

**Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ»
(КНИТУ-КАИ)**

Институт **Компьютерных технологий и защиты информации**
(наименование института, в состав которого входит кафедра, ведущая дисциплину)

Кафедра **Систем информационной безопасности**
(наименование кафедры, ведущей дисциплину)

АННОТАЦИЯ

**к рабочей программе
дисциплины (модуля)**

«Информационная безопасность телекоммуникационных систем»

Индекс по учебному плану: **Б1.Б.38**

Специальность: **10.05.02 «Информационная безопасность телекоммуникационных систем»**

Квалификация: **специалист по защите информации**

Специализация: **Защита информации в системах связи и управления**

Виды профессиональной деятельности: **научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная**

Ответственный за реализацию Образовательной программы 10.05.02

Заведующий кафедрой СИБ, к.т.н., доцент И.В. Аникин

Казань - 2017 г.

1. Цель и задачи учебной дисциплины

Цель изучения дисциплины: изучение и практическое освоение студентами методов и технологий обеспечения информационной безопасности (ИБ) корпоративных телекоммуникационных систем (ТКС) и сетей передачи данных (СПД) в процессе их эксплуатации.

Задачи изучения дисциплины:

- ознакомление с архитектурой и основными структурными элементами современных корпоративных ТКС и СПД;
- изучение принципов и методов построения инфраструктуры корпоративных ТКС на основе Модели Взаимодействия Открытых Систем (МВОС);
- изучение механизмов и технологий обеспечения интегральной информационной безопасности корпоративных ТКС и СПД;
- освоение методов и технологий интеграции корпоративных ТКС в государственную и международную информационную среду;
- изучение методических рекомендаций по проверке соответствия ТКС требованиям нормативно-правовых и методических документов в области информационной безопасности.

2. Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины

Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины: ПК-6, ПК-10.

3. Структура дисциплины и трудоемкость ее составляющих

Таблица. Распределение фонда времени по семестрам, неделям и видам занятий для очной формы обучения

Наименование раздела и темы	Всего часов	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах / интерактивные часы)				Коды составляющих компетенций	Формы и вид контроля освоения составляющих компетенций (из фонда оценочных средств)
		лекции	ла. раб.	пр. зан.	сам. раб.		
Раздел 1. Архитектура, структурный состав и методы реализации корпоративных ТКС на основе МВОС							ФОС ТК-1
Тема 1.1. Архитектура и структурный состав корпоративных ТКС	26	2/2	–	–	24	ПК-6.3	Тесты
Тема 1.2. Принципы и методы построения ТКС на основе МВОС	58	4/4	6/6	–	48	ПК-6.3 ПК-6.У ПК-6.В	Тесты, отчет о выполнении лаб. раб.

<i>Раздел 2. Принципы, методы и технологии обеспечения интегральной безопасности корпоративных ТКС и СПД</i>							ФОС ТК-2
Тема 2.1. Интегральная безопасность корпоративных ТКС и СПД	60	12/12	12/12	–	36	ПК-6.3 ПК-6.У ПК-6.В	Тесты, отчет о выполнении лаб. раб.
Экзамен	36	–	–	–	36	ПК-6.3 ПК-6.У ПК-6.В	<i>ФОС ПА-1 - комплексное задание</i>
Всего за семестр:	180	18/18	18/18	–	144		
<i>Раздел 3. Обеспечение ИБ в рамках сервис-ориентированных архитектур (СОА) корпоративных ТКС</i>							ФОС ТК-3
Тема 3.1. ИБ ТКС как совокупность сервисов СОА	42	6/6	–	–	36	ПК-10.3 ПК-10.У	Тесты
<i>Раздел 4. Комплексная задача мониторинга и проверки ИБ в гетерогенных инфокоммуникационных средах ТКС и СПД</i>							ФОС ТК-4
Тема 4.1. Обеспечение ИБ в виртуальных и «облачных» средах ТКС	46	4/4	6/6	–	36	ПК-10.3 ПК-10.В	Тесты, отчет о выполнении лабораторной работы
Тема 4.2. Мониторинг и аудит ИБ ТКС в процессе эксплуатации	56	8/8	12/12	–	36	ПК-10.3 ПК-10.У ПК-10.В	Тесты, отчет о выполнении лабораторной работы
Экзамен	36	–	–	–	36	ПК-10.3 ПК-10.У ПК-10.В	<i>ФОС ПА-2 - комплексное задание</i>
Всего за семестр:	180	18/18	18/18	–	144		
ИТОГО:	360	36/36	36/36	–	288		

4. Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1. Основная литература

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для студ. вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2014. – 944с.
2. Мельников В.П. Защита информации: учебник / В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе – М.: Академия, 2014. – 304 с.

4.2. Основное информационное обеспечение дисциплины (модуля)

Основное информационное обеспечение по дисциплине «Информационная безопасность телекоммуникационных систем» размещено в электронной образовательной среде Black Board. [Электронный ресурс]: web-портал <http://>

www.bb.kai.ru/. - Режим доступа: Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=_95397_1&course_id=_9723_1&mode=reset.

5. Кадровое обеспечение дисциплины (модуля)

5.1. Базовое образование

Высшее образование в области информационной безопасности или информатики и вычислительной техники и /или наличие ученой степени и/или ученого звания в указанной области и /или наличие дополнительного профессионального образования – профессиональной переподготовки в области информационной безопасности или информатики и вычислительной техники и /или наличие заключения экспертной комиссии о соответствии квалификации преподавателя профилю преподаваемой дисциплины.

5.2. Профессионально-предметная квалификация преподавателей

Наличие научных и/или методических работ по организации или методическому обеспечению образовательной деятельности по направлению информационной безопасности, выполненных в течение трех последних лет.

5.3. Педагогическая (учебно-методическая) квалификация преподавателей

К ведению дисциплины допускаются кадры, имеющие стаж научно-педагогической работы (не менее 1года), практический опыт работы в области информационной безопасности на должностях руководителей или ведущих специалистов более 3 последних лет.

Обязательное прохождение повышения квалификации (стажировки) не реже чем один раз в три года соответствующее области информационной безопасности, информатики и вычислительной техники, либо в области педагогики.