	
6 Управление компьютерными инцидентами	+		

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

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

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПК-2	+	+	+	Защита отчета, Зачёт, Тест, Реферат, Отчет по практическому занятию
ПК-4	+	+	+	Защита отчета, Зачёт, Тест, Отчет по практическому занятию
ПК-16		+	+	Защита отчета, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.
Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
2 Разработка	Разработка подсистемы аутентификации	8	ПК-16, ПК-2,

компонентов средств защиты информации	средств защиты информации: аутентификация с использованием пароля, внешних аутентификаторов.		ПК-4
	Разработка подсистемы обеспечения целостности средства защиты информации.	8	
	Разработка подсистемы криптографической защиты информации для средства защиты информации.	8	
	Итого	24	
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	Разработка методики проведения испытаний разработанных компонентов средств защиты информации. Проведение тестирования разработанных подсистем.	8	ПК-16, ПК-4
	Итого	8	
Итого за семестр		32	

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
2 семестр				
1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	Написание рефератов	12	ПК-2	Зачёт, Реферат, Тест
	Написание рефератов	6		
	Проработка лекционного материала	2		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Итого	22		
2 Разработка компонентов средств защиты информации	Подготовка к практическим занятиям, семинарам	24	ПК-16, ПК-2, ПК-4	Зачёт, Защита отчета, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Итого	29		
3 Программы и	Подготовка к практиче-	8	ПК-16, ПК-4	Зачёт, Защита отче-

методики испытаний средств и систем обеспечения информационной безопасности	ским занятиям, семинарам			та, Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Итого	9		
Итого за семестр		60		
Итого		60		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
2 семестр				
Зачёт			30	30
Защита отчета	10	10	10	30
Отчет по практическому занятию	10	10	10	30
Реферат			5	5
Тест			5	5
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	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. Рябко, Б. Я. Криптографические методы защиты информации [Электронный ресурс]: учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097 (дата обращения: 23.03.2020). — Режим доступа: для авториз. пользователей. — Режим доступа: https://e.lanbook.com/book/111097 (дата обращения: 24.03.2020).
2. Бабенко, Людмила Клементьевна. Защита информации с использованием смарт-карт и электронных брелоков. - М. : "Гелиос АРВ" , 2003. - 352 с. (наличие в библиотеке ТУСУР - 29 экз.)

12.2. Дополнительная литература

1. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс]: монография / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2016. — 304 с. — ISBN 978-5-9912-0439-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111005 (дата обращения: 23.03.2020). — Режим доступа: для авториз. пользователей. — Режим доступа: https://e.lanbook.com/book/111005 (дата обращения: 24.03.2020).
2. Искусство тестирования программ : Пер. с англ. / Гленфорд Дж. Майерс; Ред. пер. Б. А. Позин. - М. : Финансы и статистика, 1982. - 176 с. : ил. - Библиогр. в конце глав. -Библиогр.: с. 172-173. -Предм. указ.: с. 173-174. - (в пер.) : Б. ц. (наличие в библиотеке ТУСУР - 3 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в компьютерных системах [Электронный ресурс]: Методические рекомендации к практическим занятиям / Е. Г. Годенова - 2012. 79 с. — Режим доступа: https://edu.tusur.ru/publications/1231 (дата обращения: 24.03.2020).
2. Защита информации в компьютерных системах [Электронный ресурс]: Методические рекомендации к организации самостоятельной работы / Е. Г. Годенова - 2012. 9 с. — Режим доступа: https://edu.tusur.ru/publications/1232 (дата обращения: 24.03.2020).
3. 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: 24.03.2020).

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

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:

- Моноблок Asus V222GAK-BA021D: IntelJ5005/ DDR44G / 500Gb/ WiFi / мышь/ клавиатура (10шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security
- Microsoft Windows 10
- Visual Studio

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

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

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

Описание имеющегося оборудования:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Аппаратные средства аутентификации пользователя «eToken Pro»;
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;

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

Устройства чтения смарт-карт и радиометок: Адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Kaspersky endpoint security
- Microsoft Windows 10
- VirtualBox
- Visual Studio
- Аппаратно-программные средства управления доступом к данным, шифрования: 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
- Средство сканирования защищенности компьютерных сетей: MaxPatrol Education

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:
- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

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

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. 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 МКTrusT 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 МКTrusT присутствует IP-телефон, построенный на «гарвардской» архитектуре

d) МКTrusT 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 МКTrusT:

a) Используется выбор режима в процессе загрузки компьютера

b) Используется дополнительное устройство, содержащее операционную систему для соот-

ветствующего 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)

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

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. Зачёт

Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.

Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом;

Принципы построения средств защиты информации от несанкционированного доступа: взаимодействие с аппаратными средства защиты информации; конфигурирование;

Принципы построения средств защиты информации от несанкционированного доступа: аудит; мониторинг и оперативное управление; контроль печати.

Системы управления жизненным циклом средств аутентификации;

Средства обеспечения безопасности компьютерной сети;

Средства обеспечения мониторинга и аудита событий информационной безопасности в корпоративных сетях.

Методы и средства ограничения доступа к компонентам вычислительных систем.

Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.

Модели безопасного взаимодействия в АС.

Процедура идентификации и аутентификации: защита на уровне аппаратных средств, защита на уровне загрузчиков операционной среды.

Методы аутентификации в программных средствах защиты 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.

Применение криптографических средств защиты информации в компонентах средств защиты информации. Обеспечение конфиденциальности информации криптографическими методами.

Обеспечение целостности информации криптографическими методами.

Методы тестирования при разработке программного обеспечения;

Создание методики испытаний компонентов средств защиты информации.

14.1.3. Темы рефератов

ПАК “Соболь”

ПАК “Аккорд АМДЗ”

КСЗИ “Панцирь-К”.

Подсистема безопасности операционной системы Windows

Аудит событий безопасности в операционной системе Windows

Поставщик служб криптографии ОС Windows

Поставщик служб криптографии КриптоПро и его интеграции в ОС Windows

Электронные платежные системы – принципы функционирования и защиты информации

Управление криптографическими ключами. Генерация ключей

Управление криптографическими ключами. Хранение ключей

Управление криптографическими ключами. Распределение ключей

Методы защиты программ от изучения

Методы и средства исследования программ

Методы и средства ограничения доступа к компонентам ЭВМ

Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям

Защита от изменения и контроль целостности

Проблемы обеспечения безопасности при удалённом доступе

Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях

Архитектура межсетевых экранов

14.1.4. Вопросы для подготовки к практическим занятиям, семинарам

Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом;

Принципы построения средств защиты информации от несанкционированного доступа: взаимодействие с аппаратными средства защиты информации; конфигурирование;

Принципы построения средств защиты информации от несанкционированного доступа: аудит; мониторинг и оперативное управление; контроль печати.

Методы аутентификации в программных средствах защиты 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.

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;

– 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.