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
_____ И.С. Вершинин
«31» 08 2017 г.
Регистрационный номер 4010 – 17/М – 092

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине
«Программно-аппаратная защита информации»

(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.ДВ.03.02**

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)

«Программно-аппаратная защита 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 «Программно-аппаратная защита 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 «Программно-аппаратная защита 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 «Программно-аппаратная защита 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 «Программно-аппаратная защита 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 формирова-

ния 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 «Программно-аппаратная защита 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 «Программно-аппаратная защита 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 «Программно-аппаратная защита 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	*Методы и средства защиты от НСД к информации*	ПК-7	ПК-7.З	Экзамен
2.	3	*Методы защиты программного обеспечения*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен
3.	3	*Программно-аппаратные средства защиты от НСД к 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 «Программно-аппаратная защита 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. *Методы и средства защиты от НСД к информации*	**10**			**10**	
Тест текущего контроля по разделу	10			10	
Раздел 2. *Методы защиты программного обеспечения*		**20**		**20**	
Тест текущего контроля по разделу		10		10	
Защита лабораторных работ		10		10	
Раздел 3. *Программно-аппаратные средства защиты от НСД к 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

ЗАДАНИЕ 1. Выберете пароль, наиболее полно удовлетворяющий требованиям стойкости.

1. September.
2. SmirnovIvan.
3. Ivan123
4. Crlqj.
5. PCktL5(.

ЗАДАНИЕ 2. Для системы парольной аутентификации срок действия пароля T изменили с 3 месяцев до 6 месяцев. Увеличится или уменьшится вероятность взлома пароля в этом случае?

1. Увеличится.
2. Уменьшится.
3. Не изменится.

ЗАДАНИЕ 3. Пусть P – вероятность взлома пароля, V – скорость перебора паролей злоумышленником, T – срок действия пароля, L – длина пароля, A – мощность алфавита символов пароля. Какая из ниже представленных формул является формулой оценки стойкости парольной защиты?

1. $P = \frac{V \cdot T}{A \cdot L}$

2. $P = \frac{V \cdot T}{A^L}$

3. $P = \frac{A^L}{V \cdot T}$

4. $P = \frac{A \cdot L}{V \cdot T}$

ЗАДАНИЕ 4. Что из ниже перечисленного является достоинством парольных систем аутентификации.

1. Парольные системы аутентификации являются наиболее стойкими при правильном выборе пароля.
2. Парольные системы аутентификации можно использовать как для решения задач разграничения доступа к компьютерам, так и в помещения, на охраняемые объекты.
3. Парольные системы аутентификации наиболее дешевые и распространенные.
4. Пароли легко запомнить.

ЗАДАНИЕ 5. Какие из ниже перечисленных устройств являются только устройствами идентификации пользователей (возможно несколько вариантов ответов)?

1. iButton.
2. смарт-карты.
3. e-Token.
4. электронный ключ HASP.
5. карты proximity.

ЗАДАНИЕ 6. Каким образом закрывается ключевая информация в базах данных аутентификации ОС?

1. Ключевая информация в базах данных аутентификации ОС не хранится.
2. Шифруется.
3. Закрывается с использованием однонаправленного преобразования.

ЗАДАНИЕ 7. В чем состоит опасность получения злоумышленником прав доступа на запись в базу данных аутентификации пользователей?

1. Злоумышленник может выяснить пароли всех пользователей компьютерной системы.
2. Злоумышленник может получить только администраторские права доступа к компьютерной системе.
3. Злоумышленник может получить права доступа любого пользователя компьютерной системы.
4. Злоумышленник может скопировать базу данных аутентификации компьютерной системы.

ЗАДАНИЕ 8. В чем состоит опасность получения злоумышленником прав доступа на чтение из базы данных аутентификации пользователей?

1. Злоумышленник может прочитать пароли всех пользователей компьютерной системы.
2. Злоумышленник может прочитать пароли всех пользователей компьютерной системы, кроме администраторского.
3. Злоумышленник может выяснить идентификаторы всех пользователей компьютерной системы.
4. Злоумышленник может узнать ключ шифрования паролей.

ЗАДАНИЕ 9. В чем заключается отличие второй от первой типовой схемы хранения ключевой информации в базах данных аутентификации

1. Во второй схеме используются более стойкие функции хэширования.
2. Во второй схеме, в отличие от первой закрываются и ключи и идентификаторы пользователей.
3. Во второй схеме, в отличие от первой, одинаковым паролям соответствуют различные хэш-образы.
4. В первой схеме, в отличие от второй пользователи не могут обладать одинаковыми паролями

ЗАДАНИЕ 10. Какие элементы и в каком виде входят в эталон аутентификации в первой типовой схеме хранения ключевой информации?

1. Аутентификатор пользователя в закрытом виде.
2. Идентификатор в открытом виде, аутентификатор в закрытом виде.
3. Идентификатор в закрытом виде, аутентификатор в закрытом виде.

ЗАДАНИЕ 11. Какой из ниже представленных способов хэширования паролей доступа является более стойким ко взлому?

1. Хэш NTLM.
2. Хэш LANMAN.

ЗАДАНИЕ 12. Сколько хэш-образов пароля хранится в базе данных аутентификации Windows NT?

1. 1
2. 2
3. 3
4. 4

ЗАДАНИЕ 13. Какие алгоритмы используются для закрытия паролей базах SAM Windows NT, 2000, XP?

1. MD4
2. RC4
3. DES
4. IDEA
5. SHA.

ЗАДАНИЕ 14. Какая функция хэширования используется для формирования хэша NTLM?

1. MD4
2. RC4
3. DES
4. IDEA
5. SHA.

ЗАДАНИЕ 15. Пароли какой длины наиболее эффективны с точки зрения своей стойкости ко взлому для систем, построенных на базе WINDOWS NT.

1. 7
2. 10
3. 14
4. 15
5. 16
6. 20
7. 24
8. 32
9. Чем больше, тем лучше.

ЗАДАНИЕ 16. Знает ли операционная система Windows 2000 те пароли, с помощью которых злоумышленник проходит локальную аутентификацию?

1. Да, она их берет их из базы данных аутентификации и сравнивает с введенным.
2. Да, она берет из зашифрованный вариант из базы данных аутентификации, расшифровывает и сравнивает с введенным.
3. Нет.

ЗАДАНИЕ 17. Какое из ниже перечисленных требований является основным для протоколов удаленной аутентификации пользователей?

1. Должен использоваться выделенный канал, вероятность подключения к которому злоумышленника чрезмерно мала.
2. Пароли должны передаваться в зашифрованном виде.
3. Пароли должны передаваться к закрытом виде и каждый раз различные.
4. Аутентифицирующая информация не должна передаваться ни в открытом, ни в закрытом виде.

ЗАДАНИЕ 18. Какие из ниже представленных протоколов являются протоколами удаленной аутентификации?

1. DES.
2. MD4
3. CHAP.
4. SHA.
5. S/KEY.
6. RC4

ЗАДАНИЕ 19. Какой из одноразовых паролей в S/KEY отсылается первым – Y2=MD4(Y1) или Y3=MD4(Y2)?

1. Y1
2. Y2
3. Y3

ЗАДАНИЕ 20. В течение какого количества времени действует одноразовый пароль в S/KEY?

1. В зависимости от настроек пользователя.
2. В течении одной секунды.
3. В течение одной минуты.
4. В течение одного сеанса аутентификации.
5. Пока сервер не передаст нам следующий одноразовый пароль.

ЗАДАНИЕ 21. Какую информацию возможно хранить в энергонезависимой памяти устройства Touch Memory?

1. Пароль доступа к ЭВМ.
2. Зашифрованный пароль доступа к ЭВМ.

3. Возможное время доступа к ЭВМ.
4. Список пользователей, имеющих доступ к ЭВМ.
5. Лучше никакой информации там не хранить.
6. Количество запусков программы.
7. Срок окончания лицензии работы программы.

ЗАДАНИЕ 22. Каков объем пользовательского идентификатора в устройстве iButton?

1. 32 бита.
2. 48 бит.
3. 64 бита.
4. 128 бит.

ЗАДАНИЕ 23. Какое из ниже перечисленных устройств выполняет те же самые функции, что и устройство iButton DS1990A?

1. смарт-карта.
2. e-Token.
3. электронный ключ HASP.
4. карта proximity.

ЗАДАНИЕ 24. Какой из ниже перечисленных компонентов не входит в состав iButton?

1. Энергонезависимая память.
2. Литиевая батарейка.
3. ПЗУ.
4. Монитор разграничения доступа пользователя к защищаемым ресурсам.
5. Таймер.

ЗАДАНИЕ 25. Какие из ниже перечисленных устройств предпочтительнее использовать для идентификации пользователя, входящего в защищенное помещение (аутентификация не требуется) (возможно несколько вариантов ответа)?

1. iButton
2. смарт-карты
3. e-Token
4. электронные ключи HASP Standard
5. электронные ключи HASP Memo
6. электронные ключи HASP Time
7. карты proximity

ЗАДАНИЕ 26. Укажите типы пластиковых карт, относящихся к пассивным.

1. Карты со штрих-кодом.
2. Карты с магнитной полосой.
3. Карты-счетчики.
4. Карты с памятью.
5. Карты с микропроцессором.

ЗАДАНИЕ 27. Атака на какой из ниже перечисленных блоков может позволить взломать злоумышленнику рабочую лицензионную программу посредством модификации одного его байта?

1. Блок внедрения механизмов защиты.
2. Блок установки характеристик среды.
3. Блок сравнения характеристик среды.
4. Блок ответной реакции.
5. Блок противодействия нейтрализации защитных механизмов.

ЗАДАНИЕ 28. Посредством атаки не какой из ниже перечисленных блоков, пишутся как правило, эмуляторы электронных ключей, имитирующие их отклик?

1. Блок внедрения механизмов защиты.
2. Блок установки характеристик среды.
3. Блок сравнения характеристик среды.
4. Блок ответной реакции.
5. Блок противодействия нейтрализации защитных механизмов.

ЗАДАНИЕ 29. В каком из следующих типов защит отсутствует в явном виде подсистема внедрения механизмов защиты?

1. Встроенных.
2. Пристыковочных.

ЗАДАНИЕ 30. В каком из следующих типов защит более просто реализовать защиту ПО от внутреннего исследования?

1. Встроенных.
2. Пристыковочных.

ЗАДАНИЕ 31. Реализацию каких из ниже перечисленных блоков желательно исключить в явном виде (включить в неявном) в систему защиты ПО от несанкционированного использования?

1. Блок внедрения механизмов защиты.
2. Блок установки характеристик среды.
3. Блок сравнения характеристик среды.
4. Блок ответной реакции.
5. Блок противодействия нейтрализации защитных механизмов.

ЗАДАНИЕ 32. Какие из следующих типов электронных ключей семейства HASP обладают функцией шифрования и функцией отклика?

1. HASP Standard
2. Memo HASP
3. Time HASP
4. Net HASP
5. Все.

Вопросы оценки практических навыков

Пример заданий

1. Особенности исследования в отладчиках кода программ, генерируемого Delphi. Привести исследование таких программ. Представить рекомендации по усилению защиты программного кода в Delphi от отладки.

2. Особенности исследования и взлома компонент Delphi. Представить рекомендации по усилению защиты программ от данного типа исследования.

3. Реализация привязки программы к типу компьютерного оборудования и к заданному месту на диске.

4. Разбор логической головоломки CrackMe. Провести разбор, исследование одной из логических головоломок, выбранной Вами. Провести подробные результаты исследования.

5. Исследования в IDA Pro программного кода языков высокого уровня (Pascal, C++). Реализовать взлом одной из таких программ.

Контрольные вопросы

1. Парольные подсистемы идентификации и аутентификации. Количественная оценка стойкости парольной защиты.
2. Аппаратные устройства идентификации и аутентификации пользователей. Устройства Touch Memory. Карты Proximity. Их архитектура, функционирование, назначение.
3. Типовые решения в области организации ключевых систем. Утверждение о подмене эталона.
4. Формат и формирование баз данных аутентификации Windows NT/2000, UNIX.
5. Системы биометрической идентификации и аутентификации. Их архитектура, особенности функционирования. Коэффициенты FAR и FRR. Кривая рабочих характеристик приемника биометрического устройства.
6. Общая модульная структура системы защиты ПО от несанкционированного копирования. Основные ее подсистемы, их функционирование и взаимосвязь.
7. Встроенные и пристыковочные системы защиты ПО от несанкционированного копирования. Требования к блокам установки и сравнения характеристик среды в системах защиты ПО от несанкционированного копирования.
8. Базовые методы нейтрализации систем защиты от несанкционированного копирования.
9. Семейство электронных ключей HASP. Их типы, внутренняя структура, назначение. Способы и возможности защиты ПО с помощью электронных ключей HASP. Система FAS.
10. Электронные ключи HASP. Система RUS, ее назначение и использование. Модель защиты структурным кодом PCS в ключах HASP.
11. Семейство электронных ключей Guardant. Архитектура, возможности и устройство памяти разнотипных ключей Guardant. Отличительные особенности ключей Guardant от HASP.
12. Устройство аппаратного алгоритма шифрования ключей Guardant. Способы создания аппаратных алгоритмов.
13. Понятие изолированной программной среды.
14. Устройство, назначение и архитектура СЗИ НСД АККОРД. Контроль доступа к объектам файловой системы СЗИ НСД АККОРД.
15. Архитектура и функции устройства КРИПТОН. Иерархия ключевой информации в устройстве КРИПТОН.
16. Понятие обратного проектирования. Задачи, решаемые злоумышленником при обратном проектировании. Классификация средств обратного проектирования.
17. Основные приемы, используемые злоумышленником при отладке и дизассемблировании ПО. Специфика атак на модули проверки ключевой

информации, на модули проверки истечения временного срока работы программы.

18. Отлов злоумышленником вызова WinAPI функций при взломе ПО. Базовые WinAPI функции, используемые злоумышленником для локализации кода защиты.
19. Базовые методы защиты от отладчиков реального режима.
20. Базовые методы защиты от отладчиков защищенного режима.
21. Методы противодействия дизассемблированию ПО.
22. Методы противодействия отладке и дизассемблированию ПО, основанные на использовании недокументированных команд и недокументированных возможностей процессора.
23. Метод противодействия отладке и дизассемблированию ПО, основанный на особенностях конвейеризации исполняемых команд процессорами семейства INTEL.
24. Шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию ПО.
25. Понятие пластиковых карт и их классификация. Виды пластиковых карт и их физическая архитектура.
26. Карты с магнитной полосой, их особенности и физическая архитектура. Стандарты ISO7810, ISO7811.
27. Карты-счетчики и карты с памятью. Структура памяти карт с памятью фирмы Athena.

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