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 **Систем информационной безопасности**

УТВЕРЖДАЮ

Ответственный за ОП

_____ И.В. Аникин

«31» 08 2017 г.

Регистрационный номер 4050-17/134-ф

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

«Защита информации в компьютерных сетях»

Индекс по учебному плану: **Б1.В.ДВ.10.01**

Направление подготовки: **10.03.01 «Информационная безопасность»**

Квалификация: **бакалавр**

Профиль: **Комплексная защита объектов информатизации**

Виды профессиональной деятельности: **эксплуатационная, проектно-технологическая, экспериментально-исследовательская, организационно-управленческая**

Заведующий кафедрой СИБ И.В. Аникин

Разработчик: к.т.н., доцент кафедры СИБ Л.А. Александрова

Казань 2017 г.

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

«Защита информации в компьютерных сетях»

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению 10.03.01 «Информационная безопасность», учебному плану направления 10.03.01 «Информационная безопасность».

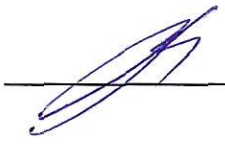
Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Защита информации в компьютерных сетях». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению 10.03.01 «Информационная безопасность». 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.

Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению 10.03.01 «Информационная безопасность» 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 4

1. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ 6

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 6

3. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В 6

ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 6

4. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЯ ШКАЛЫ ОЦЕНИВАНИЯ 7

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРУ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ 10

6 КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 12

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ 24

Введение

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации в компьютерных сетях» – 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 10.03.01 «Информационная безопасность».

Задачи ФОС по дисциплине «Защита информации в компьютерных сетях»

– 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 в компьютерных сетях» 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 в компьютерных сетях» разработан в соответствии с требованиями ФГОС ВО по напрвлению 10.03.01 «Информационная безопасность» 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 в компьютерных сетях» изучается в 1 семестре при очной форме обучения и завершается промежуточной аттестацией в форме зачета.

2. Оценочные средства для промежуточной аттестации

Таблица 1

Оценочные средств для промежуточной аттестации

(очная форма обучения)

№ п/п	Семестр	Форма промежуточной аттестации	Оценочные средства
1.	7	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 соответствующих разделов дисциплины 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.	7	Раздел 1. Основы защиты информации в компьютерных сетях	ПК-1 ПК-3	ПК-1.З ПК-1.У ПК-3.З ПК-3.У	экзамен

2.	7	Раздел 2. Средства защиты информации в компьютерных сетях	ПК-1 ПК-3	ПК-1.З ПК-1.У ПК-3.З ПК-3.У	экзамен
3	7	Раздел 3. Системы анализа защищенности компьютерных сетей	ПК-1 ПК-3 ПСК-3.4	ПК-1.З ПК-1.У ПК-1.В ПК-3.З ПК-3.У ПК-3.В ПСК-3.4.З ПСК-3.4.У ПСК-3.4.В	экзамен

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

Показатели и критерии оценивания сформированности компетенций, 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.	7	ПК-1. ПК-3 ПСК-3.4	ПК-1.З ПК-1.У ПК-3.З ПК-3.У ПСК-3.4.З ПСК-3.4.У	Теоретические навыки	- Иметь представление об общих основах по вопросам настройки и обслуживания программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять типовые работы по настройке технических и программно-аппаратных средств защиты информации. - Иметь представление об основных технологиях администрирования подсистем информационной безопасности. - Умение использовать основные информационные технологий по вопросам администрирования компьютерных сетей. - Знание основ организации аттестации объектов информатизации, в соответствии с нормативными документами.	- Владеть общими основами по вопросам установки, настройки и обслуживания программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять типовые работы по настройке и обслуживанию технических и программно-аппаратных средств защиты информации. - Знание базовых технологий администрирования подсистем информационной безопасности. - Умение применять основные информационные технологии администрирования компьютерных сетей. - Знание основ организации и сопровождения	- Владеть системой знаний по вопросам установки, настройки и обслуживанию программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации. - Владеть системой знаний о технологиях администрирования подсистем информационной безопасности. - Умение применять современные, перспективные информационные технологии администрирования компьютерных сетей. - Знание основ организации и сопровождения аттестации объектов информатизации в соответствии с требованиями стандартов сферы информационной безопасности. - Умение организовать и со-

					- Умение организовать аттестацию объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности.	аттестации объектов информатизации в соответствии с требованиями сферы информационной безопасности. - Умение организовать и сопровождать аттестацию объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности.	провождать аттестацию объектов информатизации в соответствии с требованиями стандартов сферы информационной безопасности.
2.	7	ПК-1. ПК-3 ПСК-3.4	ПК-1.В ПК-3.В ПСК-3.4.В	Практические навыки	- Владение базовыми технологиями в сфере проведения работ по настройке технических и программно-аппаратных средств защиты информации. - Владение основными понятиями администрирования подсистемами информационной безопасности. - Владение основными технологиями организации аттестации объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности.	- Владение основными технологиями проведения работ по настройке и обслуживанию технических и программно-аппаратных средств защиты информации. - Владение базовыми технологиями администрирования подсистемами информационной безопасности. - Владение основными технологиями организации и сопровождения аттестации объектов информатизации в соответствии с требованиями информационной безопасности.	- Владение технологиями проведения работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации. - Владение современными технологиями администрирования подсистемами информационной безопасности. - Владение технологиями организации и сопровождения аттестации объектов информатизации в соответствии требованиями стандартов сферы информационной безопасности.

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 «Международные и российские нормативно-правовые акты и стандарты в области обеспечения информационной безопасности» 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	промежуточной аттестации (экзамен)
Раздел 1. Основы защиты информации в компьютерных сетях	**20**			**20**	
Тест текущего контроля по разделу	20			20	
Раздел 2. Средства защиты информации в компьютерных сетях		**30**		**30**	
Тест текущего контроля по разделу		20		20	
Защита лабораторных работ		10		10	
Раздел 3. Системы анализа защищенности компьютерных сетей			**20**	**20**	
Защита лабораторных работ			20	20	
Промежуточная аттестация (экзамен):					**30**
– тест промежуточной аттестации по дисциплине					20
– ответы на контрольные вопросы					10

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

Межсетевой экран позволяет:

- блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов
- не допускать проникновение на защищаемый компьютер сетевых червей
- препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере
- видеть действия котрые выполняет пользователь на другом компьютере
- использовать принтер подключённый к другому компьютеру

- MAC-адрес является адресом:

- канального уровня
- сетевого уровня
- транспортного уровня
- прикладного уровня

- ip-адрес является адресом:

- канального уровня
- сетевого уровня
- транспортного уровня
- прикладного уровня

Доменное имя является адресом:

- канального уровня
- сетевого уровня
- транспортного уровня
- прикладного уровня

URL является адресом:

- канального уровня
- сетевого уровня
- транспортного уровня
- прикладного уровня

Решения по обеспечению информационной безопасности:

- Высокопроизводительные системы защиты каналов;
- Автоматизированные системы в защищенном исполнении;
- Защита периметра информационной системы;
- Все ответы верны.

Методические документы государственных органов России:

- руководящие документы ФСТЭК;
- приказы ФСБ;
- конституция РФ;
- указы президента.

Какие документы относятся к актам федерального законодательства:

- международные стандарты;

- международные договоры РФ;

- приказы ФСБ;

- указы президента РФ;

Целостность информации:

- свойство информационных ресурсов, заключающееся в возможности их изменения любым субъектом

- свойство информационных ресурсов, заключающееся в возможности их изменения только единственным пользователем

- свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения

- свойство информационных ресурсов, заключающееся в их существовании в виде единого набора файлов

ИСПДн::

- информационная система персональных данных

- информационная система по персонализации данных населения

- информационный сервис по защите персональных данных

- информационная система по управлению данными

Доступность информации:

- свойство системы, заключающееся в осуществлении беспрепятственного доступа к информационным ресурсам любых субъектов

- свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц

- свойство системы, заключающееся в осуществлении закрытого доступа к информации любых субъектов

- свойство информационных ресурсов, заключающееся в легкости их несанкционированного получения и дальнейшего распространения (несанкционированного копирования)

Типы ИС существуют:

- Специальные

- Простые

- Сложные

- Типовые

Конфиденциальность информации:

- свойство информационных ресурсов, заключающееся в их существовании в неискаженном виде (неизменном поотношению к некоторому фиксированному ее состоянию)
- свойство информационных ресурсов, заключающееся в их шифровании
- свойство информационных ресурсов, заключающееся в их недоступности для неуполномоченных лиц
- свойство информационных ресурсов, заключающееся в их существовании в виде не защищенного паролем набора

Принципы обеспечения информационной:

- неизменность
- системность
- непрерывность
- дешевизна
- комплексность
- Законность

Информационной безопасность (один ответ):

- конфиденциальность, целостность, доступность
- неприкосновенность, целостность, доступность
- конфиденциальность, целостность, публичность
- достоверность, доступность, целостность
- конфиденциальность, целостность, достоверность

Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов первоначальных данных?

- К4
- К1
- К3
- К2

Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов первоначальных данных?

- К4
- К1
- К3
- К2

Субъект персональных данных:

- физическое лицо
- любое физическое или юридическое лицо
- юридическое лицо
- оператор персональных данных

Для чего используется сертификат открытого ключа ЭЦП?

- для идентификации
- для аутентификации

- для авторизации
- для шифрования

Какие виды электронной подписи определены в ФЗ «Об электронной подписи»? (один ответ)

- квалифицированная электронная подпись и неквалифицированная электронная подпись
- простая электронная подпись, усиленная неквалифицированная электронная подпись,
- усиленная квалифицированная электронная подпись
- простая электронная подпись, и усложненная электронная подпись
- простая электронная подпись, квалифицированная электронная подпись

Что такое лицензирование?

- деятельность по выявлению электронных устройств, по предназначенных для негласного получения информации в помещениях и технических средствах
- допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну
- осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны
- мероприятия, связанные с выдачей лицензий на осуществление лицензируемых видов деятельности и надзор за соблюдением лицензиатами соответствующих лицензионных требований и условий

Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабаты-

ваемых в них, не приводит к значительным негативным последствиям для субъектов первоначальных данных?

- К4
- К1
- К3
- К2

18. Какие органы осуществляют контроль и надзор за соблюдением требований ФЗ-152? (один ответ)

- Роскомнадзор
- ФСБ, ФСТЭК, Роскомнадзор
- правительство РФ и ФСБ
- ФСБ и ФСТЭК

Какие процедуры включает в себя система ЭЦП? (один ответ)

- процедуру формирования и проверки цифровой подписи
- процедуру формирования цифровой подписи
- процедуру шифрования и формирования цифровой подписи
- процедуру проверки цифровой подписи

Сферы использования технологии PKI: (один овет)

- электронная коммерция
- электронный документооборот, web-приложения, VPN, электронная почта, электронная коммерция
- электронный документооборот

- электронный документооборот, web -приложения, VPN

VPN:

- обеспечивает защиту информации во время ее хранения на конечных компьютерах
- антивирусная защита
- межсетевой экран
- поддерживает сетевые протоколы аутентификации

Тип VPN Extranet позволяет:

- организовывать защищенное взаимодействие между компанией и ее партнерами, уровень доверия к которым такой же, как к своим сотрудникам
- организовывать защищенное взаимодействие между компанией ее партнерами, уровень доверия к которым намного ниже, чем к своим сотрудникам
- организовывать защищенное взаимодействие между филиалами одной компании (сегментами одной сети)
- организовывать защищенное взаимодействие между разными отделами одной компании

Для организации удаленного доступа, то есть для взаимодействия между сегментом корпоративной сети и удаленным пользователем, необходимо использовать:

Выберите один ответ:

- Extranet VPN
- Client-Server VPN
- Remote access VPN

- Intranet VPN

Тип VPN, который позволяет работать с сетями фирм-партнеров:

- Extranet
- Client-Server
- Intranet
- Remote access

Сколько бит содержит IPv4 адрес?

- 128
- 16
- 32
- 48

На каком уровне OSI работают мост и коммутатор?

- 3
- 4
- 1
- 2

На каком уровне OSI работают репитер и хаб? (один ответ)

- 3
- 4
- 1
- 2

Неправильный вариант ответа:

- хаб может проверить физический адрес (источник и пункт назначения),содержащиеся в пакете.
- хаб повторяет входные сигналы на всех своих портах, кроме того, с которого сигналы поступают
- хаб выполняет функцию восстановления электрических параметров сигнала
- хаб выполняет функцию объединения сегментов локальной сети на физическом уровне

Оценка практических умений и навыков

Типовые задачи:

- Опишите последовательность действий при использовании межсетевого экрана
- Опишите модель защиты индивидуальных сообщений
- Описать сценарий защиты потока сообщений
- Описать методику использования криптографических методов при защите сетевых сообщений

6.2. Контрольные вопросы

1. Модель сети. Межсетевая модель взаимодействия
2. Уровни взаимодействия сетевой модели и их характеристика
3. Протоколы сетевого уровня
4. Протоколы транспотного уровня
5. Протоколы верхнего уровня

6. Обеспечения подлинности сообщений
7. Принципы организации процедур подтверждения подлинности
8. Избыточность и способы ее организации
9. Процедура поддтверждения подлинности
10. Протоколы взаимной проверки подлинности
11. Функции подтверждения подлинности и их реализация
12. Конфиденциальность и шифрование. Три класса систем шифрования.
13. Истинные цифровые сигнатуры. Недостатки и преимущества
14. Защита потока сообщений
15. Защита протоколов передачи сообщений
16. Защита целостности процесса установления связи
17. Защита целостности процесса передачи данных
18. Защита целостности процесса завершения связи
19. Наблюдение за потоками сообщений в сети
20. Конфиденциальность потока сообщений
21. Защита потока сообщений.
22. Защита потока сообщений. Маскировка адресов назначения
23. Защита потока сообщений. Защита конфигурации сообщений.
24. Защита потока сообщений.. Защита трафика
25. Защита потока сообщений. Защита от наблюдения за установлением соединений
26. Защита потока сообщений. Маскировка отправителя.

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