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/б-023

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине **«Защита информации»**

Индекс по учебному плану: **Б1.В.02**

Направление подготовки: **09.03.01 «Информатика и вычислительная техника»**

Квалификация: **бакалавр**

Профили подготовки: **Вычислительные машины, комплексы, системы и сети, Автоматизированные системы обработки информации и управления, Программное обеспечение средств вычислительной техники и автоматизированных систем, Системы автоматизированного проектирования (электронные средства), Системы автоматизированного проектирования машиностроения.**

Виды профессиональной деятельности: **научно-исследовательская, проектно-конструкторская**

Заведующий кафедрой И.В. Аникин

Разработчик М.В. Тумбинская

Казань 2017 г.

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

Защита информации

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению подготовки 09.03.01 «Информатика и вычислительная техника», учебному плану направления подготовки 09.03.01 «Информатика и вычислительная техника».

Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Защита информации». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению подготовки 09.03.01 «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 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5).

Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению подготовки 09.03.01 «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 «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 бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

Задачи ФОС по дисциплине «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 «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 «Защита информации» разработан в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 «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 «Защита информации» изучается в 5 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 «Защита информации» при очной форме обучения.

Таблица 1

Оценочные средств для промежуточной аттестации
(очная форма обучения)

№ п/п	Семестр	Форма промежуточной аттестации	Оценочные средства
1.	8	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 «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.	8	Введение в защиту информации	ОПК-5 ПК-3	ОПК-5.З ПК-3.З	экзамен
2.	8	Политики информационной безопасности. Системы шифрования.	ОПК-5	ОПК-5.З ОПК-5.В	экзамен
3	8	Особенности применения методов и средств защиты информации.	ОПК-5	ОПК-5.З ОПК-5.У ОПК-5.В	экзамен

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

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

Таблица 3

Показатели и критерии оценивания сформированности компетенций на экзамене

№ п/п	Этап формирования (семестр)	Код формируемой компетенции (составляющей компетенции)		Критерии оценивания	Показатели оценивания (планируемые результаты обучения)		
					Пороговый уровень	Продвинутый уровень	Превосходный уровень
1.	8	ОПК-5	ОПК-5.З ОПК-5.У	Теоретические навыки	- Знать свойства защищенности информации и систем её обработки; - Знать угрозы информационной безопасности и классификацию каналов несанкционированного доступа к информации; - Знать основные методы разграничения доступа и процессы идентификации, аутентификации и авторизации пользователей; - Уметь разрабатывать модели угроз информации	- Знать процедуры определения политики безопасности и сущность субъектно-объектной модели компьютерной системы; - Знать принципы организации современных систем шифрования; - Знать особенности защиты информации в сетях - Умение принимать адекватные решения при выборе средств защиты информации на основе анализа угроз	- Детально знать способы защиты программного обеспечения и операционных систем - Уметь использовать технические средства защиты программ и данных

2	8	ПК-3	ПК-3.З	Теоретические навыки	Имеет представление о моделях компонентов информационных систем	Знает особенности представления моделей компонентов информационных систем, включая модели баз данных	Знает особенности применения моделей компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек – электронно-вычислительная машина»
3	8	ОПК-5	ОПК-5.В	Практические навыки	- Начальные навыки разработки и создания типовых схем защиты информации на основе современных средств обеспечения информационной безопасности	- Навыки работы реализации криптографических алгоритмов, обеспечивающих высокую стойкость шифров	Глубокие навыки использования встроенных в ОС Windows механизмов безопасности для защиты компьютерной информации

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 «Защита информации» приведено в таблице 5.

Таблица 5

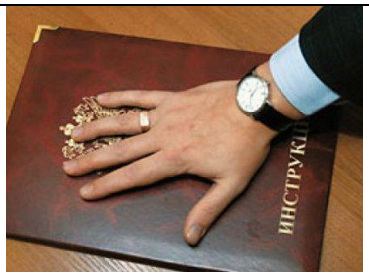
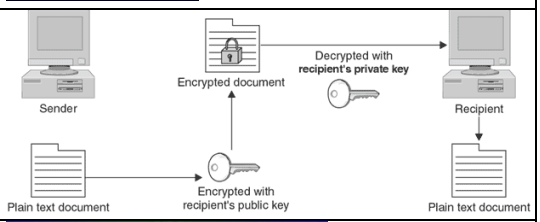
Формирование оценки по итогам освоения дисциплины

Наименование контрольного мероприятия	Рейтинговые показатели				
	I аттестация	II аттестация	III аттестация	по результатам текущего контроля	по итогам промежуточной аттестации (зачета /экзамена)
Раздел 1. Введение в защиту информации	**20**			**20**	
Тест текущего контроля по разделу	10			10	
Защита лабораторных работ	10			10	
Раздел 2. Политики информационной безопасности. Системы шифрования.		**20**		**20**	
Тест текущего контроля по разделу		10		10	
Защита лабораторных работ		10		10	
Раздел 3. Особенности применения методов и средств защиты информации.			**20**	**20**	
Тест текущего контроля по разделу			10	10	
Защита лабораторных работ			10	10	
Промежуточная аттестация (Экзамен):					**40**
– тест промежуточной аттестации по дисциплине					20
– ответы на контрольные вопросы в письменной форме по билетам					20

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. *Типовые тестовые задания*

1. Установите соответствие между методами защиты информации и графической иллюстрацией примера их реализации.

1. Физические методы защиты информации	
2. Законодательные методы защиты информации	
3. Организационные методы защиты информации	
4. Программные методы защиты информации	
	

1. Установите соответствие между средствами и методами защиты информации.

1. Физические	маскировка или методы шифрования – программное обеспечение, специально предназначенное для выполнения функций защиты информации
2. Программные	препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации
3. Организационные	методы аудита информационной безопасности
4. Технические	методы контроля и управления доступом
	методы оценки затрат материального ущерба и других последствий от возможной реализации угроз

2. Анализ информационной безопасности предприятия, проводимый оперативно, в реальном времени или периодически, называется…

3. Локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе называется …

4. Наука о методах шифрования и дешифрования, называется…

5. Электронные идентификаторы являются средствами идентификации и аутентификации.

На рисунке изображено средство идентификации, называемое…

6. «Маски» вирусов используются для ..... известных вирусов.

7. При асимметричном шифровании для шифрования и расшифровки используются .... ключа

8. Наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа называется …

9. К симметричным алгоритмам шифрования относятся: ГОСТ, Blow-fish, ..., CAST.

10. К асимметричным алгоритмам шифрования относятся: ...., El-Gamal.

11. Функции Федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи согласно ФЗ "Об информации, информационных технологиях и о защите информации":

- организует мониторинг сайтов и страниц сайтов в сети "Интернет"
- утверждает методику определения количества пользователей сайта или страницы сайта в сети "Интернет" в сутки
- по необходимости запрашивает информацию у организаторов распространения информации в сети "Интернет", блогеров и иных лиц
- *определяет провайдера для сайта в сети "Интернет" для определения правомочий его действий*
- *размещает на своем сайте в сети "Интернет" персональные данные блогеров*

13. В реестр нарушителей ограничения доступа к информации в сети "Интернет", обрабатываемой с нарушением законодательства РФ в области персональных данных согласно статьи 15.5 ФЗ "Об информации, информационных технологиях и о защите информации" включаются ...

- доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных
- сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных
- *доменные имена сайтов в сети "Интернет", содержащие информацию в области персональных данных*
- *сетевые адреса сайтов в сети "Интернет", содержащие информацию в области персональных данных*

14. К основным задачам инженерно-технической защиты информации относятся:

- предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения
- защита носителей информации от уничтожения в результате воздействия стихийных сил
- защита конфиденциальной информации при ее хранении на открытых носителях

- *предотвращение утечки информации по различным техническим каналам*

- *аудит происходящих событий в информационной системе*

15. К инженерно-технической защите информации относятся методы защиты:

- аппаратные
- физические
- программные
- *правовые*
- *административные*

Оценка практических умений и навыков:

Типовые вопросы-ситуации по оценке практических умений и навыков:

1. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T. Исходные данные – $P=10^{-6}$, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю.

2. Необходимо зашифровать исходное сообщение «Я учусь в КНИТУ-КАИ» шифром Гронсфельда, ключ К=193431.

3. Зашифровать сообщение «Я люблю свой университет» по методу Вижинера с помощью ключевого слова «Галактика».

6.2. Контрольные вопросы

1. Классификация подсистем идентификации и аутентификации пользователей.

2. Парольные подсистемы идентификации и аутентификации личности.

3. Количественная оценка стойкости парольной защиты.

4. Классификация защитных мер. Примеры.

5. Функции хэширования и электронно-цифровая подпись.

6. Разграничение доступа к ресурсам.

7. Политики безопасности. Классификация политик безопасности.

8. Политики избирательного разграничения доступа.

9. Проблема обеспечения целостности и подлинности информации.

10. Инфраструктура открытых ключей PKI.

11. Разграничение доступа к ресурсам. Мандатные политики безопасности.

12. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей.

13. Типовые схемы хранения ключевой информации.

14. Отечественный стандарт симметричного шифрования.

15. Межсетевые экраны. Классификация и принципы использования.

16. Методы и средства криптографической защиты.

17. Принципы криптографической защиты информации.

18. Традиционные симметричные криптосистемы.

19. Шифрование методом замены.

20. Шифрование методами перестановки.

21. Защита информации в компьютерных сетях.

22. Основные угрозы и причины уязвимости сети INTERNET.

23. Классификация типовых удаленных атак на интрасети.

24. Элементы криптоанализа.

25. Криптоанализ, основанный на исследовании частотности символов в тексте.

26. Защита информации в компьютерных сетях. Виртуальные частные сети (VPN).

27. Инженерно-техническая защита информации. Радиомикрофоны.

28. Правовое обеспечение информационной безопасности. Статья 272 УК РФ. Статья 273 УК РФ. Статья 274 УК РФ. Статья 146, нарушение авторских и смежных прав. Статья 147, нарушение изобретательских и патентных прав.

1. **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