Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

С.1.1.28 «Программно-аппаратные средства обеспечения информационной безопасности»

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
Специализация «Создание автоматизированных систем в защищенном исполнении»

форма обучения – очная
курс – 4, 5
семестр – 8, 9
зачетных единиц – 7, 3
часов в неделю – 7, 2
всего часов – 252, 108
в том числе:
лекции – 54, 18
лабораторные занятия – 72, 18
самостоятельная работа – 126, 72
зачет – 9 семестр
экзамен – 8 семестр
курсовой проект – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: *формирование* профессиональных навыков, связанных с эксплуатацией и обслуживанием программно-аппаратных средств защиты информации

Задачи изучения дисциплины: дать основы программно-аппаратных средств защиты информации; создать представления о принципах, методах и средствах выявления угроз безопасности автоматизированных систем; развитие способностей к логическому и алгоритмическому мышлению и осуществлению проверки защищенности объектов на соответствие требованиям нормативных документов.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» является дисциплиной базовой части профессионального цикла дисциплин ФГОС ВПО по специальности 10.05.03 "Информационная безопасность автоматизированных систем"

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» базируется на знаниях, полученных в рамках изучения следующих дисциплин: «Организация ЭВМ и вычислительных систем», «Сети и системы передачи информации», «Криптографические методы защиты информации».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15)

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25)

Студент должен **знать**:

- принципы функционирования, правила эксплуатации и обслуживания программно-аппаратных средств защиты информации

- современные средства и методы проведения контрольных проверок средств защиты информации
- аппаратно-программные средства диагностики систем защиты информации;
- порядок сертификации средств защиты информации

Студент должен **уметь**:

- проводить установку программно-аппаратных средств защиты информации, проверять их техническое состояние, проводить техническое обслуживание и текущий ремонт, устранение отказов и восстановление работоспособности;
- выбирать, строить и анализировать показатели защищенности программно-аппаратных средств защиты информации;
- проводить мониторинг защищенности автоматизированных систем
- проводить испытания средств защиты информации

Студент должен **владеть**:

- навыками технического обслуживания и настройки программно-аппаратных средств обеспечения информационной безопасности;
- навыками анализа эффективности использования программно-аппаратных средств защиты информации;
- инструментальными средствами мониторинга защищенности автоматизированных систем;
- методиками подтверждения соответствия средств защиты информации требованиям нормативных документов;

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7		8	9
8 семестр									
1	1-3	1	Основные понятия программно-аппаратной защиты информации	36/6	12/4		-		24
1	4-6	2	Идентификация пользователей КС-субъектов доступа к данным	36/8	10/6		-		26
2	7-9	3	Средства и методы ограничения доступа к файлам	60/6	10/4		24/2		26
2	10-13	4	Аппаратно-программные средства криптографической защиты информации	60/6	10/4		24/2		26
2	14-18	5	Методы и средства ограничения доступа к компонентам ЭВМ	60/6	12/4		24/2		24
9 семестр									
3	1-8	6	Управление криптографическими ключами	/6	8/4		6/2		24
3	9-12	7	Защита программ от несанкционированного копирования	/6	4/4		6/2		24
3	13-18	8	Защита программных средств от исследования	/2	6/2		6		24
Всего				360/46	72/32		90/14		198

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение

1	2	3	4	5
			8 семестр	
1	2	1	Предмет и задачи программно-аппаратной защиты информации	**1,3,4**
1	2	2	Основные понятия защиты информации	**1,2,5**
1	2	3	Уязвимость компьютерных систем.	
1	4	4	Политика безопасности в компьютерных системах. Оценка защищенности	**1,2,6**
1	2	5	Механизмы защиты	**1,3,8**
2	2	6	Идентификация и аутентификация пользователя. Основные понятия и концепции	**1,4,11**
2	2	7	Идентификация и аутентификация пользователя. Основные понятия и концепции. Типовые схемы.	**1,2,11**
2	2	8	Взаимная проверка подлинности пользователей	**1,2,3,11**
2	2	9	Протоколы идентификации с нулевой передачей знаний	**1,2,11**
2	2	10	Схема идентификации Гиллоу-Куискуотера	**1-2,7**
3	4	11	Защита информации в КС от несанкционированного доступа. Система разграничения доступа к информации в КС	**1-3**
3	2	12	Концепция построения систем разграничения доступа	**1-3**
3	2	13	Организация доступа к ресурсам КС	**1-3,8-11**
3	2	14	Обеспечение целостности и доступности информации в КС	**1,2,5**
4	2	15	Полностью контролируемые компьютерные системы	
4	2	16	Основные элементы и средства защиты от НСД	**1,2,6**
4	2	17	Системы защиты информации от несанкционированного доступа	**1,3,8**
4	2	18	Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру	**1,4,11**
4	2	19	Система защиты данных Crypton Sigma	**1,2,11**
5	4	20	Защита информации в ПЭВМ	**1,2,3,11**
5	4	21	Виды мероприятий по защите информации	**1,2,11**
5	4	22	Современные системы защиты ПЭВМ от несанкционированного доступа к информации	**1-2,7**
			9 семестр	
6	2	23	Управление криптографическими ключами. Генерация и хранение ключей	**1-3,8-11**
6	2	24	Управление криптографическими ключами. Распределение ключей	**1,2,5**
6	2	25	Протокол аутентификации и распределения ключей для симметричных криптосистем	
6	2	26	Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей	**1,2,6**
7	2	27	Методы, затрудняющие считывание и препятствующие использованию скопированной информации	**1,3,8**
7	2	28	Средства защиты ПО от копирования	**1,4,11**
8	2	29	Средства защиты ПО от исследования	**1,2,11**

8	2	30	Общая характеристика и классификация компьютерных вирусов и средств нейтрализации компьютерных вирусов	**1,2,3,11**
8	2	31	Классификация методов защиты от компьютерных вирусов	**1,2,11**
				1-2,7

6. Содержание коллоквиумов

Учебным планом не предусмотрены

7. Перечень практических занятий

№ темы	Всего часов	Наименование практической работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	**2**	**4**	**3**
3,5	**14**	Принцип функционирования программно-аппаратного комплекса «Соболь».	**1-3, 8**
3,5	**14**	Принцип функционирования программно-аппаратного комплекса «Аккорд».	**1-3, 8**
3,5	**16**	Принцип функционирования программно-аппаратного комплекса «SecretNet».	**1-3, 9**
3,4,5,6	**16**	Принцип функционирования программно-аппаратного комплекса «Криптон».	**1-3, 13**
7,8	**12**	Защита программного обеспечения от несанкционированного использования	**1-3, 14**

8. Перечень лабораторных работ

Учебным планом не предусмотрены

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	**2**	**3**	**4**
1-8	98	Работа с учебной литературой. Разбор вопросов по теме занятия. Работа с источниками и поиск информаций в Интернете. Подготовка устного доклада. Подготовка к самостоятельной проверочной работе.	1-16
6-8	50	Подготовка к зачету	
1-5	50	Подготовка к экзамену	

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [15,16]

10. Расчетно-графическая работа

Учебным планом не предусмотрена

11. Курсовая работа

Учебным планом не предусмотрена

12. Курсовой проект

Темы курсовых

1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.
2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
3. Анализ методов и средств анализа защищенности беспроводных сетей.
4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
5. Виброакустические средства современных систем обеспечения информационной безопасности.
6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
8. Средства обеспечения информационной безопасности банков данных.
9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.
11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.
13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.
15. Инструментальные средства анализа рисков информационной безопасности.
16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Профессиональные компетенции, знания, навыки и умения оцениваются в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем»

В процессе освоения дисциплины осуществляется формирование следующих компетенций:

ПК-13: способностью участвовать в проектировании средств защиты информации автоматизированной системы

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: принципы функционирования, правила эксплуатации и обслуживания программно-аппаратных средств защиты информации	Лекции, практические занятия, самостоятельная работа	Тестирование, зачет, экзамен
Умеет: проводить установку программно-аппаратных средств защиты информации, проверять их техническое состояние, проводить техническое обслуживание и текущий ремонт, устранение отказов и восстановление работоспособности;	Лекции, практические занятия, самостоятельная работа	Тестирование рефераты
Владеет: навыками технического обслуживания и настройки программно-аппаратных средств обеспечения информационной безопасности	Лекции, практические занятия, самостоятельная работа, курсовой проект.	Отчеты по лабораторным работам, отчет по курсовому проекту.

ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации ;

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: современные средства и методы проведения контрольных проверок средств защиты информации	Лекции, практические занятия, самостоятельная работа	Тестирование, зачет, экзамен
Умеет: выбирать, строить и анализировать показатели защищенности программно-аппаратных средств защиты информации;	Лекции, практические занятия, самостоятельная работа	Тестирование рефераты
Владеет: навыками работы с информационно-образовательной средой СГТУ;	Лекции, практические занятия, самостоятельная работа, курсовой проект.	Отчеты по лабораторным работам, отчет по курсовому проекту.

ПК-15: способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: аппаратно-программные средства диагностики систем защиты информации;	Лекции, практические занятия, самостоятельная работа	Тестирование, зачет, экзамен
Умеет:	Лекции, практические	Тестирование

проводить мониторинг защищенности автоматизированных систем	занятия, самостоятельная работа	рефераты
Владеет: навыками анализа эффективности использования программно-аппаратных средств защиты информации;	Лекции, практические занятия, самостоятельная работа, курсовой проект.	Отчеты по лабораторным работам, отчет по курсовому проекту.

ПК-25: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: порядок сертификации средств защиты информации	Лекции, практические занятия, самостоятельная работа	Тестирование, зачет, экзамен
Умеет: проводить испытания средств защиты информации	Лекции, практические занятия, самостоятельная работа	Тестирование рефераты
Владеет: методиками подтверждения соответствия средств защиты информации требованиям нормативных документов;	Лекции, практические занятия, самостоятельная работа, курсовой проект.	Отчеты по лабораторным работам, отчет по курсовому проекту.

При выставлении экзаменационных оценок предлагается руководствоваться следующим:

оценки «отлично» заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой.

оценки «хорошо» заслуживает студент, показавший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания.

оценки «удовлетворительно» заслуживает студент, показавший знание учебно-программного материала в объеме, необходимом для дальнейшей учебы и профессиональной деятельности.

оценки «неудовлетворительно» заслуживает студент, показавший пробелы в знаниях основного учебно-программного материала, допустивший принципиальные ошибки в выполнении предусмотренных программой заданий.

: Вопросы для зачета

1.Основные понятия программно-аппаратной защиты информации.

2. Способы идентификации и аутентификации субъектов КС.

3. Способы НСД к информации и защиты от него в компьютерных системах.

4. Методы противодействия динамическим способам снятия защиты программ от

копирования.

5. Методы защиты программ от исследования.

6. Подходы к задаче защиты от копирования программ.

7. Общая характеристика и классификация компьютерных вирусов.

8. Общая характеристика средств нейтрализации компьютерных вирусов.

9. Защита на уровне загрузчиков операционной среды.

10. Архитектура подсистемы безопасности ОС Windows.

11. Разграничение прав пользователей в ОС Windows.

12. Аудит событий безопасности в ОС Windows.

13. Домены безопасности.

14. Микроядерная архитектура с точки зрения создания защищенных операционных

систем.

15. Аутентификация пользователей при локальном и удаленном доступе к КС.

16. Средства обеспечения целостности и конфиденциальности при передаче

информации по каналам связи.

17. Технология и классификация VPN.

18. Требования к межсетевым экранам.

19. Методы поиска уязвимостей.

20. Симметричные и асимметричные алгоритмы шифрования информации.

21. Функции удостоверяющего центра.

22. Структура удостоверяющего центра.

23. Концепция иерархии ключей.

24. Генерация и хранение ключей.

25. Распределение ключей.

Вопросы для экзамена

1.Использование программно-аппаратных средств для защиты информации.

2. Дискретное, мандатное и ролевое разграничение доступа к объектам КС.

3. Способы идентификации и аутентификации субъектов КС.

4. Способы фиксации фактов доступа к файлам. Журналы доступа.

5. Способы защиты информации на съемных дисках.

6. Основные схемы резервного копирования.

7. Программные закладки и их воздействие на компьютеры.

8. Защита данных от разрушающих программных воздействий.

9. Формирование и поддержка замкнутой программной среды.

10. Классификация средств исследования программ.

11. Методы и средства защиты от несанкционированного копирования.

12. Юридические аспекты несанкционированного копирования программ.

13. Защита массивов информации от изменения.

14. Формирование хеш-функций, требования к построению и способы реализации.

15. Формальные модели безопасности ОС.

16. Реализация механизмов безопасности на аппаратном уровне.

17. Архитектура подсистемы безопасности ОС Windows.

18. Создание защищенной операционной системы.

19. Аутентификация пользователей при локальном и удаленном доступе к КС.

20. Понятие и классификация межсетевых экранов.

21. Технология и классификация VPN.

22. Принцип работы систем обнаружения вторжений.

23. Анализ защищенности системы при помощи сканера безопасности.

24. Взаимная проверка подлинности пользователей.

25. Программно-аппаратные средства криптографической защиты информации.

26. Требования, предъявляемые к удостоверяющему центру.

27. Протокол аутентификации и распределения ключей для симметричных

криптосистем.

28. Протокол для асимметричных криптосистем с использованием сертификатов

открытых ключей.

29. Атаки и методы защиты на уровне СУБД.

30. Модели безопасности, применяемые при построении защиты в СУБД.

18

31. Транзакция и восстановление.

32. Технологии тиражирования и синхронизации данных

33. Кластерная организация серверов баз данных.

34. Концепция защиты от НСД к информации.

35. Модель нарушителя при локальном НСД.

36. Модель нарушителя при удаленном НСД.

37. Этапы разработки модели угроз.

38. Стандарты безопасности и их роль.

39. Порядок сертификации средств защиты информации.

40. Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности

14. Образовательные технологии

Изучение курса «Программно-аппаратные средства защиты информации» предусматривает использование компьютеров с доступом в Интернет. При помощи компьютеров, в частности, осуществляется доступ к

ресурсам электронной библиотеки СГТУ им. Гагарина Ю.А., каталога и электронного читального зала библиотеки.

Выполнение практических работ предусматривает использование компьютерных классов с возможностью администрирования программно - аппаратных комплексов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

а) основная литература:

1. Мартемьянов Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности [Электронный ресурс]: учебное пособие/ Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 332 с.— Режим доступа: http://www.iprbookshop.ru/12009.— ЭБС «IPRbooks», по паролю
2. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - М. : ИЦ "Академия", 2006. - 240 с. ISBN 5-7695-2706-4 Экземпляры всего: 19
3. Хорев П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - 4-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. ISBN 978-5-7695-5118-5 Экземпляры всего: 18
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

б) дополнительная литература:

5. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Креопалов В.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871.— ЭБС «IPRbooks», по паролю
6. Куприянов А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с ISBN 978-5-7695-5761-3 Экземпляры всего: 22
7. Мельников В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : ИЦ "Академия", 2006. - 336 с. ISBN 5-7695-2592-4 Экземпляры всего: 13
8. Одинцов А. А. Экономическая и информационная безопасность предпринимательства : учеб. пособие / А. А. Одинцов. - 2-е изд., испр. и доп. - М. : ИЦ "Академия", 2008. - 336 с. ISBN 978-5-7695-5001-0 Экземпляры всего: 20
9. Пластун И. Л. Технология построения защищенных автоматизированных систем и сетей : учеб. пособие для студ. спец.

075500, 220400 / И. Л. Пластун; М-во образования и науки Рос. Федерации, Саратовский гос. техн. ун-т. - Саратов : СГТУ, 2010. - 96 с. ISBN 978-5-7433-2232-9 Экземпляры всего: 40

в) периодические издания

10. Информационная безопасность регионов [Текст] : науч.-техн. журнал. - Саратов : Изд-во СГСЭУ, 2007 - . - Выходит раз в три месяца. - ISSN 1995-5731 http://elibrary.ru/title_about.asp?id=28126

в)Интернет-ресурсы

11. Код безопасности. Режим доступа: http://www.securitycode.ru/ Дата обращения 05.05.2015
12. ОКБ САПР. Режим доступа http://www.accord.ru/ Дата обращения 05.05.2015
13. ООО Фирма «АНКАД» . Режим доступа http://ancud.ru/crtk.html/ Дата обращения 05.05.2015
14. Интернет портал ISO27000.RU . Искусство управления информационной безопасностью. Режим доступа http://www.iso27000.ru/ Дата обращения 05.05.2015

ИСТОЧНИКИ ИОС

15. https://portal.sstu.ru/Fakult/FETIP/IBS/c3114/default.aspx (ИОС СГТУ)
16. https://portal.sstu.ru/Fakult/FETIP/IBS/c3114_9/default.aspx (ИОС СГТУ)

16. Материально-техническое обеспечение

Для проведения лекционных занятий необходима лекционная аудитория с компьютеризированным рабочее место преподавателя, мультимедийный проектор, подключенный к рабочему месту преподавателя или интерактивная доска.

Для проведения лабораторных занятий необходима учебно-научная специализированная лаборатория с достаточным количеством компьютеризированных рабочих мест, с возможностью администрирования программно -аппаратных комплексов.