Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2024 13:49:29
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2024

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Составители:

старший преподаватель	Коновалова А.Д.
ассистент	Курцев Е.А.
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

«06» __09__ 2024 г., протокол № 2

Директор ВШИСиКТ	к.э.н., доцент	Филиппова О.А.
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование у обучающихся общепрофессиональной компетенции в области применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.
- формирование у обучающихся профессиональной компетенции в области установки, настройки, обслуживания и безопасной эксплуатации программных, программно-аппаратных и технических средств защиты информации.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	Основание (ПС) *для профессиональных компетенций
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знает основные характеристики, достоинства и недостатки средств криптографической и технической защиты информации в автоматизированных системах. ИОПК-9.2. Применяет средства криптографической и технической защиты информации от утечки. ИОПК-9.3. Применяет технические средства контроля эффективности применяемых мер защиты информации	**Знает:** назначение, классификацию, основные характеристики, достоинства и ограничения программно-аппаратных, криптографических и технических средств защиты информации **Умеет:** выбирать и применять программно-аппаратные средства защиты с учетом угроз, требований к объекту защиты, совместимости и условий эксплуатации **Владеет:** навыками настройки базовых механизмов криптографической и технической защиты, контроля их состояния и оценки эффективности применяемых мер	
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных, в том числе криптографических, и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации. ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	**Знает:** порядок установки, первичной настройки, обслуживания и безопасной эксплуатации программных, программно-аппаратных и технических средств защиты информации **Умеет:** устанавливать средства защиты по технической документации, настраивать параметры работы, выполнять резервирование конфигурации, обновление и диагностику **Владеет:** навыками администрирования средств защиты, документирования конфигурации, контроля работоспособности и устранения типовых неисправностей	06.032 «Специалист по безопасности компьютерных систем и сетей»

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части, Блока 1. Дисциплины (модули) образовательной программы (Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**80/58**
занятия лекционного типа (лекции)	28/22
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	36/26
лабораторные работы	16/10
Самостоятельная работа всего, в т.ч.:	**1/41**
Самоподготовка по темам (разделам) дисциплины	1/41
Контроль (часы на экзамен, зачет)	**27/9**
Промежуточная аттестация	**Экзамен**

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 1. АРХИТЕКТУРА И КЛАССИФИКАЦИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ** Содержание лекции: Место программно-аппаратных средств в комплексной системе защиты. Классификация по назначению и уровню применения. Модели угроз и нарушителя как основа выбора средств. Требования совместимости, надежности и доверия.	4/3				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №1. Исследование состава программно-аппаратного комплекса защиты.		2/1			Отчет по лабораторной работе
	Практическая работа №1. Инвентаризация средств защиты и формирование профиля требований к защищаемому объекту.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов

ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 2. ДОВЕРЕННАЯ ЗАГРУЗКА, АППАРАТНЫЕ КОРНИ ДОВЕРИЯ И КОНТРОЛЬ ЦЕЛОСТНОСТИ** Содержание лекции: Принципы доверенной вычислительной среды. UEFI Secure Boot, TPM и аппаратный корень доверия. Измеренная загрузка. Контроль целостности программной среды и конфигурации.	4/3				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №2. Настройка доверенной загрузки и проверка контроля целостности.		2/1			Отчет по лабораторной работе
	Практическая работа №2. Анализ механизмов доверенной загрузки и контроля целостности.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 3. АППАРАТНЫЕ СРЕДСТВА ИДЕНТИФИКАЦИИ, АУТЕНТИФИКАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ** Содержание лекции: Токены, смарт-карты, считыватели и биометрические устройства. Многофакторная аутентификация. Хранение учетных данных и сертификатов. Риски утраты, подмены и клонирования аутентификаторов.	4/3				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №3. Настройка многофакторной аутентификации с использованием токена или его программной модели.		2/1			Отчет по лабораторной работе
	Практическая работа №3. Разработка схемы многофакторной аутентификации.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 4. КРИПТОГРАФИЧЕСКИЕ ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА И УПРАВЛЕНИЕ КЛЮЧАМИ** Содержание лекции: Криптографические модули, аппаратные модули безопасности и криптографические шлюзы. Генерация и хранение ключей. Жизненный цикл ключевого материала. Резервирование, разграничение полномочий и аудит операций.	4/3				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №4. Выполнение криптографических операций и работа с сертификатами.		2/1			Отчет по лабораторной работе
	Практическая работа №4. Организация жизненного цикла ключей.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9	**ТЕМА 5. ПРОГРАММНО-АППАРАТНЫЕ**	4/3				Лекция-

ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ** Содержание лекции: Межсетевые экраны, VPN-шлюзы, системы обнаружения и предотвращения вторжений. Фильтрация трафика и сегментация. Схемы включения средств защиты. Производительность, отказоустойчивость и журналирование.					визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №5. Развертывание межсетевого экрана и защищенного сетевого соединения.		2/1			Отчет по лабораторной работе
	Практическая работа №5. Проектирование межсетевого экранирования и защищенного соединения.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 6. СРЕДСТВА ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ, СЕРВЕРОВ И ХРАНИЛИЩ ДАННЫХ** Содержание лекции: Контроль устройств и приложений, защита конечных точек, шифрование носителей и резервных копий. Разграничение доступа к данным. Изоляция в виртуальной среде. Контроль событий безопасности.	4/3				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №6. Настройка защиты конечной точки и шифрования данных.		2/1			Отчет по лабораторной работе
	Практическая работа №6. Разработка политики защиты конечных точек и данных.			4/3		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9 ИОПК-9.1 ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 7. УСТАНОВКА, НАСТРОЙКА И ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ СРЕДСТВ ЗАЩИТЫ** Содержание лекции: Подготовка к развертыванию. Работа с технической документацией. Базовая и усиленная конфигурация. Управление обновлениями, резервными копиями и изменениями. Мониторинг работоспособности и безопасная эксплуатация.	2/2				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №7. Установка и первичная настройка средства защиты.		2/2			Отчет по лабораторной работе
	Практическая работа №7. Разработка регламента установки и обслуживания средства защиты.			6/4		Отчет по практической работе
	Самостоятельная работа.				0/5	Самостоятельное изучение учебных материалов
ОПК-9 ИОПК-9.1	**ТЕМА 8. КОНТРОЛЬ ЭФФЕКТИВНОСТИ, ДИАГНОСТИКА И ЖИЗНЕННЫЙ ЦИКЛ**	2/2				Лекция-визуализация

ИОПК-9.2 ИОПК-9.3 ПК-1 ИПК-1.1 ИПК-1.2	**СРЕДСТВ ЗАЩИТЫ** Содержание лекции: Приемочные и периодические проверки. Критерии работоспособности и эффективности. Диагностика неисправностей, восстановление и откат конфигурации. Вывод из эксплуатации и безопасное уничтожение данных.					(в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №8. Проверка работоспособности комплекса средств защиты.		2/2			Отчет по лабораторной работе
	Практическая работа №8. Разработка программы проверки эффективности комплекса средств защиты.			6/4		Отчет по практической работе
	Самостоятельная работа.				1/6	Самостоятельное изучение учебных материалов
	ИТОГО	**28/22**	**16/10**	**36/26**	**1/41**	

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

–качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;

–качество оформления отчета по работе;

–качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Беляков, С. Л. Основы разработки программ на языке С++ для систем информационной безопасности : учеб. пособие / С. Л. Беляков, А. В. Боженюк, М. В. Петряева. - Документ read. - Ростов- на Дону [и др.] : Изд-во Юж. федер. ун-та, 2020. - 151 с. - Лаб. работы. - Прим. тест. вопр. - URL: https://znanium.com/read?id=374992 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-9275-3521-7. - Текст : электронный.

2. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2024. - 400 с. - (Высшее образование). - URL: https://znanium.ru/read?id=443251 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-106478-8. - Текст : электронный.

3. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. – Изд. 3-е, стер. – Документ read. – Санкт-Петербург [и др.] : Лань, 2024. – 321 с. – URL: https://reader.lanbook.com/book/370967 (дата обращения: 29.04.2024). - Режим доступа: для авториз. пользователей. – ISBN 978-5-507-49077-6. – Текст : электронный.

4. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00. - Текст : электронный.

5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ read. - Москва : ФОРУМ [и др.], 2022. - 592 с. : ил. - (Высшее образование - Бакалавриат) (Высшее образование - Бакалавриат). - Предм. указ. - URL: https://znanium.ru/read?id=389857 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8199-0730-6. - 978-5-16-106148-0. - Текст : электронный.

Дополнительная литература

6. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации : [справ. изд.] / Г. А. Бузов. - Москва : Горячая линия - Телеком, 2010. - 237 с. : ил. - ISBN 978-5-9912-0121-6 : 255-40. - Текст : непосредственный.

7. Введение в информационную безопасность : учеб. пособие для вузов / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под ред. В. С. Горбатова. - Москва : Горячая линия - Телеком, 2011. - 288 с. : ил. - (Учебное пособие для высших учебных заведений). - ISBN 978-5-9912-0160-5 : 275-30. - Текст : непосредственный.

8. Малюк, А. А. Теория защиты информации / А. А. Малюк. - Москва : Горячая линия - Телеком, 2013. - 184 с. : табл. - ISBN 978-5-9912-0246-6 : 448-10. - Текст : непосредственный.

9. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учеб. пособие / С. Н. Никифоров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2023. - 93 с. - Прил. - URL: https://reader.lanbook.com/book/288974 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45868-4. - Текст : электронный.

10. Платонов, В. В. Программно-аппаратные средства защиты информации : учеб. для вузов по направлению подгот. "Информ. безопасность" / В. В. Платонов. - Документ Adobe Acrobat. - Москва : Академия, 2013. - 63,7 МБ, 332 с. : ил., табл. - (Высшее профессиональное образование. Бакалавриат). - Прил. - URL: http://elib.tolgas.ru/publ/kay/Platonov_Progr_apparat_sredstva.pdf (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-7695-9327-7. - Текст : электронный.

11. Проскурин, В. Г. Защита программ и данных : учеб. пособие для вузов по направлению подгот. "Информ. безопасность" (бакалавр) и специальностям: "Компьютер. безопасность", "Информ. безопасность автоматизир. систем" / В. Г. Проскурин. - Москва : Академия, 2012. - 208 с. : ил. - (Высшее профессиональное образование. Информационная безопасность. Бакалавриат). - Прил. - ISBN 978-5-7695-9288-1 : 481-80. - Текст : непосредственный.

12. Учебно-методический комплекс по дисциплине "Программно-аппаратные средства защиты информации" : для студентов направления подгот. 10.03.01 "Информ. безопасность" / Поволж. гос. ун-т сервиса (ПВГУС), Каф. "Приклад. информатика в экономике" ; сост.: С. М. Бобровский. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2016. - 5,99 МБ, 196 с. - Прил. - URL: http://elib.tolgas.ru/publ/UMK_Bobrovskij_Program_apparat_sredstva_zasch_inform.pdf (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - 0-00. - Текст : электронный.

13. Хорев, П. Б. Программно-аппаратная защита информации : учеб. пособие для вузов по направлениям "Информ. безопасность" и "Информатика и вычисл. техника" / П. Б. Хорев. - Москва : ФОРУМ, 2009. - 351 с. : ил. - (Высшее образование). - ISBN 978-5-91134-353-8 : 275-60. - Текст : непосредственный.

14. Яшин, В. Н. Информатика. Программные средства персонального компьютера : учеб. пособие для вузов по направлению "Приклад. информатика" и др. экон. специальностям / В. Н. Яшин. - Документ read. - Москва : ИНФРА-М, 2018. - 236 с. - (Высшее образование - Бакалавриат). - URL: https://znanium.ru/read?id=302916 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-100158-5. - Текст : электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU : Электронное периодическое издание : сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 02.09.2024). – Текст: электронный.
2. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 02.09.2024). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
3. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 02.09.2024). - Текст : электронный.
4. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 02.09.2024). - Текст : электронный.
5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.

6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.
7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Oracle VM VirtualBox	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
3	Wireshark	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
4	OpenSSL	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
5	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Лабораторные работы.

Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования // Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации // Помещение для хранения и профилактического обслуживания учебного оборудования (Г-413)», оснащенная следующим оборудованием: рабочие места обучающихся; Рабочее место преподавателя; Учебно-наглядные пособия, обеспечивающие тематические иллюстрации. Компьютер Аксус Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный DraperLuma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб. Лаборатория оснащена кондиционером.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Экзамен	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество	Баллы за единицу	Максимум баллов
Активность и тематический контроль на лекциях	8	1	8
Лабораторные и практические работы	8	8	64
Самостоятельная работа / рубежное тестирование	4	7	28
			100 баллов

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа №1. Инвентаризация средств защиты и формирование профиля требований к защищаемому объекту.
Задание 1. Составить перечень информационных ресурсов и компонентов условного объекта защиты.
Задание 2. Определить актуальные угрозы и предполагаемые действия нарушителя.
Задание 3. Классифицировать необходимые программные, программно-аппаратные и технические средства защиты.
Задание 4. Сопоставить функции выбранных средств с выявленными угрозами.
Задание 5. Оформить профиль требований и обосновать состав комплекса защиты.

Практическая работа №2. Анализ механизмов доверенной загрузки и контроля целостности.
Задание 1. Определить состав доверенной вычислительной среды и границы доверия.
Задание 2. Сравнить назначение UEFI Secure Boot, TPM и программных средств контроля целостности.
Задание 3. Выбрать объекты контроля и критерии обнаружения несанкционированных изменений.
Задание 4. Разработать сценарии штатной проверки и проверки после изменения контролируемого объекта.
Задание 5. Оценить возможные способы обхода контроля и предложить компенсирующие меры.

Практическая работа №3. Разработка схемы многофакторной аутентификации.
Задание 1. Проанализировать категории пользователей и защищаемые ресурсы.
Задание 2. Определить требования к факторам аутентификации для разных категорий доступа.
Задание 3. Разработать схему привязки токенов или сертификатов к учетным записям.
Задание 4. Описать сценарии выдачи, замены, блокировки и восстановления аутентификаторов.
Задание 5. Оформить регламент многофакторной аутентификации и обосновать выбранные решения.

Практическая работа №4. Организация жизненного цикла ключей.
Задание 1. Определить участников и операции жизненного цикла ключевой информации.
Задание 2. Разработать схему генерации, выдачи, хранения и использования ключей.
Задание 3. Определить порядок резервного копирования, смены и отзыва ключей.

Задание 4. Оценить риски компрометации ключевого материала на каждом этапе.
Задание 5. Сформировать организационные и технические меры снижения выявленных рисков.

Практическая работа №5. Проектирование межсетевого экранирования и защищенного соединения.
Задание 1. Проанализировать структуру сети и выделить защищаемые сегменты.
Задание 2. Разработать схему размещения межсетевого экрана и точек завершения защищенного соединения.
Задание 3. Сформировать минимально необходимый набор правил фильтрации.
Задание 4. Определить требования к аутентификации, шифрованию и журналированию соединения.
Задание 5. Оценить влияние предложенной схемы на доступность и производительность.

Практическая работа №6. Разработка политики защиты конечных точек и данных.
Задание 1. Определить защищаемые данные и категории пользователей рабочей станции.
Задание 2. Разработать правила разграничения доступа к файлам и параметрам системы.
Задание 3. Выбрать способ шифрования данных и порядок управления ключами восстановления.
Задание 4. Определить требования к резервному копированию и восстановлению защищенных данных.
Задание 5. Оформить политику защиты конечной точки и обосновать выбранные меры.

Практическая работа №7. Разработка регламента установки и обслуживания средства защиты.
Задание 1. Проанализировать системные требования и условия совместимости выбранного средства защиты.
Задание 2. Составить последовательность установки и первичной настройки.
Задание 3. Определить порядок резервного копирования конфигурации и обновления компонентов.
Задание 4. Разработать перечень контролируемых показателей работоспособности.
Задание 5. Оформить регламент обслуживания и форму журнала учета изменений.

Практическая работа №8. Разработка программы проверки эффективности комплекса средств защиты.
Задание 1. Определить цель, объект и границы проверки комплекса средств защиты.
Задание 2. Сформировать перечень проверяемых функций и критерии оценки результатов.
Задание 3. Разработать тестовые воздействия и определить ожидаемые реакции средств защиты.
Задание 4. Предусмотреть действия по восстановлению и откату при нештатной ситуации.
Задание 5. Оформить программу и методику проверки комплекса средств защиты.

8.2.2. Типовые задания для лабораторных работ

Лабораторная работа №1. Исследование состава программно-аппаратного комплекса защиты.
Цель работы: изучить состав программных, программно-аппаратных и технических средств защиты учебного объекта, определить их назначение, основные функции, параметры управления и источники диагностической информации, а также получить навыки документирования архитектуры комплекса защиты.

Задание 1. Получить исходные данные об учебном объекте защиты и доступных средствах защиты.

Задание 2. Выполнить инвентаризацию программных, программно-аппаратных и технических компонентов.
Задание 3. Определить назначение и основные функции каждого средства.
Задание 4. Проверить доступные параметры управления и источники диагностической информации.
Задание 5. Оформить схему комплекса защиты и результаты исследования.

Лабораторная работа №2. Настройка доверенной загрузки и проверка контроля целостности.
Цель работы: изучить механизмы доверенной загрузки и контроля целостности информационной системы, исследовать возможности UEFI, Secure Boot и TPM, а также получить практические навыки настройки и проверки целостности защищаемых объектов.

Задание 1. Исследовать параметры UEFI и доступные механизмы безопасной загрузки.
Задание 2. Проверить состояние Secure Boot и доступные сведения TPM.
Задание 3. Настроить контроль целостности выбранных файлов или конфигурационных объектов.
Задание 4. Изменить контролируемый объект и зафиксировать реакцию средства.
Задание 5. Восстановить исходное состояние и оформить результаты проверки.

Лабораторная работа №3. Настройка многофакторной аутентификации с использованием токена или его программной модели.
Цель работы: изучить принципы многофакторной аутентификации и использования криптографических аутентификаторов, получить навыки настройки учетных записей, сертификатов и токенов, а также проверки штатных и ошибочных сценариев аутентификации.

Задание 1. Создать учебные учетные записи и настроить требования к факторам аутентификации.
Задание 2. Подготовить ключевую пару и сертификат пользователя.
Задание 3. Настроить привязку сертификата или программной модели токена к учетной записи.
Задание 4. Проверить штатные и ошибочные сценарии входа, блокировки и восстановления доступа.
Задание 5. Зафиксировать результаты и сформулировать требования к учету аутентификаторов.

Лабораторная работа №4. Выполнение криптографических операций и работа с сертификатами.
Цель работы: изучить практическое применение криптографических механизмов для защиты информации, получить навыки формирования ключевой пары, работы с сертификатами, шифрования, расшифрования и электронной подписи, а также контроля целостности подписанных данных.

Задание 1. Сформировать ключевую пару и создать запрос на сертификат.
Задание 2. Получить сертификат и проверить его основные поля и срок действия.
Задание 3. Выполнить шифрование и расшифрование тестовых данных.
Задание 4. Сформировать электронную подпись и проверить ее после изменения исходных данных.
Задание 5. Оформить результаты и указать места безопасного хранения ключевого материала.

Лабораторная работа №5. Развертывание межсетевого экрана и защищенного сетевого соединения.

Цель работы: изучить принципы сетевой фильтрации и защиты соединений, получить практические навыки настройки межсетевого экрана, формирования правил доступа, организации защищенного соединения и анализа сетевых журналов.

Задание 1. Подготовить учебную схему из двух сетевых сегментов.
Задание 2. Настроить межсетевой экран и минимально необходимый набор правил фильтрации.
Задание 3. Настроить защищенное соединение между двумя узлами или сегментами.
Задание 4. Проверить разрешенный и запрещенный трафик и проанализировать журналы.
Задание 5. Зафиксировать результаты и оценить влияние конфигурации на доступность.

Лабораторная работа №6. Настройка защиты конечной точки и шифрования данных.
Цель работы: изучить основные механизмы защиты конечных устройств и данных, получить навыки разграничения доступа пользователей к защищаемой информации, создания зашифрованных хранилищ и проверки механизмов восстановления доступа.

Задание 1. Создать учебные учетные записи и настроить разграничение доступа к файлам.
Задание 2. Проверить доступ пользователей к защищаемым данным.
Задание 3. Создать зашифрованный контейнер или защищенный том.
Задание 4. Проверить доступ к данным при штатном и нештатном сценариях.
Задание 5. Выполнить резервирование параметров восстановления и оформить результаты.

Лабораторная работа №7. Установка и первичная настройка средства защиты.
Цель работы: получить практические навыки установки и первичной настройки средства защиты информации, изучить требования к его развертыванию, параметры администрирования, резервирования конфигурации и диагностики работы средства.

Задание 1. Проверить соответствие учебной системы требованиям выбранного средства защиты.
Задание 2. Выполнить установку или развертывание программной модели средства.
Задание 3. Настроить основные параметры и права администрирования.
Задание 4. Создать резервную копию конфигурации и проверить диагностические сообщения.
Задание 5. Оформить протокол установки и перечень параметров для дальнейшего обслуживания.

Лабораторная работа №8. Проверка работоспособности комплекса средств защиты.
Цель работы: получить навыки комплексной проверки работоспособности средств защиты информации, оценки их реакции на предусмотренные воздействия, анализа журналов и диагностических данных, а также восстановления работоспособности после нештатных ситуаций.

Задание 1. Подготовить учебный стенд и зафиксировать исходное состояние комплекса защиты.
Задание 2. Выполнить предусмотренные программой тестовые воздействия.
Задание 3. Собрать журналы, зафиксировать реакции средств защиты и выявленные отклонения.
Задание 4. Выполнить восстановление или откат после нештатного воздействия.
Задание 5. Оформить акт проверки с выводом о работоспособности комплекса.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *экзамен (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов и заданий для подготовки к экзамену

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Понятие и назначение программно-аппаратных средств защиты информации.
2. Место программно-аппаратных средств в комплексной системе защиты информации.
3. Классификация средств защиты по назначению и уровню применения.
4. Угрозы, учитываемые при выборе программно-аппаратных средств защиты.
5. Сравнение программных, аппаратных и программно-аппаратных средств защиты.
6. Понятие доверенной вычислительной среды.
7. Назначение аппаратного корня доверия.
8. Функции TPM в системе защиты информации.
9. Принципы безопасной и измеренной загрузки.
10. Методы контроля целостности программной среды.
11. Аппаратные идентификаторы, токены и смарт-карты.
12. Принципы многофакторной аутентификации.
13. Назначение и ограничения биометрических средств аутентификации.
14. Назначение аппаратных модулей безопасности HSM.
15. Аппаратные генераторы случайных чисел и требования к ним.
16. Средства защищенного хранения криптографических ключей.
17. Жизненный цикл ключевой информации.
18. Назначение криптографических шлюзов.
19. Программно-аппаратные межсетевые экраны и их функции.
20. Программно-аппаратные VPN-шлюзы и области их применения.
21. Системы обнаружения и предотвращения вторжений.
22. Средства защиты конечных точек и контроля приложений.
23. Шифрование носителей и защищенное хранение данных.
24. Средства контроля подключаемых устройств и каналов передачи данных.
25. Журналирование событий программно-аппаратных средств защиты.
26. Показатели надежности и отказоустойчивости средств защиты.
27. Влияние средств защиты на производительность информационной системы.
28. Совместимость программно-аппаратных средств с информационной инфраструктурой.
29. Методы контроля эффективности применяемых мер защиты.
30. Критерии выбора программно-аппаратного средства защиты для заданного объекта.

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

1. Этапы жизненного цикла программно-аппаратного средства защиты.
2. Подготовка исходных данных перед установкой средства защиты.
3. Анализ системных требований и совместимости средства защиты.
4. Использование технической и эксплуатационной документации при развертывании.
5. Порядок установки программных компонентов средства защиты.
6. Порядок подключения аппаратных компонентов средства защиты.
7. Первичная настройка учетных записей и ролей администраторов.
8. Принцип минимальных привилегий при администрировании средств защиты.
9. Формирование безопасной базовой конфигурации.
10. Настройка криптографических параметров и ключевого материала.
11. Интеграция средства защиты с сетевой инфраструктурой.
12. Интеграция средства защиты с каталогами пользователей и службами аутентификации.
13. Резервное копирование конфигурации средства защиты.
14. Восстановление конфигурации после сбоя.
15. Управление обновлениями и исправлениями безопасности.
16. Контроль версий программных компонентов и сигнатур.
17. Мониторинг состояния и производительности средства защиты.
18. Анализ журналов и диагностических сообщений.
19. Периодическая проверка работоспособности средства защиты.
20. Диагностика типовых неисправностей программно-аппаратных средств.
21. Действия администратора при отказе средства защиты.
22. Организация отказоустойчивости и резервирования.
23. Управление изменениями конфигурации средств защиты.
24. Инвентаризация и учет программно-аппаратных средств защиты.
25. Требования к защищенному удаленному администрированию.
26. Порядок проведения приемочных испытаний после установки.
27. Документирование настроек и результатов технического обслуживания.
28. Правила безопасной эксплуатации средства защиты пользователями.
29. Вывод средства защиты из эксплуатации.
30. Безопасное удаление ключей, конфигурации и служебных данных при списании.