Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования «Казанский национальный исследовательский
технический университет им. А.Н. Туполева-КАИ»
Институт **Компьютерных технологий и защиты информации**

Кафедра **Компьютерных систем**

УТВЕРЖДАЮ
Ответственный за ОП
Верш И.С. Вершинин
« 31 » 08 2017 г.
Регистрационный номер 4010-17/11-25

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине

Администрирование безопасности компьютерных систем и сетей
(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.ДВ.01.01**

Направление подготовки: **09.04.01 «Информатика и вычислительная техника»**

Квалификация: **магистр**

Магистерская программа: **Системное и сетевое администрирование (информатика как вторая компетенция)**

Виды профессиональной деятельности: **научно-исследовательская**

Заведующий кафедрой СИБ И.В. Аникин

Разработчик: доцент каф. СИБ Г.С. Корнилов

Казань 2017 г.

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

Администрирование безопасности компьютерных систем и сетей

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению 09.04.01 «Информатика и вычислительная техника», учебному плану специальности 09.04.01 «Информатика и вычислительная техника».

Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Администрирование безопасности компьютерных систем и сетей». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника». В составе ФОС присутствуют оценочные средства в виде тестовых заданий и контрольных вопросов различного уровня сложности, которые позволяют провести оценку порогового, продвинутого и превосходного уровней освоения компетенций по дисциплине.

ФОС обладают необходимой степенью приближенности к задачам будущей профессиональной деятельности обучающихся, связанным со применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий (ПК-7). Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методической комиссии института КТЗИ от «31» августа 2017 г., протокол № 8.

Председатель УМК института КТЗИ _____ В.В. Родионов

Содержание

Введение

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Администрирование безопасности компьютерных систем и сетей» – это комплект методических и контрольно-измерительных материалов, предназначенных для определения уровня сформированности компетенций, оценивания знаний, умений, владений на разных этапах освоения дисциплины для проведения промежуточной аттестации обучающихся по дисциплине.

ФОС ПА является составной частью учебного и методического обеспечения программы магистратуры по направлению 09.04.01 «Информатика и вычислительная техника».

Задачи ФОС по дисциплине «Администрирование безопасности компьютерных систем и сетей»:

– оценка запланированных результатов освоения дисциплины обучающимися в процессе изучения дисциплины, в соответствии с разработанными и принятыми критериями по каждому виду контроля;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков и формирования компетенций, определенных в ФГОС ВО по направлению подготовки

ФОС ПА по дисциплине «Администрирование безопасности компьютерных систем и сетей» сформирован на основе следующих основных принципов оценивания:

– пригодности (валидности) (объекты оценки соответствуют поставленным целям обучения);

– надежности (использования единообразных стандартов и критериев для оценивания запланированных результатов);

– эффективности (соответствия результатов деятельности поставленным задачам).

ФОС ПА по дисциплине «Администрирование безопасности компьютерных систем и сетей» разработан в соответствии с требованиями ФГОС ВО по

направлению 09.04.01 «Информатика и вычислительная техника» для аттестации обучающихся на соответствие их персональных достижений требованиям поэтапного формирования соответствующих составляющих компетенций и включает контрольные вопросы (или тесты) и типовые задания, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций.

1. Формы промежуточной аттестации по дисциплине

Дисциплина «Администрирование безопасности компьютерных систем и сетей» изучается в 3 семестре при очной форме обучения и завершается промежуточной аттестацией в форме зачета.

2. Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации по дисциплине «Администрирование безопасности компьютерных систем и сетей» при очной форме обучения.

Таблица 1

Оценочные средств для промежуточной аттестации
(очная форма обучения)

№ п/п	Семестр	Форма промежуточной аттестации	Оценочные средства
1.	3	Экзамен	ФОС ПА

3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Перечень компетенций и их составляющих, которые должны быть сформированы при изучении темы соответствующего раздела дисциплины «Администрирование безопасности компьютерных систем и сетей», представлен в таблице 2.

Таблица 2

Перечень компетенций и этапы их формирования
в процессе освоения дисциплины

№ п/п	Этап формирования (семестр)	Наименование раздела	Код формируемой компетенции (составляющей компетенции)		Форма промежуточной аттестации
1.	3	*Организационно-правовые и методологические основы деятельности администратора безопасности*	ПК-7	ПК-7.З	Экзамен
2.	3	*Безопасность уровня сетевого взаимодействия, операционных систем и узлов сети*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен
3.	3	*Безопасность уровня баз данных и приложений*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен

4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкалы оценивания

Показатели и критерии оценивания сформированности компетенций на зачете, приведены в таблице 3.

Таблица 3

Показатели и критерии оценивания сформированности компетенций на зачете

№ п/п	Этап формирования (семестр)	Код формируемой компетенции (составляющей компетенции)		Критерии оценивания	Показатели оценивания (планируемые результаты обучения)		
					Пороговый уровень	Продвинутый уровень	Превосходный уровень
1.	7	ПК-7	ПК-7.3	Теоретические навыки	- основных программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз - основных программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз - основных подходов организации работы малых коллективов исполнителей, принятия управленческих решений в сфере профессиональной	- Знание основных сертифицированных ФСТЭК программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз - Знание нескольких разнотипных программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз для одной из платформ - Умение практически применять и конфигурировать в соответ-	- Знание основных сертифицированных ФСТЭК программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз в различных ОС - Знание программных средств системного и прикладного назначения, используемых для обхода механизмов противодействия статическому и динамическому исследованию ПО - Умение практически применять и конфи-

					деятельности, разработки предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы - Умение практически применять внутренние механизмы защиты от НСД для операционных систем - Умение практически применять одно из программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз	ствии с требованиями внутренние механизмы защиты от НСД для операционных систем - Умение практически применять несколько разнотипных программных средств системного и прикладного назначения, используемых для проведения компьютерных экспертиз для одной из платформ	гурировать в соответствии с требованиями внутренние механизмы защиты от НСД для операционных систем и СЗИ НСД, сертифицированных ФСТЭК - Умение описывать алгоритм функционирования на основе статического и динамического исследования программного кода

2.	7	ПК-7	ПК-7.У ПК-7.В	Практические навыки	Владение навыками активного и пассивного анализа защищенности с применением одного из программных средств	Владение навыками активного и пассивного анализа защищенности с применением нескольких программных средств	Владение навыками описания алгоритмов функционирования на основе статического и динамического исследования программного кода

Формирование оценки при промежуточной аттестации по итогам освоения дисциплины зависит от уровня освоения компетенций, которые обучающийся должен освоить по данной дисциплине. Связь между итоговой оценкой и уровнем освоения компетенций (шкала оценивания) представлена в таблице 4.

Таблица 4

Описание шкалы оценивания

Шкала оценивания		Описание оценки в требованиях к уровню и объему компетенций
Словесное выражение	Выражение в баллах	
отлично	от 86 до 100	Освоен **превосходный** уровень всех компетенций (составляющих компетенций)
хорошо	от 71 до 85	Освоен **продвинутый** уровень всех компетенций (составляющих компетенций)
удовлетворительно	от 51 до 70	Освоен **пороговый** уровень всех компетенций (составляющих компетенций)
неудовлетворительно	до 51	Не освоен **пороговый** уровень всех компетенций (составляющих компетенций)

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

Формирование оценки по результатам текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Администрирование безопасности компьютерных систем и сетей» приведено в таблице 5.

Таблица 5

Формирование оценки по итогам освоения дисциплины

Наименование контрольного мероприятия	Рейтинговые показатели				
	I аттестация	II аттестация	III аттестация	по результатам текущего контро-ля	по итогам промежуточной аттестации (зачета /экзамена)
Раздел 1. *Организационно-правовые и ме-тодологические основы дея-тельности ад-министратора безопасности*	**10**			**10**	
Тест текущего контроля по разделу	10			10	
Раздел 2. *Безопасность уровня сетевого взаимодействия, операционных систем и узлов сети*		**20**		**20**	
Тест текущего контроля по разделу		10		10	
Защита лабораторных работ		10		10	
Раздел 3. *Безопасность уровня баз данных и приложений*			**20**	**20**	
Тест текущего контроля по разделу			10	10	
Защита лабораторных работ			10	10	
Промежуточная аттестация (зачет):					**50**
– тест промежуточной аттестации по дисциплине					20
– ответы на контрольные вопросы в письменной форме					30

6 Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

6.1 Тестовые задания

1.

Какие функциональные элементы не входят в состав КИС:

- ❑ Рабочие места
- ❑ Серверы
- ❑ Средства телекоммуникации
- ■ Пользователи
- ❑ Телеслужбы

2.

Многоуровневая структура КИС включает в себя следующие уровни:

- ■ Уровень защиты АРМ
- ■ Уровень защиты серверов
- ■ Уровень защиты корпоративной АС
- ❑ Уровень защиты пользователей

3.

На какие из следующих источников отводится наибольшее количество атак в КИС?

- ■ Внутренних нарушителей
- ❑ Внешних нарушителей

4.

Какие из следующих способов позволяют защитить корпоративную сеть от угрозы прослушивания корпоративного трафика?

- ❑ Межсетевые экраны.
- ❑ Трансляция адресов.
- ☑ Шифрование каналов связи
- ❑ Использование систем обнаружения вторжений.
- ❑ Сканирование сетей.
- ☑ Коммутируемая инфраструктура.

5.

Что понимают под ARP-спуфингом?

- ❑ Разновидность отказа в обслуживании.
- ■ Подмена MAC-адреса узла для перенаправления трафика.
- ❑ Способ прослушивания каналов связи.
- ❑ Способ защиты от внедрения вирусов в корпоративную сеть.

6.

Какие из следующих средств защиты позволяют защитить корпоративную сеть от угроз атак в обслуживании?

- ❑ Сканирование сетей.
- ❑ Функции анти-спуфинга.
- ❑ Шифрование каналов связи.
- ☑ Ограничение объема трафика.
- ☑ Системы обнаружения вторжений.

7.

Какие из следующих способов позволяют идентифицировать уязвимости узлов корпоративной сети?

- ❑ Межсетевые экраны.
- ❑ Трансляция адресов.
- ❑ Виртуальные частные сети.
- ❑ Системы обнаружения вторжений.
- ■ Сканирование сетей.

8.

В чем заключается принцип разделения обязанностей?

- ❑ Доступ должен предоставляться только к необходимым данным
- ■ Передача критически важных функций людям с различными ролями в организации
- ❑ Обязанности пользователя должны быть максимальными
- ❑ Обязанности пользователя должны быть минимальными

9.

В чем заключается принцип минимизации прав и привилегий пользователей:

- ❑ Доступ должен предоставляться только к необходимым данным
- ■ Передача критически важных функций людям с различными ролями в организации
- ❑ Права пользователя должны быть максимальными

10.

Что понимают под унаследованной системой?

- ❑ Устаревшая КИС
- ❑ КИС, доставшаяся от прежнего владельца
- ■ любой технически устаревший компонент КИС

11.

Что понимается под деревом:

- ■ набор доменов, которые используют единое связанное пространство имен.
- ❑ логически связанный набор компьютеров
- ❑ логически связанный набор сегментов

12.

Что понимается под лесом:

- ■ объединение деревьев, которые поддерживают единую схему

- ❑ объединение компьютеров, которые поддерживают единую схему
- ❑ объединение сегментов, которые поддерживают единую схему

13.

Какие структурные объекты не содержит БД Active Directory:

- ❑ разделы;
- ❑ домены;
- ❑ деревья доменов;
- ■ пользовательские пароли
- ❑ леса;
- ❑ сайты;
- ❑ организационные единицы.

14.

Для чего используется назначенный корневой домен:

- ■ для запуска AD;
- ❑ для создания учетных записей фактических пользователей и групп.

15.

Для чего используется неназначенный корневой домен:

- ❑ для запуска AD;
- ■ для создания учетных записей фактических пользователей и групп.

16.

Содержит учетные записи назначенный корневой домен:

- ❑ Содержит все
- ❑ Не содержит ни каких
- ■ Содержит учетные записи «по умолчанию».

17.

Какие существует типы доверительных отношений:

- ❑ транзитивные доверительные отношения;
- ❑ односторонние доверительные отношения;
- ☑ многосторонние доверительные отношения;
- ❑ доверительные отношения леса;
- ☑ недоверительные отношения леса;
- ❑ доверительные отношения области.

18.

Какие объекты не содержат OU?

- ❑ компьютеры;
- ❑ контакты;
- ❑ группы;
- ■ жесткие диски;
- ■ флэшки;
- ❑ inetOrgPerson;
- ❑ принтеры;
- ❑ пользователи;
- ❑ общедоступные папки;
- ❑ организационные единицы.

19.

Когда рекомендуется развертывать один домен:

■ Если организация часто реорганизуется, и пользователи передвигаются между деловыми подразделениями

❑ Между подразделениями организации существуют медленные сетевые подключения или в офисах имеется много пользователей.

20.

Что такое SID:

■ Идентификатор защиты

❑ аутентификатор защиты

❑ относительный идентификатор

21.

Где хранятся DACL списки:

■ В дескрипторах защиты

❑ В маркерах доступа

22.

Где хранятся SACL списки:

■ В дескрипторах защиты

❑ В маркерах доступа

23.

Какие задачи решает протокол Kerberos?

■ Аутентификация

❑ Контроль доступа

❑ Криптографическая защита

24.

Какое из следующих правил конфигурирования межсетевого экрана является более безопасным?

■ запрещать все, что не разрешено в явной форме;

❑ разрешать все, что не запрещено в явной форме.

25.

Какие из следующих видов межсетевых экранов способны запретить выполнение команды «Записать файл» внутри протокола FTP?

❑ Пакетные фильтры.

❑ Межсетевые экраны сеансового уровня.

☑ Межсетевые экраны прикладного уровня.

☑ Межсетевые экраны экспертного уровня.

26.

Какие из следующих видов межсетевых экранов способны запретить загрузку аудио и видеофайлов из Internet на рабочих местах?

- ❑ Пакетные фильтры.
- ❑ Межсетевые экраны сеансового уровня.
- ☑ Межсетевые экраны прикладного уровня.
- ☑ Межсетевые экраны экспертного уровня.

27.

Среди следующих протоколов выделите те, которые относятся к канальному уровню.

- ☑ L2TP
- ❑ SKIP
- ☑ PPTP
- ❑ SSL
- ☑ L2F
- ❑ SOCKS
- ❑ IPSec

28.

Какой из следующих протоколов используется для согласования ключей в рамках протокола SKIP?

- ■ Диффи-Хеллмана.
- ❑ ISAKMP
- ❑ RSA.

29.

Какие узлы выносятся в демилитаризованную зону?

- ❑ Все сервера организации
- ❑ Рабочие станции организации
- ■ Сервера организации, доступные извне

30.

Безопасно ли устанавливать на сайте разрешения Write (Запись)

- ❑ Да
- ■ Нет

31.

Какая из следующих утилит является фильтром пакетов?

- ❑ cmd
- ■ iptables
- ❑ accept
- ❑ ls

32.

Для чего предназначена таблица Mangle

- ■ для внесения изменений в заголовки пакетов
- ❑ для выполнения преобразований сетевых адресов
- ❑ для фильтрации пакетов

33.

Для чего предназначена таблица NAT

- ❑ для внесения изменений в заголовки пакетов
- ■ для выполнения преобразований сетевых адресов
- ❑ для фильтрации пакетов

34.

Для чего предназначена таблица FILTER

- ❑ для внесения изменений в заголовки пакетов
- ❑ для выполнения преобразований сетевых адресов
- ■ для фильтрации пакетов

35.

Какая команда пропускает сетевой пакет

- ■ ACCEPT
- ❑ DROP
- ❑ REJECT

36.

Какая команда отбрасывает сетевой пакет

- ❑ ACCEPT
- ■ DROP
- ❑ REJECT

37.

Какая команда отбрасывает сетевой пакет

- ❑ ACCEPT
- ❑ DROP
- ■ REJECT

38.

Какой файл используется для указания хостов, которые имеют право доступа к службе RPC:

- ■ /etc/hosts.allow
- ❑ /etc/hosts.deny
- ❑ /etc/exports.

39.

Какой файл используется для указания хостов, которые не имеют право доступа к службе RPC:

- ❑ /etc/hosts.allow
- ■ /etc/hosts.deny
- ❑ /etc/exports.

40.

Для чего используется файл .htaccess

- ■ для ограничения доступа к некоторому каталогу
- ❑ для внесения изменений в заголовки пакетов

❑ для выполнения преобразований сетевых адресов

41.

Что такое IAS?

■ Служба аутентификации
❑ Служба криптографической защиты
❑ WEB-сервер

42.

Что такое карантин доступа к сети

❑ Перенос зараженных вирусами файлов в специализированный каталог
❑ Отключение небезопасного компьютера от общей сети
■ Запрет доступа к внутренней сети на период проверки соответствия атрибутов конфигурации удаленного компьютера требуемым, указанным в сценарии.

43.

Основное назначение ЭЦП?

■ подтверждение целостности и аутентичности электронного документа;
❑ подтверждение неотказуемости электронного документа;
❑ подтверждение факта отправки электронного документа;
❑ подтверждение факта получения электронного документа.

44.

Какое из определений ЭЦП является верным?

■ ЭЦП – это результат шифрования на секретном ключе пользователя дайджеста сообщения;
❑ ЭЦП – это результат вычисления хэш-значения электронного документа;
❑ ЭЦП – это отсканированный вариант рукописной подписи человека;
❑ ЭЦП – это криптографическое преобразование документа с последующим его хэшированием.

45.

Основное назначение цифровых сертификатов?

■ обеспечение безопасного канала распределения открытых ключей пользователей;
❑ проверить принадлежность открытых ключей их владельцам;
❑ автоматизировать процесс установки и проверки ЭЦП документов;
❑ разграничение ответственности между субъектами электронного документооборота.

46.

Какой из следующих сервисов не требуется для реализации технологии PKI?

❑ криптографические сервисы
❑ сервисы управления сертификатами
■ сервисы идентификации пользователей
❑ сервисы регистрации

47.

Что не относится к основным компонентам технологии PKI

- ❑ реестр сертификатов
- ❑ архив сертификатов
- ❑ регистрационный центр
- ■ центр контроля ЭЦП

48.

Случай угрозы, когда нарушитель посылает документ абоненту В, подписавшись именем абонента А называется:

- ❑ повтор
- ■ маскарад
- ❑ подмена
- ❑ протокол 16-с

49.

Случай угрозы, когда злоумышленник повторяет наш переданный документ, который абонент А посылал абоненту Б, называется:

- ■ повтор
- ❑ подмена
- ❑ маскарад
- ❑ протокол 16-с
- ❑ ренегатство

50.

Какие существуют типы угроз, направленных на нарушение целостности передаваемых сообщений и подлинность авторства?

- ❑ чтение
- ☑ повтор
- ☑ подмена
- ❑ запись
- ☑ маскарад
- ❑ смена прав
- ☑ ренегатство
- ☑ активный перехват

51.

Какой из следующих сервисов не требуется для реализации технологии PKI?

- ❑ криптографические сервисы
- ❑ сервисы управления сертификатами
- ■ сервисы идентификации пользователей
- ❑ сервисы регистрации

52.

В чем заключается принципиальное отличие между протоколами SSH и Telnet

- ■ SSH шифрует весь трафик, включая и передаваемые пароли
- ❑ telnet шифрует весь трафик, включая и передаваемые пароли

53.

Какое шифрование используется в SSL для подтверждения подлинности отправителя и получателя:

- ❑ Симметричное
- ■ Асимметричное

54.

В каком режиме работы IPSec конечные точки криптографического туннеля совпадают с конечными точками потоков информации

- ■ Транспортном
- ❑ Туннельном

55.

Какой из следующих протоколов передает пароли по сети в открытом виде?

- ■ PPP
- ❑ CHAP
- ❑ MS-CHAP

56.

При какой архивации выполняется копирование всех выбранных файлов на резервный носитель со сбросом битов архива.

- ■ Полной
- ❑ Добавочной
- ❑ Разностной

57.

При какой архивации выполняется копирование только файлов с установленным битом архива, а у скопированных файлов этот бит сбрасывается.?

- ❑ Полной
- ■ Добавочной
- ❑ Разностной

58.

При какой архивации выполняется копирование выбранных файлов без сброса бита архива?

- ❑ Полной
- ❑ Добавочной
- ■ Разностной

59.

Какая из следующих утилит является средством резервирования

- ❑ Ls
- ❑ Iptables
- ■ Dump
- ❑ Restore

60.

Какая из следующих утилит является средством восстановления

- ❑ Ls
- ❑ Iptables
- ❑ Dump
- ■ Restore

61.

Какой из следующих уровней RAID является зеркальным дисковым массивом:

- ❑ RAID 0
- ■ RAID 1
- ❑ RAID 2
- ❑ RAID 3
- ❑ RAID 4
- ❑ RAID 5
- ❑ RAID 6

62.

Какой из следующих уровней RAID зарезервирован для массивов, применяющих код Хемминга:

- ❑ RAID 0
- ❑ RAID 1
- ■ RAID 2
- ❑ RAID 3
- ❑ RAID 4
- ❑ RAID 5
- ❑ RAID 6

63.

Какой из следующих уровней RAID используют чётность для защиты данных от двойных неисправностей.

- ❑ RAID 0
- ❑ RAID 1
- ❑ RAID 2
- ❑ RAID 3
- ❑ RAID 4
- ❑ RAID 5
- ■ RAID 6

64.

Какой тип события будет внесен в журнал аудита, если приложение откажется запускаться

- ❑ Информационное
- ❑ Предупреждающее
- ■ Ошибка
- ❑ Успешный аудит
- ❑ Неудачный аудит

65.

Какой тип события будет внесен в журнал аудита, если пользователь не прошел регистрацию в системе

- ❑ Информационное
- ❑ Предупреждающее
- ❑ Ошибка
- ❑ Успешный аудит
- ■ Неудачный аудит

66.

Какой из журналов аудита содержит события от компонентов операционной системы.

- ❑ Журнал приложений
- ■ Системный журнал
- ❑ Журнал безопасности

67.

Какие категории имеют сообщения аудита от системы печати

- ❑ cron
- ■ lpr
- ❑ kern
- ❑ console

68.

Укажите самый высокий уровень важности сообщений аудита

- ❑ Alert
- ❑ Crit
- ■ Emerg
- ❑ err

69.

Что такое шаблон безопасности

- ■ Основное хранилище параметров системы безопасности
- ❑ текстовый файл с расширением .inf
- ❑ эталонная конфигурация узла

70.

Что из ниже перечисленного не является секцией шаблона безопасности

- ❑ Политика паролей
- ❑ Политика аудита
- ■ Резервное копирование
- ❑ Системный реестр
- ❑ Файловая система

71.

В каком из шаблонов безопасности следует разрешать запуск служб и получение прав, необходимых для исполнения роли

- ❑ Базовом шаблоне
- ■ Добавочном шаблоне

72.

Системы обнаружения вторжений являются:

- ❑ Превентивными средствами обеспечения безопасности
- ■ Активными средствами обеспечения безопасности

73.

Анализ системных журналов реализуется в:

- ❑ NIDS
- ■ HIDS

74.

Обнаружение атак, осуществляемых на всю сеть, реализуется в:

- ❑ HIDS
- ■ NIDS

75.

В режиме сниффера работает

- ■ NIDS
- ❑ HIDS

76.

IDS Snort является

- ❑ HIDS
- ■ NIDS

77.

Real Secure Desktop Protection является

- ■ HIDS
- ❑ NIDS

78.

Real Secure Server Sensor является

- ■ HIDS
- ❑ NIDS

79.

Real Secure Network Sensor является

- ❑ HIDS
- ■ NIDS

80.

Какие из следующих алгоритмов являются алгоритмами хэширования:

- ❑ RSA
- ☑ MD5
- ☑ SHA
- ❑ DES
- ❑ ГОСТ 28-147-889
- ☑ ГОСТ 34.11-01

81.

Отличие систем с закрытым ключом от систем с открытым ключом:

■ системы с открытым ключом позволяют исключить явную передачу по открытым каналам секретных постоянных данных - паролей и секретных ключей для шифрования

❑ системы с открытым ключом позволяют исключить явную передачу по открытым каналам секретных данных

❑ системы с открытым ключом позволяют исключить явную передачу по закрытым каналам секретных данных

❑ системы с открытым ключом позволяют не исключают явную передачу по открытым каналам секретных данных

❑ системы с открытым ключом позволяют не исключают явную передачу по закрытым каналам секретных данных

❑ фактически ни чем не отличаются

Оценка практических умений и навыков

1. Администрирование безопасности Microsoft Windows Server.
2. Учетные записи пользователей Microsoft Windows Server.
3. Администрирование информационных систем Microsoft Windows Server. Служба имен.
4. Резервное копирование и восстановление БД. Разработка стратегии архивации.
5. Администрирование оборудования Cisco.
6. Операционная система Linux. Работа в командной строке.
7. Администрирование безопасности операционной системы Linux.
8. Настройка межсетевого экрана IPFW.
9. Администрирование информационных систем Unix. Служба имен.

6.2. Контрольные вопросы

1. Понятие корпоративных информационных сетей и систем. Их классификация. Структура.
2. Структура управления эффективностью функционирования и безопасностью КИС.
3. Основные угрозы безопасности в корпоративных сетях. Защита от них.
4. Концептуальный план защиты КИС. Разработка плана. Планирование процедуры восстановления КИС.
5. Понятие службы каталога Active Directory. Логическая структура службы AD.
6. Проектирование и реализация службы AD, ее компонентов.
7. Безопасное администрирование службы AD.
8. Общие рекомендации по проектированию защиты границ сети.
9. Обеспечение безопасности серверов IIS.
10. Средства для фильтрации сетевых пакетов: iptables и ipchains.
11. Рекомендации по обеспечению безопасности сетевой файловой системы NFS.
12. Рекомендации по обеспечению безопасности FTP и WEB.
13. Рекомендации по защите беспроводных сетей.
14. Методы обеспечения безопасности удаленного доступа.
15. Проектирование зашиты, стратегии аутентификации и учета удаленного доступа с применением IAS
16. Протоколы IPSec и SSH. Их использование.
17. Протоколы SSL и TLS.
18. Понятие виртуальных частных сетей. Организация туннелей VPN.
19. Внедрение VPN на базе Windows Server 2003.
20. Резервное копирование. Создание плана резервного копирования и выбор архивируемых данных. Типы архивации. Понятие теневого копирования.
21. RAID. Классификация RAID-массивов.

22. Организация программного RAID в Windows и Linux.
23. Мониторинг и аудит систем в ОС WINDOWS
24. Мониторинг и аудит систем в ОС LINUX.
25. Проектирование защиты для серверных ролей. Шаблоны безопасности, их проектирование, применение.
26. Проектирование защищенной инфраструктуры клиентов.
27. Системы обнаружения вторжений. Их применение, конфигурирование.

Лист регистрации изменений и дополнений

№ п/п	№ страницы внесения изменений	Дата внесения изменения	Краткое содержание изменений (основание)	Ф.И.О., подпись	«Согласовано» заведующий кафедрой, ведущей дисциплину