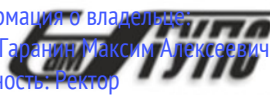


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гараня Максим Алексеевич
Должность: Ректор
Дата подписания: 11.05.2024 11:00:48
Уникальный программный ключ:
7708e3a47e66a8ee02711b298d7c78bd1e40bf88



МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Приложение
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Безопасность и защита информации в САПР

(наименование дисциплины(модуля))

Направление подготовки / специальность

09.04.01 Информатика и вычислительная техника

(код и наименование)

Направленность (профиль)/специализация

АСОИУ на транспорте

(наименование)

Содержание

1. Пояснительная записка.
2. Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций.
3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации.

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Формы промежуточной аттестации: экзамен- **2 семестр**

Код и наименование компетенции	Код достижения индикатора компетенции
ОПК-3 способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ОПК-3.1: Анализировать профессиональную информацию направленную на безопасность и защиту информации и представлять её в виде аналитических обзоров
	ОПК-3.2: Оформлять и представлять научно техническую информацию в соответствии со сложившимся академическим этикетом

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-3.1: Анализировать профессиональную информацию направленную на безопасность и защиту информации и представлять её в виде аналитических обзоров	Обучающийся знает: основные методы и средства защиты конфиденциальной информации; состав и организацию систем информационной безопасности, методы криптографических преобразований; основные стандарты и протоколы шифрования и электронной подписи; методы и средства обеспечения информационной безопасности компьютерных систем; современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования.	Вопросы тестирования №(1-5)
	Обучающийся умеет: определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий; использовать современные программные средства для защиты информации; принимать адекватные решения при выборе средств защиты информации на основе анализа угроз.	Ситуационная задача 1
	Обучающийся владеет: навыками разработки защищенных приложений; навыками создания защищенной среды с помощью аппаратно-программных средств защиты.	Ситуационная задача 2
ОПК-3.2: Оформлять и представлять научно техническую информацию в соответствии со сложившимся академическим этикетом	Обучающийся знает: основные положения законодательства в области современного авторского права и защиты информации; современные подходы к построению систем защиты информации.	Вопросы тестирования №(6-15)
	Обучающийся умеет: разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности; обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защи-	Ситуационная задача 3

	ты.	
	Обучающийся владеет: навыками самостоятельного проектирования систем защиты информации; методами оценки эффективности систем защиты информации в компьютерных системах.	Задания №(1-3)

2 семестр

Промежуточная аттестация (экзамен) проводится в одной из следующих форм:

- 1) проводится в форме устного ответа на вопросы из перечня
- 2) выполнение заданий в ЭИОС СамГУПС.

2. Типовые¹ контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций

2.1 Типовые вопросы (тестовые задания) для оценки знаниевого образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-3.1: Анализировать профессиональную информацию направленную на безопасность и защиту информации и представлять её в виде аналитических обзоров	Обучающийся знает: основные методы и средства защиты конфиденциальной информации; состав и организацию систем информационной безопасности, методы криптографических преобразований; основные стандарты и протоколы шифрования и электронной подписи; методы и средства обеспечения информационной безопасности компьютерных систем; современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования.

Примерные вопросы

1. При количественном подходе риск измеряется в терминах

денежных потерь
заданных с помощью шкалы
заданных с помощью ранжирования
объема информации

2. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации – это

идентификация
аудит
авторизация
аутентификация

3. Программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия

перехват
компрометация
наблюдение
уборка мусора

4. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется

управлением риском

¹ Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники, технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

<p>мониторингом средств защиты оптимизацией средств защиты минимизацией риска</p> <p>5. С помощью открытого ключа информация зашифровывается копируется транслируется расшифровывается</p>	
<p>ОПК-3.2: Оформлять и представлять научно-техническую информацию в соответствии со сложившимся академическим этикетом</p>	<p>Обучающийся знает: основные положения законодательства в области современного авторского права и защиты информации; современные подходы к построению систем защиты информации.</p>
<p><i>Примерные вопросы</i></p> <p>6. Согласно «Европейским критериям» для систем с высокими потребностями в обеспечении целостности предназначен класс F-IN F-DX F-DI F-AV</p> <p>7. Согласно «Европейским критериям» на распределенные системы обработки информации ориентирован класс F-DI F-IN F-AV F-DX</p> <p>8. Согласно «Оранжевой книге» с объектами должны быть ассоциированы метки безопасности электронные подписи типы операций уровни доступа</p> <p>9. Содержанием параметра угрозы безопасности информации «конфиденциальность» является несанкционированное получение уничтожение искажение несанкционированная модификация</p> <p>10. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные – это целостность детерминированность восстанавливаемость доступность</p> <p>11. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство доступность детерминированность восстанавливаемость целостность</p> <p>12. Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели искажение наблюдение компрометация перехват</p> <p>13. Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно «Европейским критериям» безопасность считается средней высокой</p>	

базовой
стандартной

14. Достоинствами аппаратной реализации криптографического закрытия данных являются
высокая производительность и простота
целостность и безопасность
доступность и конфиденциальность
практичность и гибкость

15. Достоинством дискретных моделей политики безопасности является
простой механизм реализации
числовая вероятностная оценка надежности
высокая степень надежности
динамичность

2.2 Типовые задания для оценки навыкового образовательного результата

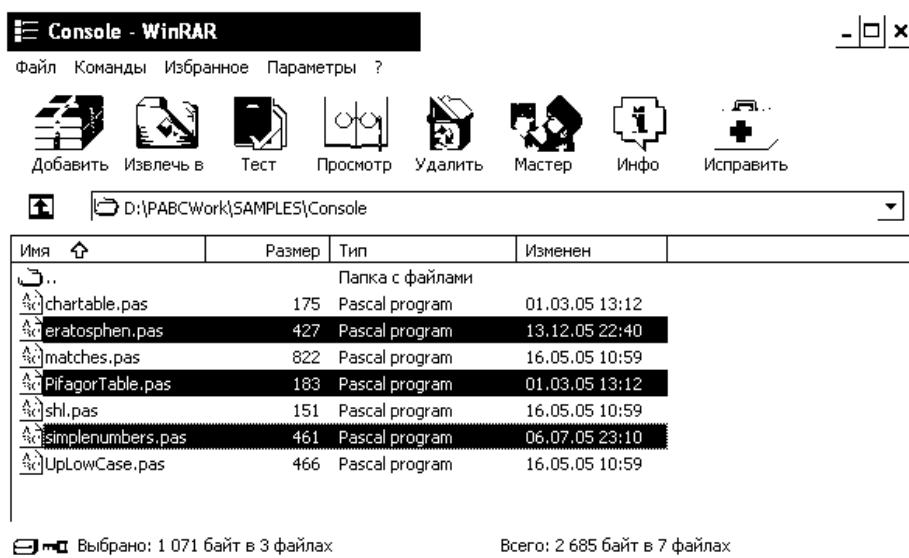
Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-3.1: Анализировать профессиональную информацию направленную на безопасность и защиту информации и представлять её в виде аналитических обзоров	Обучающийся умеет: определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий; использовать современные программные средства для защиты информации; принимать адекватные решения при выборе средств защиты информации на основе анализа угроз; разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности; обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.

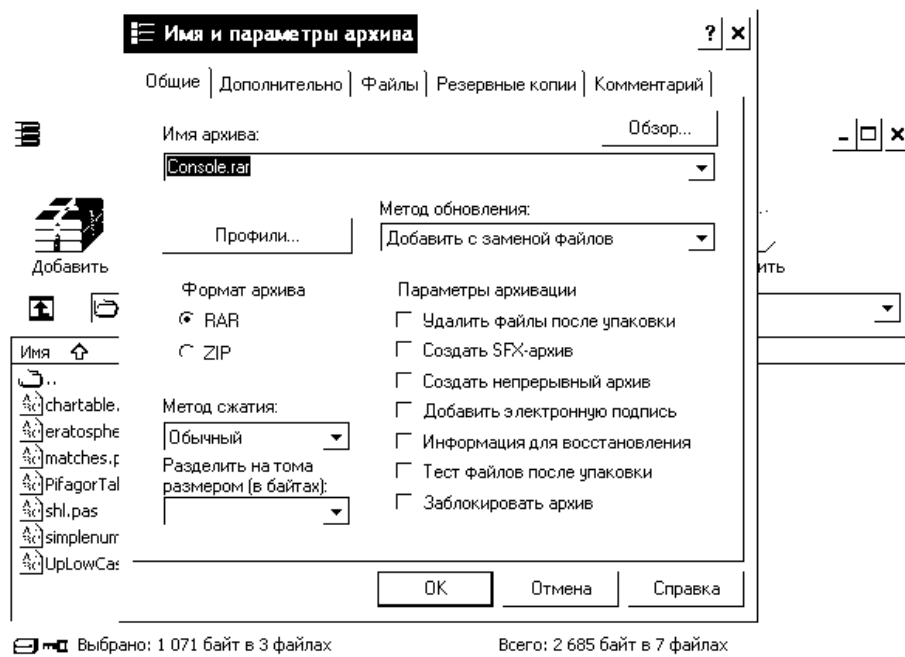
Ситуационная задача 1

Тема «Архивация данных»

1. Запустите программу резервного копирования, например, «Архивация данных», WinRAR, Хранитель V и т.п.
2. Выберите необходимые документы для резервного копирования.



3. Нажмите кнопку «Добавить».
4. На вкладке «Общие» укажите имя архивного файла.



5. Выберите необходимый метод сжатия.

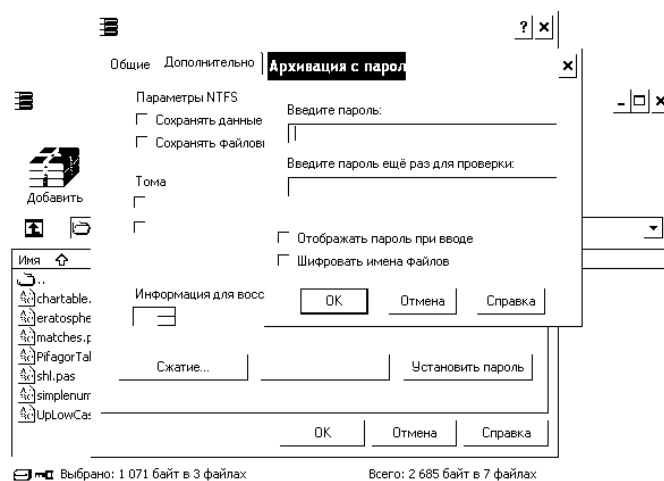
ОПК-3.1: Анализировать профессиональную информацию направленную на безопасность и защиту информации и представлять её в виде аналитических обзоров

Обучающийся владеет:
 навыками разработки защищенных приложений;
 навыками создания защищенной среды с помощью аппаратно-программных средств защиты;
 навыками самостоятельного проектирования систем защиты информации;
 методами оценки эффективности систем защиты информации в компьютерных системах.

Ситуационная задача 2

Тема «Защита архива паролем»

1. На вкладке «Дополнительно» нажмите кнопку «Установить пароль» и в открывшемся окне укажите пароль для выбранных файлов, добавляемых в указанный архив.
2. Ознакомьтесь с остальными параметрами, расположенными на вкладках «Общие», «Дополнительно», «Резервные копии», «Комментарии» окна «Имя и параметры архива» программы WinRar. Задайте необходимые параметры.
3. Нажмите кнопку «ОК», после чего в заданный архив будут добавлены выбранные файлы.
4. Убедитесь, что для просмотра содержимого добавленных файлов архива, необходимо ввести пароль.



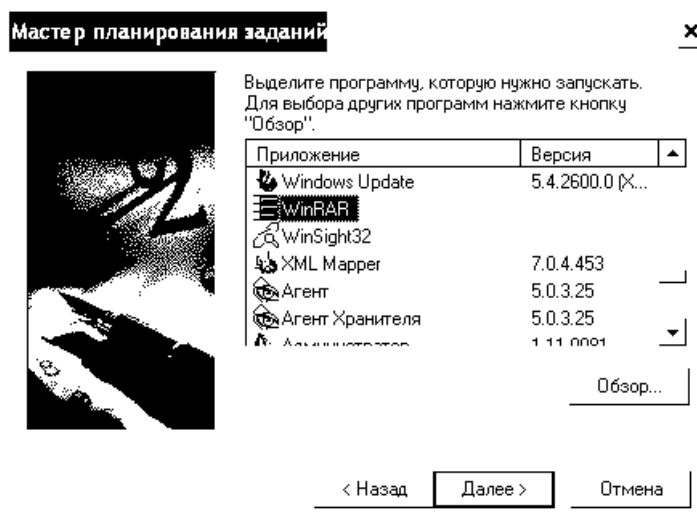
ОПК-3.2: Оформлять и представлять научно-техническую информацию в соответствии со сложившимся академическим этикетом

Обучающийся умеет:
разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности;
обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.

Ситуационная задача 3

Тема «Настройка резервного копирования данных»:

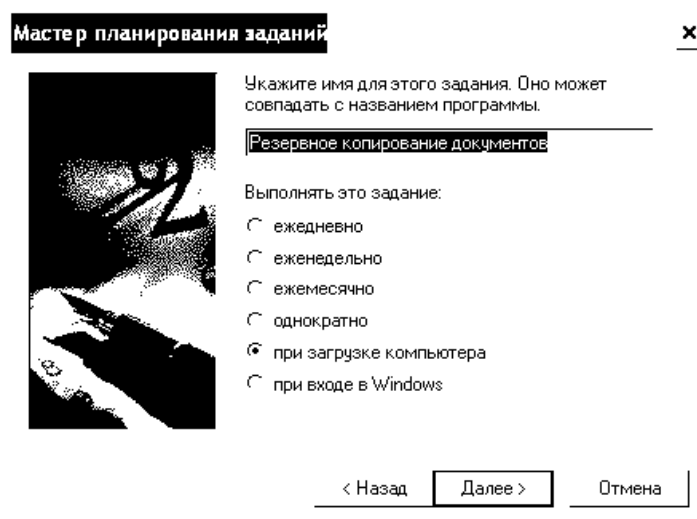
1. Запустите программу «Мастер планирования заданий».



Для того чтобы настроить запуск любой программы в назначенное время, необходимо нажать кнопку «Пуск», выбрать пункт меню «Программы» | «Стандартные» | «Служебные» | «Назначенные задания» и в открывшемся окне запустить «Добавить задание».

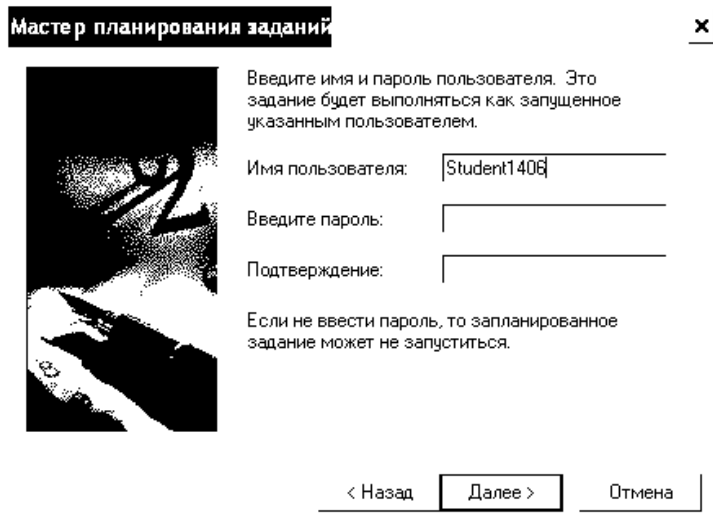
2. Выберите программу «WinRAR»

3. Укажите имя создаваемого задания и периодичность его выполнения.

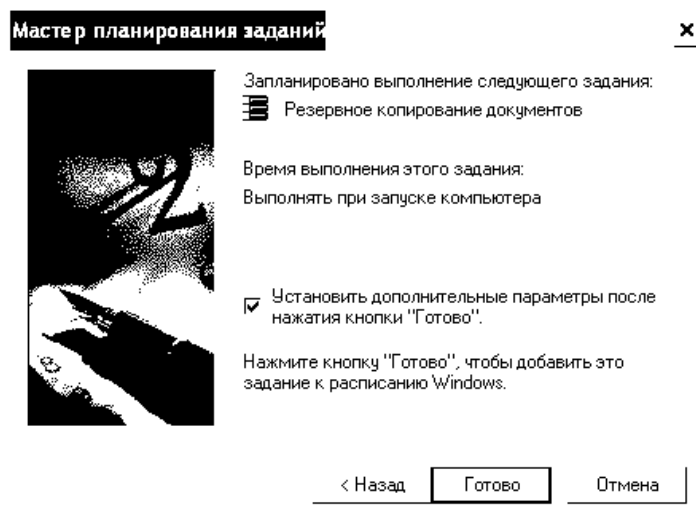


Периодичность задается в зависимости от ценности архивируемых данных и частоте их изменения. Если компьютер не выключается в ночное время, то можно выбрать период «ежедневно» и впоследствии указать ночное или обеденное время (т.е. время, когда с компьютером никто не работает). Если выбрать период «при загрузке компьютера», то данные будут архивироваться при каждом включении компьютера. Таким образом, в случае отказа оборудования в архиве будут храниться данные за предыдущий рабочий день.

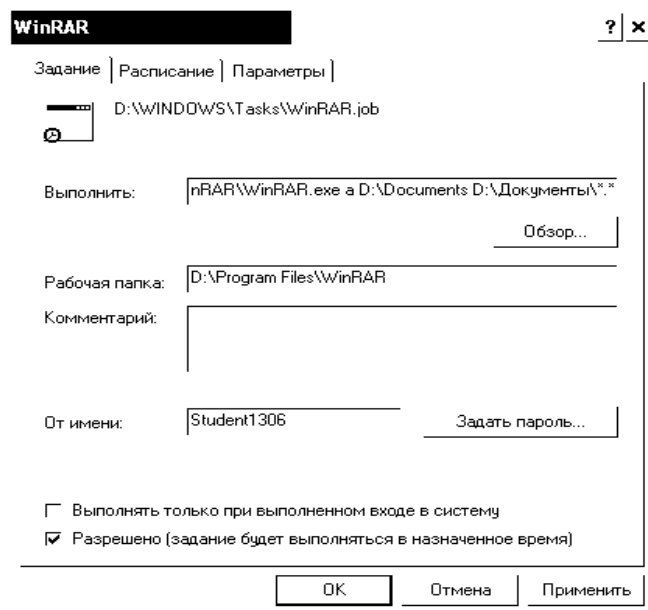
4. Укажите имя пользователя (от имени которого будет выполняться задание) и его пароль.



5. Установите галочку задания дополнительных параметров и нажмите кнопку «Готово».



6. В дополнительных параметрах на вкладке «Задания» в поле «Выполнить» укажите параметры запуска программы WinRAR: полное имя программы, команда добавления в архив, полное имя архива и шаблон архивируемых файлов (например, «C:\Program Files\WinRAR\WinRAR.exe a D:\Arhive D:\Документы»).



ОПК-3.2: Оформлять и представлять научно техническую информацию в соответствии со сложившимся академическим этикетом	Обучающийся владеет: навыками самостоятельного проектирования систем защиты информации; методами оценки эффективности систем защиты информации в компьютерных системах.
<p><i>Примеры заданий.</i></p> <p>Задание 1. Изучить и описать информационную систему, эксплуатируемую на железнодорожном транспорте.</p> <p>Задание 2. Разработать для информационной системы, эксплуатируемой на железнодорожном транспорте, схему резервирования.</p> <p>Задание 3. Разработать алгоритм модуля резервирования и восстановления информационной системы при отказе сервера баз данных.</p>	

2.3. Перечень вопросов для подготовки обучающихся к промежуточной аттестации

1. Компьютерная информация: определение, основные категории с точки зрения безопасности
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
3. Правовые основы защиты информации в РФ, Обзор законов РФ в области информационной безопасности.
4. Дискреционная и мандатная модель доступа к объектам информационных систем.
5. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы
6. Механизмы реализации услуг безопасности в информационных системах
7. Классификация криптографических алгоритмов
8. Структурная схема симметричной криптосистемы
9. Структурная схема асимметричной криптосистемы
10. Математические определения шифра, процедур шифрования и дешифрации
11. История развития криптоалгоритмов: шифр Цезаря, афинная криптосистема, шифры Виженера и Вернома
12. Частотный криптоанализ одно- и многопоточных шифров
13. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы
14. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования
15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля
16. Алгоритм шифрования TEA: структура, достоинства и недостатки
17. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB
18. Методы криптоанализа блочных шифров
19. Поточные шифры: принципы функционирования, структура
20. Методы построения нелинейных поточных шифров
21. Асимметричные криптосистемы: принципы функционирования, трудно вычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов
22. RSA: структура криптоалгоритма
23. Метод ключевого обмена Диффи-Хелмана
24. Хэш-функции: назначение и основные свойства
25. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров
26. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA
27. Инфраструктура PKI. Сертификация ключей асимметричных систем шифрования. Структура сертификата.
28. Иерархическая и сетевая модель сертификации ключей асимметричных систем шифрования.

29. Обзор современных защищенных сетевых протоколов.
30. Угрозы безопасности в глобальных сетях
31. Межсетевые экраны: назначение, основные функции, состав
32. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки
33. Проxy-сервера : назначение, основные функции, достоинства и недостатки
34. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
35. Определение вредоносной программы. Классификация вредоносных программ.
36. Компьютерные вирусы: разновидности, используемые методы заражения.
37. Сетевые черви: определение, способы распространения.
38. Троянская программа: назначение, классификация, руткиты как средство маскировки.
39. Методики защиты от вредоносных программ.
40. Модель безопасности ОС Windows. . Реализация дискреционной модели защиты доступа к ресурсам системы.
41. Аудит событий безопасности современных операционных систем.
42. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.
43. Шифрующая файловая система (EFS): принцип работы, структура зашифрованного файла, роль агентов восстановления.

3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90 % от общего объема заданных вопросов;
- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76 % от общего объема заданных вопросов;
- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы – 75–60 % от общего объема заданных вопросов;
- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60 % от общего объема заданных вопросов.

Критерии формирования оценок по результатам выполнения заданий

«Зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов в соответствии с заданием. Обучающийся полностью владеет информацией по теме работы, решил все поставленные в задании задачи.

«Не зачтено» - ставится за работу, если обучающийся правильно выполнил менее 2/3 всего задания, использовал при выполнении неправильные алгоритмы, допустил грубые ошибки при программировании, сформулировал неверные выводы по результатам работы.

Виды ошибок:

- *грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.*
- *негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.*
- *недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.*

Критерии формирования оценок по экзамену

«Отлично» (5 баллов) – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение матери-

алом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания.

«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности. Таким образом данная оценка выставляется за правильный, но недостаточно полный ответ.

«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляется конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.

«Неудовлетворительно» (0 баллов) – выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.