Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт (факультет) **Институт компьютерных технологий и защиты информации**

Кафедра **Автоматизированных систем обработки информации и управления**

УТВЕРЖДАЮ
Ответственный за ОП
_____ М.П. Шлеймович
«31» 08 2017 г.
Регистрационный номер 4030.17.65

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине (модулю) или практике

«Защита информации»

(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.04.**

Направление подготовки: **09.03.02 «Информационные системы и технологии».**

Квалификация: **бакалавр.**

Профиль подготовки: **«Информационные системы».**

Вид(ы) профессиональной деятельности: **научно-исследовательская, производственно-технологическая.**

Заведующий кафедрой СИБ И.В.Аникин

Разработчик: старший преподаватель кафедры СИБ А.Р. Абзалов

Казань 2017 г.

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

«Защита информации»

(наименование дисциплины, практики)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению подготовки 09.03.02 «Информационные системы и технологии», учебному плану направления 09.03.02 «Информационные системы и технологии».

Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины. Они полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО. В составе ФОС имеются 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 применять знания, умения и навыки для решения профессиональных задач, соответствующих компетенциям, реализуемым дисциплиной.

Замечания отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методической комиссии

«31» августа 2017 г., протокол № 8.

Председатель УМК _____ _____ В.В. Родионов

Содержание

ВВЕДЕНИЕ 4

1. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ 5

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 5

3. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 5

4. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЯ ШКАЛЫ ОЦЕНИВАНИЯ 6

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРУ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ 11

6. КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 13

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ 18

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 09.03.02 «Информационные системы и технологии».

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 09.03.02 «Информационные системы и технологии» 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 8 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 «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	зачет	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-4	ОПК-4.З	зачет
2.	8	Политики информационной безопасности. Системы шифрования.	ОПК-4	ОПК-4.З ОПК-4.В	зачет
3	8	Особенности применения методов и средств защиты информации.	ОПК-4	ОПК-4.З ОПК-4.У ОПК-4.В ПК-17.З ПК-17.У ПК-17.В	зачет

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.	8	ОПК-4	ОПК-4.З ОПК-4.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	ОПК-4	ОПК-4.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

3.	8	ПК-17	ПК-17.З ПК-17.У	Теоретические навыки	Знание основных угроз информационной безопасности объектов и методы противодействия им. Умение анализировать направления развития информационно-коммуникационных технологий объекта защиты	Знание основных направлений развития информационно-коммуникационных технологий объекта защиты, методы оценки эффективности функционирования систем информационной безопасности, способы оценки затрат и рисков Умение прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации; - обосновывать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты	Знание: - типовых структур, принципов организации, средств и технологий обеспечения информационной безопасности объектов защиты; - современных методов обеспечения информационной безопасности, вновь вводимых отечественных и международных стандартов; Умение осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты; - анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им

4.	8	ПК-17	ПК-17.В	Практические навыки	Навыком построения модели угроз объекта	Навыками прогнозирования эффективности функционирования систем информационной безопасности, оценки затраты и рисков согласно известным методикам, формирования стратегий создания систем информационной безопасности в соответствии со стратегией развития организации	Навыками применения современных методов обеспечения информационной безопасности, внедрения на объекты защиты вновь вводимых и существующих отечественных и международных стандартов, навыками анализа угроз информационной безопасности объектов и разработки соответствующих методов противодействия им.

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	
Зачтено	от 86 до 100	Освоен **превосходный** уровень всех компетенций (составляющих компетенций)
Зачтено	от 71 до 85	Освоен **продвинутый** уровень всех компетенций (составляющих компетенций)
Зачтено	от 51 до 70	Освоен **пороговый** уровень всех компетенций (составляющих компетенций)
Не зачтено	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

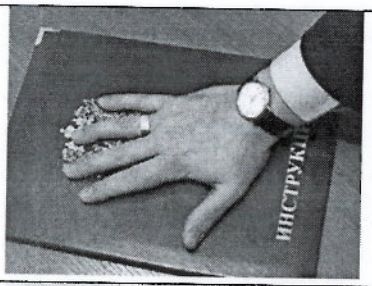
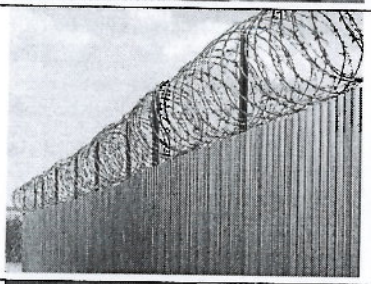
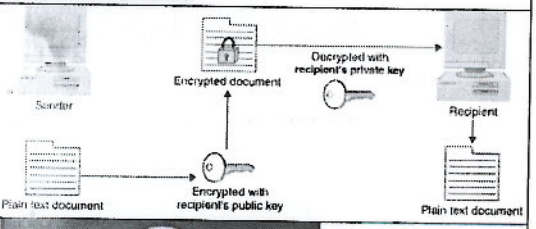
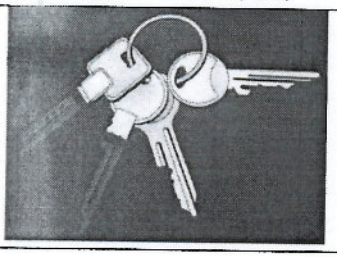
Формирование оценки по итогам освоения дисциплины

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 (зачет):					**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 «ФИО».

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.

Лист регистрации изменений

№ п/п	№ страницы внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» Председатель УМК ИКТЗИ
1	2	3	4	6
1	1	01.02.2019	Изменение наименования учредителя университета. В соответствии с утверждением устава федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский университет им. А.Н. Туполева-КАИ» в новой редакции (Приказ № 1042 от 26.11.2018) наименование «Министерство образования и науки Российской Федерации» читать как «Министерство науки и высшего образования Российской Федерации»	
2				
3				
4				
5				