ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утвержден решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

Форма обучения – очная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00DDAA21EB96DCD5ECDD494784A037C099
Владелец: Бучаев Ахмед Гамидович
Действителен: с 28.04.2023 до 21.07.2024

.

Махачкала – 2023

УДК 681.518(075.8)

ББК 32.81.73

Составитель – Эмирбеков Эльдар Меликович, старший преподаватель кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

*Фонд оценочных средств по междисциплинарному курсу «*Программно-аппаратные средства защиты информации*» разработаны в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».*

Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2023 г. – 44 с.

Рекомендован к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендован к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрен на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

СОДЕРЖАНИЕ

Назначение оценочных материалов

Фонд оценочных средств для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по междисциплинарному курсу) обучающихся по междисциплинарному курсу «Программно-аппаратные средства защиты информации» на соответствие их учебных достижений поэтапным требованиям образовательной программы 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Фонд оценочных средств по междисциплинарному курсу «Программно-аппаратные средства защиты информации» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.
-

РАЗДЕЛ 1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ВИДОВ ОЦЕНОЧНЫХ СРЕДСТВ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Планируемые результаты обучения по междисциплинарному курсу, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие	**Знать:** – виды и назначение программно-аппаратных средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает – виды и назначение программно-аппаратных средств защиты информации	**Блок А** –задания репродуктивного уровня – вопросы для обсуждения
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает – виды	

			и назначение программно-аппаратных средств защиты информации	
		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает – виды и назначение программно-аппаратных средств защиты информации	
	Уметь: - грамотно использовать аппаратные средства защиты при решении практических задач	Пороговый уровень	Обучающийся слабо (частично) умеет грамотно использовать аппаратные средства защиты при решении практических задач	**Блок В** – задания реконструктивного уровня – Лабораторные работы;
		Базовый уровень	Обучающийся с незначительными затруднениями умеет грамотно использовать аппаратные средства защиты при решении практических задач	
		Продвинутый уровень	Обучающийся умеет грамотно использовать аппаратные средства защиты при решении практических задач	
	Владеть: - применения наиболее эффективных методов и средств программно-аппаратной защиты информации	Пороговый уровень	Обучающийся слабо (частично) владеет применения наиболее эффективных методов и средств программно-аппаратной защиты информации	**Блок С** – задания практико-ориентированного уровня Лабораторные работы
		Базовый уровень	Обучающийся с небольшими затруднениями применения наиболее эффективных методов и средств программно-аппаратной защиты информации	
		Продвинутый уровень	Обучающийся свободно владеет применения наиболее эффективных методов и средств программно-аппаратной защиты информации	

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации ПК 2.5.Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств ПК	**Знать:** – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	**Блок А** –задания репродуктивного уровня – вопросы для обсуждения
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	
		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	
	Уметь: – осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	Пороговый уровень	Обучающийся слабо (частично) знает – осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	**Блок В** – задания реконструктивного уровня – Лабораторные работы;
		Базовый уровень	Обучающийся с незначительными затруднениями умеет осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных	

2.6.Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак			средств защиты	**Блок С** – задания практико-ориентированного уровня Лабораторные работы
		Продвинутый уровень	Обучающийся умеет осуществлять проверку работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
	Владеть: – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	Пороговый уровень	Обучающийся слабо (частично) владеет – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
		Базовый уровень	Обучающийся с небольшими затруднениями – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
		Продвинутый уровень	Обучающийся свободно владеет – навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по междисциплинарному курсу

Для проверки сформированности компетенции ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для обсуждения

1. Понятия: информация, информатизация, информационные технологии, информационные ресурсы.
2. Понятие программно-аппаратной защиты информации.
3. Задачи программно-аппаратной защиты информации.
4. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Лабораторная работа
Лабораторная работа № 1.
Тема: «Политика безопасности в компьютерных системах**»**
Цель работы: Ознакомиться с презентацией "Аппаратные средства и оборудование ЛВС"
Задание для работы:
1. Основные процессы жизненного цикла АС.
2. Оценка защищенности КС.
3. Взаимосвязь между стандартными процессами и стадиями.

Лабораторная работа №2
Тема: «Основные понятия и концепции**»**
Цель работы: Пробрести навыки и освоить основные методы тестирования аппаратных средств ПК с помощью тестовых программ
Задание для работы:
1. Идентификация объекта
2. Защита при обмене сообщениями

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторная работа

Практико-ориентированная лабораторная работа: «Механизмы защиты»
Задание для работы:
1. Список контроля доступа
Краткое описание:
1. Функциональное построение СЗИ организации и назначение основных подразделений.
2. Элементарные модели СЗИ организации. Семирубежная модель защиты.
Результаты и выводы: В ходе работы, студент научился разбираться и оперировать основными понятиями информационной безопасности.

Для проверки сформированности компетенции
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
репродуктивного уровня («знать»)

.

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для обсуждения

1. Виды и источники угроз информационной безопасности РФ.
2. Классификация программно-аппаратных средств защиты информации
3. Структура государственной системы обеспечения информационной безопасности РФ.
4. Правовое регулирование информационной сферы в РФ.
5. Основные нормативно-методические материалы.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Лабораторная работа
Тема: «Нормативно-методическое обеспечение создания АС**»** 37
Цель работы: исследование состава аппаратных и программных средств персонального компьютера (ПК), составляющих основу его конфигурации
Задание для работы:
1. Нормативно-методическое обеспечение АС.
2. Международные стандарты.
3. Стандарты Российской Федерации.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторная работа

1. Идентификация, аутентификация и авторизация субъектов и объектов системы
Краткое описание:

1. Последовательность и содержание основных этапов проектирования СЗИ организации.
2. Содержание процесса эксплуатации СЗИ организации.

Результаты и выводы: В ходе работы, студент научился разбираться и оперировать основными понятиями информационной безопасности.

Для проверки сформированности компетенции
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
Блок А. Задания репродуктивного уровня («знать»)

А1 Тестовые задания

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2. Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3. Атакой на КС называют:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

1. Искусственные угрозы исходя из их мотивов разделяются на:

a) непреднамеренные и преднамеренные

b) косвенные и непосредственные

c) несанкционированные и санкционированные

2. К непреднамеренным угрозам относятся:

a) ошибки в разработке программных средств КС

b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

3. К умышленным угрозам относятся:

a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

c) ошибки пользователей КС;

4. Косвенными каналами утечки называют:

a) каналы, не связанные с физическим доступом к элементам КС

b) каналы, связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

5. К косвенным каналам утечки информации относятся:

a) использование подслушивающих (радиозакладных) устройств;

b) маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);

c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

6. Непосредственными каналами утечки называют:

a) каналы, связанные с физическим доступом к элементам КС.

b) каналы, не связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

7. К непосредственным каналам утески информации относятся:

a) обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

b) перехват побочных электромагнитных излучений и наводок (ПЭМИН).

c) дистанционное видеонаблюдение;

Блок B. Задания реконструктивного уровня («уметь»)

B1. Тематика рефератов и презентаций

1. Основные подходы к защите данных от НСД
2. Организация доступа к файлам
3. Фиксация доступа к файлам
4. Доступ к данным со стороны процесса
5. Особенности защиты данных от изменения

Блок C. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

C1. Лабораторные работы

Лабораторная работа «Средства обеспечения безопасности ОС Windows»

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1. ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы: Научиться конфигурированию межсетевого экрана D-link DFL-800T для приобретения навыков защиты локальной вычислительной сети предприятия от угроз информационной безопасности со стороны пользователей глобальной сети Интернет

ЛАБОРАТОРНАЯ РАБОТА №2. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Изучить порядок настройки беспроводной точки доступа и организации беспроводных сетей по технологии Wi-Fi.

Для проверки сформированности компетенции
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации

1. Избирательная политика безопасности подразумевает, что:

a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

b) все субъекты и объекты системы должны быть однозначно идентифицированы;

c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

2. Полномочная политика безопасности подразумевает, что:

a) каждому субъекту системы присвоен уровень прозрачности (securityclearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

b) все субъекты и объекты системы должны быть идентифицированы;

c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

3. Достоверная вычислительная база - это:

a) абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

b) активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.

c) пассивный компонент системы, хранящий, принимающий или передающий информацию.

4. Достоверная вычислительная база выполняет задачи:

a) поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты

b) функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности)

c) представляет собой некоторый соответствующую проверку, организационных мер набор требований, прошедших реализуемых при помощи

5. Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

6. Идентификация объекта - это:

a) одна из функций подсистемы защиты.

b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи.

c) сфера действий пользователя и доступные ему ресурсы КС

7. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

a) авторизацией

b) аутентификацией

c) Идентификация

8. Авторизация - это:

a) предоставлением полномочий

b) подтверждение подлинности

c) цифровая подпись

9. Аутентификация – это:

a) подтверждение подлинности

b) предоставлением полномочий

c) цифровая подпись

10. Биометрическая идентификация и аутентификация пользователя это:

a) идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

b) схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

c) схема идентификации с нулевой передачей знаний.

11. Для чего используется процедура «рукопожатия»:

a) для взаимной проверки подлинности

b) для распределения ключей между подлинными партнерами

c) для безопасного использования интеллектуальных карт

12. Параллельная схема идентификации позволяет увеличить:

a) число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

b) регистрацию времени для каждого сообщения

c) объект-эталон для идентификации и аутентификации пользователей

13. Внешняя и внутренняя формы представления аутентифицирующего объекта
должны быть:

a) семантически тождественны

b) модифицированы

c) структурированы

14. Для чего были разработаны протоколы идентификации с нулевой передачей
знаний:

a) для безопасного использования интеллектуальных карт

b) для взаимной проверки подлинности

c) для распределения ключей между подлинными партнерами

15. Механизм запроса-ответа используется для:

a) проверки подлинности

b) шифрования

c) регистрации времени для каждого сообщения

16. Кто разработал алгоритм идентификации с нулевой передачей знания:

a) Гиллоу и Ж. Куискуотером

b) У. Фейге

c) А. Фиат и А. Шамир

17. Схему идентификации с нулевой передачей знаний предложили:

a) У. Фейге, А. Фиат и А. Шамир

b) Гиллоу и Ж. Куискуотером

c) А. Фиат и А. Шамир

18. Для чего создается система разграничения доступа к информации:

a) для защиты информации от НСД

b) для осуществления НСДИ

c) определения максимального уровня конфиденциальности документа

19. Какие методы организации разграничения доступа используются в КС:

a) матричный

b) структурированный
c) метод Гиллоу-Куискуотера

20. Мандатный метод основывается на:
a) многоуровневой модели защиты
b) использование матриц доступа
c) криптографическом преобразовании

21. Какой из функциональных блоков должна содержать система разграничения доступа к информации:
a) блок криптографического преобразования информации при ее хранении и передаче;
b) блок контроля среды размещения
c) блок контроля среды выполнения.

22. Диспетчер доступа реализуется в виде:
a) аппаратно-программных механизмов
b) аппаратных механизмов
c) программных механизмов

23. Под ядром безопасности понимают:
a) локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.
b) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
c) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

24. Главным условием создания ядра безопасности является:
a) обеспечение многоуровневого режима выполнения команд
b) мандатное управление
c) Матричная структура

25. Под организацией доступа к ресурсам понимается
a) весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.
b) хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.
c) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние

26. При эксплуатации механизмов аутентификации основными задачами являются:

a) генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.

b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;

c) реализация механизма виртуальной памяти с разделением адресных пространств;

27. В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа,не содержатся все категории, определенные для данного документа.

28. Правильность функционирования ядра безопасности доказывается путем:

a) полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.

b) использования дополнительных программных или аппаратно-программных средств.

c) использования строго определенного множества программ.

29. Матричное управление доступом предполагает использование:

a) матриц доступа

b) аппаратно-программных механизмов

c) субъекта допуска

30. Основной проблемой создания высокоэффективной защиты от НСД является

a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.

b) использования дополнительных программных или аппаратно-программных средств.

c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

21. Аппаратно-программмные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

c) проверяют на отсутствие закладок приборов, устройств.

32. Использование аппаратных средств снимает проблему:

a) обеспечения целостности системы.

b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования строго определенного множества программ.

33. Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются

a) аппаратно

b) программно

c) аппаратно и программно

34. Безопасность в частично контролируемым компьютерных системамах может быть обеспечена

a) изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.

b) схемой идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

c) внешней аутентификацией объекта, не принадлежащего системе;

35. Платы серии КРИПТОН, обеспечивают защиту:

a) ключей шифрования и электронной цифровой подписи (ЭЦП), так и неизменность их алгоритмов.

b) аппаратно-программных механизмов

c) реализации механизма виртуальной памяти с разделением адресных пространств;

36. К основным компонентам сети относятся:

a) центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые экраны;

b) субъекты доступа

c) платы серии КРИПТОН

37. В качестве ключевых носителей устройств криптографической защиты данных серии КРИПТОН используются:

a) дискеты, смарт-карты и Touch-Memory.

b) смарт-карты, Touch-Memory

c) дискеты, смарт-карты

38. Средства серии КРИПТОН независимо от операционной среды обеспечивают:

a) защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

b) криптомаршрутизацию

c) функции шифрования и электронной цифровой подписи.

39. В системе Secret Disk используется:

a) смешанная программно-аппаратная схема защиты с возможностью выбора

b) реализация механизма виртуальной памяти с разделением адресных пространств;

c) механизм RUN-файлов позволяет в процессе работы запускать любые программы с предварительной проверкой их целостности.

40. В чем заключается особенность системы Secret Disk:

a) для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор.

b) для доступа к защищенной информации необходим только вводимый пользователем пароль.

c) для доступа к защищенной информации необходим только электронный идентификатор.

41. Мастер-ключ в Устройствах криптографической защиты данных серии КРИПТОН загружается:

a) до загрузки операционной системы

b) после загрузки операционной системы

c) вообще не загружается

42. Криптографических функций в устройствах криптографической защиты данных серии КРИПТОН выполняются:

a) внутри платы
b) в операционной системе
c) в блоке загрузки операционной системы

43. Под защитой информации понимается

a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.

b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;

c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

44. Возможные каналы утечки информации по классификации разделяют:

a) человек, аппаратура, программа
b) человек, линия связи
c) коммутационное оборудование, человек

45. К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:

a) расшифровка программой зашифрованной информации;
b) несанкционированный доступ программы к информации;
c) копирование программой информации с носителей.

46. К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:

a) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) копирование программой информации с носителей

47. К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:

a) несанкционированный доступ программы к информации
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

48. К средствам активной защиты относятся:

a) искаженные программы (программы вирусы, искажение функций)
b) заказное проектирование
c) специальная аппаратура

49. К средствам пассивной защиты относятся:
a) частотный анализ
b) авторская эстетика
c) аппаратура защиты (ПЗУ, преобразователи)

50. К средствам собственной защиты относятся:
a) машинный код
b) сигнатура
c) корреляционный анализ

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

6. Понятие ,безопасности компьютерных систем
7. Политика безопасности в корпоративных сетях. Оценка защищенности
8. Понятие ААА пользователя

Блок С. Задания практико-ориентированного уровня для диагностирования сформированности компетенций («владеть»)

ЛАБОРАТОРНАЯ РАБОТА №1. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Изучить порядок настройки беспроводной точки доступа и организации беспроводных сетей по технологии Wi-Fi.

ЛАБОРАТОРНАЯ РАБОТА №2. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Смоделировать попытку несанкционированного доступа к информации, которой обмениваются пользователи сети через FTP-сервер. Получить навыки перехвата и анализа пакетов компьютерной сети с помощью программы-монитора.

Для проверки сформированности компетенции

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств

1. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:

a) организационные и технические
b) технические и коммутационные
c) организационные и объективные

2. Технические мероприятия направлены :

a) на недопущение выхода информативного сигнала за пределы контролируемой территории с помощью сертифицированных технических средств защиты.

b) на использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

c) на защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

3. Организационными мероприятиями предусматривается

a) исключение нахождения в местах наличия информативного сигнала злоумышленника и контроль за его действиями и передвижением

b) исключение значительной части загрузочных модулей из сферы их досягаемости.

c) исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным

4. Активные способы защиты информации при ее утечке через сеть электропитания направленные на:

a) создание маскирующего шума

b) перехвата информации

c) минимизацию паразитных связей внутри ПЭВМ

5. Пассивные способы защиты информации при ее утечке через сеть электропитания направленные на

a) минимизацию паразитных связей внутри ПЭВМ

b) создание маскирующего шума

c) перехвата информации

6. Для минимизации паразитных связей внутри ПЭВМ используются

a) радиоэкранирующие и радиопоглощающие материалы

b) двигатели-генераторы

c) разомкнутые линии

7. Под системой защиты от несанкционированного использования и копирования понимается

a) комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.

b) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.

c) комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

8. Под надежностью системы защиты от несанкционированного копирования
понимается:

a) способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.

b) способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений.

c) способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ

9. Методы, затрудняющие считывание скопированной информации основываются на

a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС

b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования дополнительных программных или аппаратно-программных средств.

10. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:

a) организационные и технические
b) технические и коммутационные
c) организационные и объективные

11. Любая криптографическая система основана на использовании:

a) криптографических ключей
b) разомкнутых линии
c) односторонних функций

12. В симметричной криптосистеме отправитель и получатель сообщения используют

a) один и тот же секретный ключ
b) разные секретных ключи
c) вообще не используют секретных ключей

13. Асимметричная криптосистема предполагает использование

a) двух ключей открытого и личного (секретного)
b) системы разграничения доступа
c) переносных носителей для хранения секретной информации

14. Под ключевой информацией понимают:

a) совокупность всех действующих в АСОИ ключей
b) совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.
c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации.

15. Какая из функций не входит в процесс управления ключами?

a) переадресация ключей
b) генерация ключей
c) распределение ключей

16. Модификация ключа - это

a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции.
b) генерирование нового ключа из последующего значения ключа с помощью односторонней (однонаправленной) функции.
c) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней (двунаправленной) функции.

17. Под функцией хранения ключей понимают

a) организацию их безопасного хранения, учета и удаления.
b) организацию их генерации, учета и удаления.
c) организацию их безопасного хранения, учета и сопостовления.

18. Механизм отметки времени позволяет каждому субъекту сети определить:

a) насколько старо пришедшее сообщение, и отвергнуть его, если появится сомнение в его подлинности.
b) были ли внесены изменения в файл.
c) какие информационные потоки в системе являются "легальными", то есть не ведут к утечке информации

19. Модель рукопожатия применяется для:

a) проверки подлинности партнеров
b) для симметричных криптосистем с секретными ключами
c) для асимметричных криптосистем с открытыми ключами

20. Каким из перечисленных способов не реализуется Распределение ключей между пользователями компьютерной сети:

a) документирование алгоритмов обеспечения защиты информации

b) использованием одного или нескольких центров распределения ключей

c) прямым обменом сеансовыми ключами между пользователями сети

21. Задача распределения ключей сводится к

a) построению протокола распределения ключей

b) взаимному подтверждению подлинности участников сеанса

c) использование минимального числа сообщений при обмене ключами

22. Протокол Kerberos основывается на

a) симметричной криптографии

b) ассиметричной криптографии

c) нескольких центров распределения ключей

23. Первым алгоритмом с открытыми ключами был алгоритм:

a) Диффи-Хеллмана

b) А. Фиата

c) А. Шамира

24. SKIP Протокол управления:

a) криптоключами

b) защищенного канала

c) симметричной криптосистемой

25. В каких режимах может выполняться изучение логики работы программы:

a) статическом

b) динамическом

c) и в статическом и в динамическом

26. Сущность статического режима заключается

a) в изучении исходного текста программы

b) в выполнение трассировки программы

c) в использование самогенерирующих кодов

27. Динамический режим изучения алгоритма программы предполагает

a) выполнение трассировки программы

b) изучении исходного текста программы

c) использование самогенерирующих кодов

28. Какой метод может противодействовать дизассемблированию

a) шифрование
b) хэширование
c) изучение

29. Сущность метода, основанного на использовании самогенерируемых кодов, заключается в том что

a) исполняемые коды программы получаются самой программой в процессе ее выполнения.

b) исполняемые коды программы получаются самой программой после процесса ее выполнения.

c) исполняемые коды программы получаются самой программой до процесса ее выполнения.

30. Трассировка программ обычно осуществляется с помощью:

a) программных продуктов, называемых отладчиками
b) шифрования
c) самогенерируемых кодов

31. Под компьютерным вирусом понимается:

a) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ.

b) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы.

c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

32. Резидентные вирусы это:

a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

b) вирусы, которые выполняются только в момент запуска зараженной программы.

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

33. Транзитные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

34. Вирусы-мутанты (MtE-вирусы) это

a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

35. Stealth-вирусы это

a) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных:
b) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.
c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

36. Загрузочные (бутовые) вирусы это:

a) вирусы, заражающие программы, хранящиеся в системных областях дисков.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

37. Трянские программы это:

a) программы которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.

b) программы , содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) программы которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

38. Файловые вирусы это:

a) вирусы, заражающие файлы с программами

b) вирусы, заражающие программы, хранящиеся в системных областях дисков.

вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

9. Понятие уязвимости компьютерных систем
10. Политика безопасности в компьютерных системах. Оценка
11. защищенности
12. Понятие идентификации пользователя

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторные работы

Лабораторная работа «Средства обеспечения безопасности ОС Windows»

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1. ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА

Цель работы: Научиться конфигурированию межсетевого экрана D-link DFL-800T для приобретения навыков защиты локальной вычислительной сети предприятия от угроз информационной безопасности со стороны пользователей глобальной сети Интернет

ЛАБОРАТОРНАЯ РАБОТА №2. ЗАЩИТА ПЕРЕДАВАЕМЫХ ДАННЫХ ПОМОЩЬЮ ШИФРОВАНИЯ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Цель работы: Приобрести навыки защиты и верификации передаваемых данных с помощью механизма шифрования и электронной цифровой подписи, используя программный продукт КриптоАРМ.

Основные сведения о программе КриптоАРМ

ЛАБОРАТОРНАЯ РАБОТА №3. РАБОТА С ЗАЩИЩЕННЫМИ ДИСКАМИ

Цель работы: Приобрести навыки работы с защищенными дисками на локальной рабочей станции с помощью программного пакета Secret Disk.

Для проверки сформированности компетенции
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Блок А. Задания репродуктивного уровня («знать»)

А1Вопросы для обсуждения

1. Каковы процедуры инициализации объекта информационной защиты?
2. Опишите типовые схемы идентификации и аутентификации пользователя.
3. Каковы недостатки и достоинства схемы простой аутентификации с помощью пароля?
4. Достоинства биометрических методов идентификации и аутентификации пользователя по сравнению с традиционными?

Основополагающие меры комплексной безопасности АС.

5. Основные подходы при проектировании.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

1. Построение программно-аппаратных комплексов шифрования
2. Проблема защиты отчуждаемых компонентов
3. Надежность средств защиты компонент
4. Несанкционированное копирование программ
5. Подходы к задаче защиты от копирования
6. Организация хранения ключей
7. Обратное проектирование ПО
8. Задачи защиты от изучения и способы их решения
9. Компьютерные вирусы

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторные работы

Лабораторная работа № 1 .

Тема: «Основные функции средств защиты от копирования»

Цель работы: Познакомится с основными функциями средств защиты от копирования.

Задание для работы:

1. Защита от копирования
2. Функции средств защиты

Лабораторная работа № 2.

Тема: «Виды мероприятий по защите информации**»**
Цель работы: Познакомится с различными видами мероприятий по защите информации.
Задание для работы:
1. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
2. Защита программ и данных от несанкционированного копирования

Лабораторная работа № 3.
Тема: «Современные системы защиты пэвм от несанкционированного доступа к информации**»**
Цель работы: Познакомится с различными современными системами защиты пэвм от несанкционированного доступа к информации.
Задание для работы:
1. Системы защиты ПЭВМ.
2. Несанкционированный доступ к информации

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Основные принципы создания средств защиты информации.
2. Описать способ контроля потоков данных, посредством применения основного правила разграничения доступа, применяемого в мандатном механизме управлениядоступом
3. Концепция построения программно–аппаратных средств обеспечения информационной безопасности.
4. Описать применение ролевого способа управления доступом.
5. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы.
6. Указать основные документы, определяющие требования к структуре и функциям СЗИ.
7. Методы ограничения доступа и управления доступом. Дискреционное управление доступом.
8. Описать порядок функционирования компонентов СЗИ от НСД Secret Net.
9. Методы ограничения доступа и управления доступом. Мандатное управлениедоступом.

10. Описать порядок функционирования ядра и основных подсистем СЗИ от НСДSecret Net.
11. Методы ограничения доступа и управления доступом. Ролевое управлениедоступом
12. Дать характеристику режимов идентификации и аутентификации, реализуемых СЗИ от НСД Secret Net
13. Структура и функции программно–аппаратных средств обеспечения информационной безопасности.
14. Описать применение механизма блокировок компьютера и видов блокировок, реализуемых СЗИ от НСД Secret Net, дать их сравнительную характеристику.
15. Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Secret Net
16. Описать процедуру доверенной загрузки операционной системы при применении электронных замков и устройствовводаидентификационныхпризнаков (УВИП).
17. Подсистемы клиента СЗИ от НСД Secret Net: ядро системы защиты, подсистема локального управления, защитные подсистемы
18. Описать общий порядок функционирования СЗИ от НСД Страж NT
19. Подсистемы клиента СЗИ от НСД Secret Net: модуль входа, подсистема контроля целостности, подсистема работы с аппаратной поддержкой
20. Описать порядок настройки подсистемы дискреционного и мандатного управления доступом СЗИ от НСД Страж NT
21. Защитные механизмы СЗИ от НСД Secret Net. Идентификация и аутентификация пользователей.
22. Описать порядок тестирования, восстановления и обеспечения целостности СЗИ от НСД Страж NT.
23. Функционирование подсистемы учета носителей СЗИ от НСД Страж NT.

24. Определить возможную конфигурацию аппаратных средств СЗИ от НСД SecretNet, применяемых для идентификации и аутентификации пользователей.
25. Определения и классификацию устройств ввода идентификационных признаков (УВИП).
26. Пояснить применение концепций распространения прав доступа и дать их сравнительную характеристику.
27. Устройства ввода идентификационных признаков. Устройства iButton.
28. Пояснить результаты применения правил выбора стойких паролей.
29. Устройства ввода идентификационных признаков. Смарт-карты. Устройства ввода на базе смарт-карт.
30. Дать сравнительную характеристику основных подходов к разработке средств защиты информации.
31. Устройства ввода идентификационных признаков. USB-ключи.
32. Пояснить применение концепции диспетчера доступа.
33. Устройства ввода идентификационных признаков. Комбинированные УВИП. Электронные замки. Общий алгоритм функционирования
34. Дать характеристику основных принципов создания средств защиты информации и их применения
35. Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Secret Net
36. Описать процедуру доверенной загрузки операционной системы при применении электронных замков и устройствовводаидентификационныхпризнаков (УВИП).
37. Дать характеристику режимов идентификации и аутентификации, реализуемых СЗИ от НСД Secret Net.
38. Указать основные документы, определяющие требования к структуре и функциям СЗИ.

РАЗДЕЛ 3.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся.очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по междисциплинарному курсу складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Ответы на устные вопросы	0-10	«неудовлетворительно» «удовлетворительно»

		«хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защита реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение презентаций	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал

			и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по междисциплинарному курсу компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами;

			обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	Оценка	Показатели	Критерии
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. Самостоятельность тестирования; 5. и т.д.	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»		Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в

			определении понятий, терминов и др.
15-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-14	«неудовлетвори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	**Показатели**	**Критерии**
9-10	«отлично»	1. Полнота данных ответов; 2. Аргументированность данных ответов; 3. Правильность ответов на вопросы; 4. и т.д.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные. Изложение материала последовательно и правильно.
7-8	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.

5-6	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0-4	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	Оценка	Показатели	Критерии
5	«отлично»	1. Полнота выполнения рефератов; 2. Своевременность	Выполнены все требования к написанию и защите реферата: обозначена проблема и

		выполнения; 3. Правильность ответов на вопросы.	обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
3-4	«хорошо»		Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
1-2	«удовлетворительно»		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.
0	«неудовлетвори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

Методика оценивания выполнения презентаций

Баллы	**Оценка**	***Показатели***	***Критерии***
5	«отлично»	1. Полнота выполнения презентаций; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Выполнены все требования к составлению презентаций: дизайн слайдов, логика изложения материала, текст хорошо написан и сформированные идеи ясно изложены и структурированы
3-4	«хорошо»		Основные требования к презентациям выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации
1-2	«удовлетворительно»		Имеются существенные отступления от требований к презентациям. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентаций или при ответе на дополнительные вопросы.
0	«неудовлетвори-тельно»		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания лабораторных работ

Баллы	***Оценка***	**Показатели**	**Критерии**
18-20	«отлично»	1. Полнота выполнения заданий	- правильно выполнены все задания лабораторной работы в соответствии с требованиями;

		2. Выполнение дополнительных заданий 3. Подготовка отчета	- правильно выполнены дополнительные задания; - своевременно предоставлен отчет о выполнении работы.
14-17	«хорошо»		- правильно выполнены все задания в основной части; - дополнительные задания выполнены не в полном объеме; - предоставлен отчет о выполнении работы, либо в случае несвоевременного предоставления отчета или с наличием несущественных ошибок в выполнении лабораторных заданиях
11-13	«удовлетворительно»		- выполнены не все, но более 50% заданий лабораторной работы; - дополнительные задания не выполнены, - несвоевременно предоставлен отчет о выполнении работы.
0-10	«неудовлетвори-тельно»		- выполнено менее 50% лабораторной работы; - не выполнены дополнительные задания; - отчет о выполнении работы не предоставлен

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной междисциплинарному курсу, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

Лист актуализации оценочных материалов по междисциплинарному курсу «Программно-аппаратные средства защиты информации»

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Фонд оценочных средств пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____