

**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)**

«Инженерно-техническая защита информации»

Индекс по учебному плану: **Б1.В.08**

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:

Обучить студентов знаниям, умениям и навыкам:

- определять задачи подсистемы технической защиты информации в комплексной системе защиты информации объекта;
- внедрять и эксплуатировать средства технической защиты информации;
- организовывать контроль эффективности подсистемы технической защиты информации и выполнению основных операций контроля.

Задачи изучения дисциплины:

Дать основы:

- технических методов и средств несанкционированного вмешательства в информационные процессы объекта защиты,
- технических методов противодействия несанкционированному вмешательству,
- работы с руководящими документами по технической защите информации, в том числе, документами, регламентирующими деятельность в этой области,
- методов анализа объектов защиты, разработки концепции технической защиты информации, реализации разработанной концепции и оценки эффективности подсистемы технической защиты информации.

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

Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины: ПК-9, ПСК-10.3, ПСК-10.4.

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. Характеристики угроз безопасности информации. Способы и средства добывания информации техническими средствами.							ФОС ТК-1

Тема 1.1. Введение	9/1	1	4/1	–	5	ПК 9.3 ПСК 10.3.3 ПСК 10.4.3	Тесты, отчет о выпол- нении лабора- торной работы
Тема 1.2. Объекты инфор- мационной защиты часть 1	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У	Тесты, отчет о выпол- нении лабора- торной работы
Тема 1.3. Объекты инфор- мационной защиты часть 2	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У	Тесты, отчет о выпол- нении лабора- торной работы
Тема 1.4. Характеристики угроз безопасности ин- формации	7/1	2/1	–	–	5	ПК 9.3 ПК 9.У ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У	Тесты
Тема 1.5. Способы и сред- ства добывания информа- ции техническими средст- вами	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У	Тесты, отчет о выполнении лабораторной работы
<i>Раздел 2. Технические каналы утечки информации. Концепция технической защиты информации. Способы и средства технической защиты. Организа- ци-онные меры по технической защите информации.</i>							<i>ФОС ТК-2 те- сты</i>
Тема 2.1. Технические ка- налы утечки информации	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У ПСК 10.3.В ПСК 10.4.В	Тесты, отчет о выпол- нении лабора- торной работы
Тема 2.2. Технические ка- налы утечки информации часть 2	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У ПСК 10.3.В ПСК 10.4.В	Тесты, отчет о выпол- нении лабора- торной работы

Тема 2.3. Технические каналы утечки информации часть 3	11/2	2/1	4/1	–	5	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У ПСК 10.3.В ПСК 10.4.В	Тесты, отчет о выполнении лабораторной работы
Тема 2.4. Концепция технической защиты информации	13/2	2/1	4/1	–	7	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У ПСК 10.3.В ПСК 10.4.В	Тесты, отчет о выполнении лабораторной работы
Тема 2.5. Способы и средства технической защиты	11/2	1/1	4/1	–	7	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У	Тесты, отчет о выполнении лабораторной работы
Экзамен	36	–	–	–	36	ПК 9.3 ПК 9.У ПК 9.В ПСК 10.3.3 ПСК 10.4.3 ПСК 10.3.У ПСК 10.4.У ПСК 10.3.В ПСК 10.4.В	<i>ФОС ПА - комплексное задание</i>
ИТОГО:	144/18	36/9	36/9	–	90		

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

4.1. Основная литература

1. *Петровский В.И.* Инженерно-техническая защита информации : учеб. пособие / В. И. Петровский, В. В. Петровский, В. И. Глова ; Мин-во образ-я и науки РФ, ФГБОУ ВПО КНИТУ-КАИ им. А.Н. Туполева. - Казань : Изд-во КГТУ им. А.Н. Туполева Т.1 : Организационная защита информации. - 2012. - 439 с.

2. *Петровский В.И.* Инженерно-техническая защита информации : учеб. пособие / В. И. Петровский, В. В. Петровский, В. И. Глова ; Мин-во образ-я и науки РФ, ФГБОУ ВПО КНИТУ-КАИ им. А.Н. Туполева. - Казань : Изд-во КГТУ им. А.Н. Туполева Т.2 : Организационная защита информации. 2012. – 511 с.

3. 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)

Корнилов Г.С. Инженерно-техническая защита информации [Электронный ресурс]: курс дистанц. обучения по направлению подготовки специалистов 10.05.02 «Информационная безопасность телекоммуникационных систем» ФГОСЗ+ / КНИТУ-КАИ, Казань, 2016 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=_86247_1&course_id=_9577_1

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.