Приложение 1

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ОДОБРЕНО:
Методичесской комиссией по укрупненным группам специальностей и направлению подготовки 10.00.00- «Информационная безопасность»
Председатель МК
подпись Мелехин В.Б.
ИОФ

УТВЕРЖДАЮ:
Декан, председатель совета факультета Компьютерных технологий, вычислительной техники и энергетики
подпись **Ш.А.Юсуфов**
ИОФ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Программно-аппаратные средства обеспечения ИБ» для контроля знаний обучающихся по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Составитель _____ Г.И.Качаева
подпись ИОФ

Фонд оценочных средств обсужден на заседании выпускающей кафедры ИБ «17.12.2018» от года, протокол №4

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.Б.30 Программно-аппаратные средства обеспечения ИБ

Зав. кафедрой _____ Г.И.Качаева
подпись ИОФ

Махачкала 2018

Введение

Для проверки знаний составляющей компетенций, формируемых в рамках дисциплины «Программно-аппаратные средства обеспечения ИБ» в фонде оценочных средств предусмотрены:

– вопросы для устного собеседования(опроса).

Для проверки деятельностной составляющей компетенций, формируемых в рамках дисциплины «Программно-аппаратные средства обеспечения ИБ» в фонде оценочных средств размещены:

– профессионально-ориентированные задания.

Конкретные задания, выносимые для проведения текущего контроля и промежуточную аттестации по дисциплине, представлены в отдельном документе «Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине», прилагаемом к рабочей программе.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, на освоение которых направлено изучение дисциплины «Программно-аппаратные средства обеспечения ИБ», с указанием этапов их формирования в процессе освоения образовательной программы:

- ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;
- ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы.

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

Показатели и критерии оценивания компетенций, используемые шкалы оценивания

Элементы компетенций (знания, умения, владения)	Показатели оценивания	Критерии оценивания	Средства оценивания	Шкалы оценивания
Знать (ПК-10)	**Знание:** программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; типовые архитектуры и принципы построения современных защищенных	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация:	Шкала 1

	информационных систем		Экзамен.	
Уметь (ПК-10)	**Умение**: проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Экзамен.	Шкала 1
Владеть (ПК-10)	**Владение**: навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Экзамен.	Шкала 2
Знать (ПК-25)	Знание: правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Экзамен.	Шкала 1
Уметь (ПК-25)	**Умение**: типовые архитектуры и принципы построения современных защищенных информационных систем; угрозы и атаки, характерные для распределенных информационных систем	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация:	Шкала 1

			Экзамен.	
Владеть (ПК-25)	**Владение:** - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Экзамен.	Шкала 2
Знать (ПК-26)	**Знание:** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Экзамен.	Шкала 1
Уметь (ПК-26)	**Умение:** -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях; - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Экзамен.	Шкала 1

	конфиденциальной информации.			
Владеть (ПК-26)	**Владение**: - поиска наиболее эффективных путей обработки информации; -мстодами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Экзамен.	Шкала 2

Описание шкал оценивания степени сформированности элементов компетенций

Шкала 1.Оценка сформированности отдельных элементов компетенций

Обозначения		**Формулировка требований к степени сформированности компетенции**		
Цифр.	Оценка	**Знать**	**Уметь**	**Владеть**
1	Неуд.	Отсутствие знаний	Отсутствие умений	Отсутствие навыков
2	Неуд.	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Удовл.	Общие, но не структурированные знания	В целом успешное, но не систематически осуществляемое умение	В целом успешное, но не систематическое применение
4	Хор.	Сформированные, но содержащие отдельные пробелы знания	В целом успешное, но содержащие отдельные пробелы умение	В целом успешное, но содержащее отдельные пробелы применение навыков
5	Отл.	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

Шкала 2. Комплексная оценка сформированности знаний, умений и владений

Обозначения	**Формулировка требований к степени сформированности**

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

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Типовые вопросы и задания для текущего контроля(оценка сформированности элементов (знаний, умений) компетенций в рамках текущего контроля по дисциплине) по разделам дисциплины

Примеры вопросов по разделу 1-5:

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Защита лабораторных работ (оценка сформированности элементов (знаний, умений) компетенций в рамках текущего контроля по дисциплине) по разделам дисциплины:

Примеры вопросов при защите лабораторной работы №1

1. Методы криптографического преобразования данных.
2. Электронная цифровая подпись.
3. Проблемы реализации методов криптографической защиты в информационных системах.
4. Характеристики криптографических средств защиты информации. Криптография и гипотеза PNP.
5. Односторонние функции.
6. Псевдослучайные генераторы.
7. Доказательства с нулевым разглашением.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Процедуры и средства оценивания элементов компетенций по дисциплине «Программно-аппаратная защита информации».

Процедура проведения	**Средство оценивания**				
	Текущий контроль				Промежуточный контроль
	Выполнение устных заданий	Выполнение письменных заданий	Выполнение практических заданий	Защита лабораторных работ	Экзамен
Продолжительность контроля	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	В соответствии с принятыми нормами времени
Форма проведения контроля	Устный опрос	Письменный опрос	Письменный опрос	Устная защита	В письменной форме
Вид проверочного задания	Устные вопросы	Письменные задания	Практические задания	Устные вопросы	экзаменационный билет
Форма отчета	Устные ответы	Ответы в письменной форме	Ответы в письменной форме	Ответы в устной форме	Ответы в письменной форме
Раздаточный материал	Нет	Справочная литература	Справочная литература	Справочная литература	Справочная литература

Методические указания для обучающихся по освоению дисциплины

Дисциплина «Программно-аппаратная защита информации» предусматривает лекции раз в неделю, лабораторные раз в две недели и практические занятия раз в неделю. Изучение дисциплины завершается зачетом. Успешное изучение дисциплины требует посещения лекций, активной работы на практических занятиях, выполнения учебных заданий преподавателя, ознакомления с основной и дополнительной литературой, нормативными правовыми актами и нормативными документами.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

При подготовке к лекционным занятиям студентам необходимо:

перед очередной лекцией необходимо просмотреть по конспект материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

При подготовке к практическому занятию студенты имеют возможность воспользоваться консультациями преподавателя.

При подготовке к практическим занятиям студентам необходимо:

приносить с собой рекомендованную преподавателем литературу к конкретному занятию;

до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно- правовые акты и материалы правоприменительной практики;

теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;

в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

в ходе семинара давать конкретные, четкие ответы по существу вопросов;

на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

4. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа №1

10. Программное обеспечение для моделирования сетей передачи данных.
11. Эмулятор GNS3.
12. Основы работы и моделирование простых схем.
13. Протоколы удаленного доступа. Протоколы telnet, ssh.
14. Обеспечение безопасности при передаче данных по сети.
15. Сравнительный анализ.
16. Протокол настройки времени.
17. Динамическая IP-маршрутизация.
18. Внутренние протоколы маршрутизации.
19. Пограничный шлюзовой протокол маршрутизации.
20. Протоколы RIP, IGRP и EIGRP.
21. Протокол динамической маршрутизации OSPF.
22. Атака типа «Отказ в обслуживании» (DoS-атака).
23. Механизмы защиты от некоторых типов DoS-атак.
24. Антиспуфинг. Защита от IP-спуфинга.
25. Защита от ARP-спуфинга.
26. Защита внутреннего периметра сети передачи данных.

Аттестационная контрольная работа №2

1. Атака типа «Отказ в обслуживании» (DoS-атака).
2. Механизмы защиты от некоторых типов DoS-атак.
3. Антиспуфинг.
4. Защита от IP-спуфинга.
5. Защита от ARP-спуфинга.
6. Защита внутреннего периметра сети передачи данных
7. Сегментация сетей п-ередачи данных.
8. Технология VLAN.
9. Передача трафика между VLAN.
10. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней.
11. Технологии VTP-сервер и Port-security.
12. Фильтрация трафика.
1. Изучение технологии ACL (AccessControlList).
2. Типы ACL.

3. Создание списков доступа.
4. Общие принципы VirtualPrivateNetwork (VPN).
5. Сравнительный анализ протоколов VPN.
6. Настройка VPN соединения через протокол GRE.
7. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
8. Применение SSLVPN
9. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.

Аттестационная контрольная работа №3

1. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
2. Применение SSLVPN
3. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
4. Основы работы в ОС семейства Linux.
5. Управление правами доступа.
6. Администрирование пользователей.
7. Управление файлами и каталогами.
8. Ссылки.
9. Архивирование и резервное копирование системы.
10. Восстановление системы после критических сбоев из архивов.
11. Администрирование БД MSSQL.
12. Управление правами доступа.
13. Архивирование и восстановление БД.
14. Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных.
15. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.
16. Административные меры обеспечения комплексной безопасности в информационных системах

Перечень вопросов на экзамен

1. Программное обеспечение для моделирования сетей передачи данных.
2. Эмулятор GNS3.
3. Основы работы и моделирование простых схем.
4. Протоколы удаленного доступа. Протоколы telnet, ssh.
5. Обеспечение безопасности при передаче данных по сети.
6. Сравнительный анализ.
7. Протокол настройки времени.
8. Динамическая IP-маршрутизация.
9. Внутренние протоколы маршрутизации.
10. Пограничный шлюзовой протокол маршрутизации.
11. Протоколы RIP, IGRP и EIGRP.
12. Протокол динамической маршрутизации OSPF.
13. Атака типа «Отказ в обслуживании» (DoS-атака).
14. Механизмы защиты от некоторых типов DoS-атак.
15. Антиспуфинг. Защита от IP-спуфинга.
16. Защита от ARP-спуфинга.
17. Защита внутреннего периметра сети передачи данных.
18. Атака типа «Отказ в обслуживании» (DoS-атака).
19. Механизмы защиты от некоторых типов DoS-атак.
20. Антиспуфинг.
21. Защита от IP-спуфинга.
22. Защита от ARP-спуфинга.
23. Защита внутреннего периметра сети передачи данных

24. Сегментация сетей передачи данных.
25. Технология VLAN.
26. Передача трафика между VLAN.
27. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней.
28. Технологии VTP-сервер и Port-security.
29. Фильтрация трафика.
30. Изучение технологии ACL (AccessControlList).
31. Типы ACL.
32. Создание списков доступа.
33. Общие принципы VirtualPrivateNetwork (VPN).
34. Сравнительный анализ протоколов VPN.
35. Настройка VPN соединения через протокол GRE.
36. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
37. Применение SSLVPN
38. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
39. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
40. Применение SSLVPN
41. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
42. Основы работы в ОС семейства Linux.
43. Управление правами доступа.
44. Администрирование пользователей.
45. Управление файлами и каталогами.
46. Ссылки.
47. Архивирование и резервное копирование системы.
48. Восстановление системы после критических сбоев из архивов.
49. Администрирование БД MSSQL.
50. Управление правами доступа.
51. Архивирование и восстановление БД.
52. Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных.
53. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.
54. Административные меры обеспечения комплексной безопасности в информационных системах.

.

Вопросы проверки остаточных знаний

1. Угрозы безопасности компьютерных систем.
2. Противодействие угрозам безопасности.
3. Защита компьютерной системы от взлома.
4. Модель КС.
5. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.
6. Реализация механизмов безопасности на аппаратном уровне Безопасность компьютерной сети.
7. Защита от анализаторов протоколов.
8. Технология защиты информации на основе смарт-карт.
9. Состав комплекса «Аккорд».
10. Принцип работы комплекса «Аккорд».
11. Механизм замкнутой программной среды Secret Net.

Учебно-методическое и информационное обеспечение дисциплины (модуля) «Программно-аппаратные средства обеспечения ИБ»

Рекомендуемая литература и источники информации

№	Виды занятий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк, лб, срс	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс]: учебно-методическое пособие	Фомин Д.В.	Саратов: Вузовское образование, 2018.— 218 с.	http://www.iprbookshop.ru/77317.html	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс]: учебно-методическое пособие	Помешкин А.А., Коротких И.В.	Новосибирск: Новосибирский государственный технический университет, 2012.— 47 с	http://www.iprbookshop.ru/45015.html	
4.	Лк, пр, срс	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие	Прокушев Я.Е.	Санкт-Петербург: Интермедия, 2017.— 160 с.	http://www.iprbookshop.ru/66799.html	
5.	Лк, пр, срс	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность»	Л.Х. Мифтахова [и др.].	Санкт-Петербург: Интермедия, 2018.— 408 с.	http://www.iprbookshop.ru/73644.html	
6.	Лк, пр, срс	Программно-аппаратные средства защиты информационных систем [Электронный ресурс]: учебное пособие	Ю.Ю. Громов [и др.].	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017.— 193 с.	http://www.iprbookshop.ru/85968.html	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
7.	Лк, лб, срс	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание	А.И. Астайкин [и др.]	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 с.	http://www.iprbookshop.ru/60959.html.	

8.	Лк, лб, срс	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс]		Москва: Московский технический университет связи и информатики, 2016.— 31 c.	http://www.iprbookshop.ru/61529.html
9.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета			
10.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека			
11.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.			