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/И-072

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине
«Методы и средства защиты информации»

(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.ДВ.03.01**

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)

«Методы и средства защиты информации»

(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 «Методы и средства защиты информации» – 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 «Методы и средства защиты информации»:

– 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 «Методы и средства защиты информации» 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 «Методы и средства защиты информации» 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 «Методы и средства защиты информации» изучается в 3 семестре при очной форме обучения и завершается промежуточной аттестацией в форме экзамена.

2. Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации по дисциплине «Методы и средства защиты информации» при очной форме обучения.

Таблица 1

Оценочные средства 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 «Методы и средства защиты информации», 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	*Введение. Определение и общее содержание проблемы информационной безопасности. Угрозы информационной безопасност и меры защиты информации.*	ПК-7	ПК-7.З	Экзамен
2.	3	*Политики безопасности и системы разграничения доступа. Методы криптографической защиты информации. Защита программного обеспечения*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен
3.	3	*Особенности защиты информации в сетях. Нормативное обеспечение защиты информации.*	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.	3	ПК-7	ПК-7.3	Теоретические навыки	Знание перспективных методов исследования и решения профессиональных задач	Знание перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники	Знание перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий

2.	3	ПК-7	ПК-7.У ПК-7.В	Практические навыки	умение применять перспективные методы исследования и решения профессиональных задач практически выполнять работы по установке, настройке и обслуживанию программных (в том числе криптографических) средств защиты информации. Владеть навыками исследования и решения профессиональных задач Владеть навыками обслуживания программных (в том числе криптографических) средств защиты информации	умение применять перспективные методы исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники практически выполнять работы по установке, настройке и обслуживанию программно-аппаратных (в том числе криптографических) средств защиты информации навыками исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники	умение применять перспективные методы исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий; практически выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть навыками исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий

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 «Методы и средства защиты информации» 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 контроля	по итогам промежуточной аттестации (зачета /экзамена)
Раздел 1. *Введение. Определение и общее содержание проблемы информационной безопасности. Угрозы информационной безопасност и меры защиты информации.*	**10**			**10**	
Тест текущего контроля по разделу	10			10	
Раздел 2. *Политики безопасности и системы разграничения доступа. Методы криптографической защиты информации. Защита программного обеспечения*		**20**		**20**	
Тест текущего контроля по разделу		10		10	
Защита лабораторных работ		10		10	
Раздел 3. *Особенности защиты информации в сетях. Нормативное обеспечение защиты информации.*			**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

Тестовые задания

1. Что из перечисленного является верным?

а) субъект доступа – это пассивный компонент, который может стать причиной потока информации от субъекта к объекту или изменения состояния системы

б) субъект доступа – это активный компонент, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы

в) объект доступа – это пассивный компонент системы, не хранящий, не принимающий и не передающий информацию

г) объект доступа – это активный компонент системы, хранящий, принимающий или передающий информацию

2. Свойства информации с точки зрения информационной безопасности

а) интерпретируемость, связность, активность

б) уязвимость, угроза, атака

в) полнота и непротиворечивость

г) целостность, конфиденциальность, доступность

3. Расставьте в порядке логического следования событий в АСОИ

а) возникновение угрозы, наличие уязвимости, реализация атаки

б) наличие уязвимости, возникновение угрозы, реализация атаки

в) реализация атаки, наличие уязвимости, возникновение угрозы

г) наличие уязвимости, реализация атаки, возникновение угрозы

4. Какая угроза реализуется при атаке на чтение закрытой информации?

а) нарушение конфиденциальности информации

б) нарушение доступности информации

в) нарушение целостности информации

г) нарушение работоспособности системы обработки информации

5. Что из перечисленного не является каналом утечки информации?

а) виброакустический канал

б) электромагнитный канал

в) визуальный канал

г) информационный канал

д) Волго-Донской канал им. В.И. Ленина

6. Нарушение какого принципа обеспечения ИБ может дать возможность злоумышленнику внедрить в АСОИ программную закладку?

а) принцип простоты применения защитных мер и средств

б) принцип открытости алгоритмов и механизмов защиты

в) принцип разумной достаточности

г) принцип непрерывности защиты

7. К какой мере обеспечения информационной безопасности относится использование криптографических средств преобразования информации?

а) правовая

б) программно-аппаратная

в) морально-этическая

г) организационно-административная

8. Основная цель создания политики безопасности информационной системы

а) определить множество субъектов и объектов компьютерной системы

б) наделить полномочиями пользователей информационной системы

в) определить условия, которым подчиняется поведение подсистемы безопасности

г) обеспечить целостность, конфиденциальность и доступность информации

9. Какая политика безопасности не обеспечивает конфиденциальность?

а) политика безопасности Хариссона-Руззо-Ульмана

б) политика безопасности Биба

в) политика безопасности Белла-ЛаПадулы

г) мандатная политика безопасности

10. Какая политика безопасности контролирует целостность информации?

а) политика безопасности Белла-ЛаПадулы

б) политика безопасности Хариссона-Руззо-Ульмана

в) политика безопасности Белла-ЛаПадулы

г) дискреционная политика безопасности

11. Какая политика безопасности разрешает проблему программных закладок?

а) мандатная политика безопасности

б) дискреционная политика безопасности

в) политика безопасности Хариссона-Руззо-Ульмана

г) политика безопасности Белла-ЛаПадулы

12. Какое из перечисленных определений является верным?

а) идентификация – подтверждение принадлежности аутентификатора пользователю

б) аутентификация – подтверждение принадлежности идентификатора пользователю

в) авторизация – предъявление пользователем идентификатора для идентификации

г) верификация – наделение полномочиями субъекта системы

13. Какое из перечисленных требований не относится к парольной защите?

а) проверка и отбраковка пароля по словарю

б) задание минимальной длины пароля

в) установление минимального срока действия пароля

г) использование задержки при вводе неправильного пароля

14. Для обеспечения конфиденциальности информации используется

а) кодирование

б) электронная цифровая подпись

в) шифрование

г) цифровой сертификат

15. Что из перечисленного не может использоваться в системах биометрической идентификации/аутентификации пользователей?

а) рукописный почерк

б) клавиатурный почерк

в) мышиный почерк

г) крысиный почерк

16. Какая из криптоаналитических атак требует привлечения предельных вычислительных ресурсов?

а) атака методом анализа частотности закрытого текста

б) атака по словарю

в) атака по открытому тексту

г) атака методом полного перебора всех возможных ключей

17. Основной недостаток симметричной криптосистемы

а) проблема генерации ключевой информации

б) низкая скорость работы симметричных криптоалгоритмов

в) отсутствие эффективных алгоритмов симметричного шифрования

г) проблема хранения и распространения ключей шифрования

18. На каком ключе происходит шифрование сообщения в асимметричной криптосистеме?

а) секретном

б) ассиметричном

в) открытом

г) сообщение шифруется как на открытом, так и на секретном ключе (зависит от используемого алгоритма)

19. Реализация асимметричных криптосистем основана на использовании

а) однонаправленных функций

б) свойств электронной цифровой подписи

в) функций хэширования

г) процедур идентификации и аутентификации отправителей секретных сообщений

20. Понятие, не относящееся к свойствам функций хэширования

а) рассеивание

б) чувствительность к изменениям

в) открытость

г) необратимость

21. Основное назначение электронных ключей HASP

а) использование в качестве идентификатора пользователя

б) защита программ от несанкционированного использования

в) ограничение работы программ по времени

г) шифрование данных

Вопросы оценки практических навыков

Пример заданий

1. Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик P,V,T? При их уменьшении?
2. Проклассифицируйте традиционные алгоритмы шифрования. Кратко охарактеризуйте эти классы.
3. Охарактеризуйте методику криптоанализа, основанную на исследовании частотности закрытого текста.
4. Зная, что собой представляет система Вернама, опишите методику атаки по открытому тексту на архив ARJ.
5. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?
6. В какой контейнер можно внедрить большее количество информации без обнаружения модификаций – в текст или в насыщенное изображение?

7. В какой контейнер можно внедрить большее количество информации без обнаружения модификаций – в оперную увертюру, записанную с CD-качеством, или в репортаж со спортивного стадиона?

8. В чем заключается проблема системы Z? Показать и прокомментировать в сформированном отчете группу команд, реализующих систему Z.

Контрольные вопросы

1. Основные понятия и определения предмета защиты информации (понятие доступа, свойства безопасности информации, уязвимость, угроза, атака, каналы реализации угроз)
2. Принципы и меры обеспечения информационной безопасности в АСОИ
3. Понятие политики безопасности и их классификация
4. Политики избирательного разграничения доступа (модель Харрисона-Руззо-Ульмана)
5. Мандатные политики безопасности (модель Белла-ЛаПадуллы)
6. Ролевая политика безопасности (модель RBAC)
7. Пониятие идентификации и аутентификации субъектов. Классификация подсистем идентификации и аутентификации
8. Парольные системы идентификации и аутентификации пользователей
9. Идентификация и аутентификация пользователей с использованием технических устройств
10. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя
11. Принципы криптографической защиты информации
12. Принципы симметричного шифрования. Примеры простейших симметричных шифров
13. Шифрование методом замены. Примеры шифров замены
14. Шифрование методами перестановки. Примеры шифров перестановки
15. Шифрование методом гаммирования. Примеры алгоритмов ГПСЧ
16. Обзор и харктеристика основных методов криптоанализа
17. Недостатки симметричных криптосистем. Принципы асимметричного шифрования
18. Комбинированный метод шифрования и его достоинства
19. Понятие и примеры однонаправленных функций
20. Проблема обеспечения целостности информации
21. Функции хэширования и электронно-цифровая подпись
22. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей
23. Типовые схемы хранения ключевой информации
24. Защита баз данных аутентификации в ОС Windows NT
25. Электронные ключи HASP

26. Политика безопасности контроля целостности информации (модель Биба)
27. Элементы теории чисел
28. Современные симметричные системы шифрования (на примере DES и ГОСТ)
29. Инфраструктура открытых ключей PKI
30. Иерархия ключевой информации
31. Подходы к распределению ключевой информации
32. Протоколы безопасной удаленной аутентификации пользователей
33. Проблема защиты программного обеспечения от несанкционированного использования
34. Модульная архитектура технических средств защиты ПО от несанкционированного использования
35. Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования
36. Базовые методы нейтрализации систем защиты от несанкционированного использования
37. Понятие и средства обратного проектирования.
38. Локализация кода модуля защиты посредством отлова WinAPI функций в режиме отладки
39. Базовые методы противодействия отладчикам
40. Базовые методы противодействия дизассемблированию ПО
41. Защита от отладки, основанная на особенностях конвейеризации процессора
42. Использование недокументированных инструкций и недокументированных возможностей процессора
43. Шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию
44. Руководящие документы государственной технической комиссии России. Критерии защищенности АС и СВТ.

Лист регистрации изменений и дополнений

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