**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)

Регистрационный № \_\_\_\_\_\_\_\_\_

**АННОТАЦИЯ**

**к рабочей программе**

дисциплины (модуля)

**«Введение в профессиональную деятельность»**

Индекс по учебному плану: **Б1.Б.12**

Специальность: **10.03.01 «Информационная безопасность»**

Квалификация: **бакалавр**

Профили: **Организация и технология защиты информации  
Комплексная защита объектов информатизации**

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

Разработчик: доцент кафедры Систем информационной безопасности, к.т.н., доцент

\_\_\_\_\_\_\_\_\_\_\_ Александрова Л.А.

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: раскрытие основных положений Федерального Государственного образовательного стандарта по специальности, подготовка к профессиональной деятельности в области обеспечения информационной безопасности телекоммуникационных систем.

Задачи изучения дисциплины:

- раскрытие социальной значимости и сущности будущей профессии;

- раскрытие составляющих квалификационной характеристики специалиста по защите информации;

- раскрытие основных терминов, задач и принципов информационной безопасности общества, государства, личности;

- формирование практических навыков организации информационной деятельности;

- формирование ответственности за социальную значимость профессии.

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

Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины: ОК-5.

## 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. Социальная значимость специалиста информационной безопасности.* | | | | | | | | | | | | | *ФОС ТК-1* | |
| Тема 1.1. Сущность и значение специальности | 6/1 | | 2/1 | | – | | – | | 4 | | ОК-5.З | | Тесты | |
| Тема 1.2. Квалификационная характеристика специалиста | 4/1 | | 2/1 | | – | | – | | 2 | | ОК-5.З | | Тесты | |
| *Раздел 2. Защита информации и информационная безопасность* | | | | | | | | | | | | | *ФОС ТК-2* | |
| Тема 2.1. Основные понятия в области систем обеспечения информационной безопасности и защиты информации | 12/2 | | 4/2 | | – | | – | | 8 | | ОК-5.З | | Тесты | |
| Тема 2.2. Задачи и принципы построения защищенных информационных систем | 6/1 | | 2/1 | | – | | – | | 4 | | ОК-5.З | | Тесты | |
| Тема 2.3. Информационная безопасность телекоммуникационных систем | 12/1 | | 2/1 | | – | | – | | 10 | | ОК-5.З  ОК-5.У  ОК-5.В | | Тесты,  отчет о выполнении самостоятельной работы | |
|  |  | |  | |  | |  | |  | |  | |  | |
| *Раздел 3. Правовая защита информационной безопасности* | | | | | | | | | | | | | *ФОС ТК-3* | |
| Тема 3.1. Роль правовой защиты в сфере информационной безопасности | 12/1 | | 2/1 | | – | | – | | 10 | | ОК-5.З  ОК-5.У  ОК-5.В | | Тесты,  отчет о выполнении самостоятельной работы | |
| Тема 3.2.Уголовная и административная ответственность за нарушение информационной безопасности | 20/2 | | 4/2 | | – | | – | | 16 | | ОК-5.З  ОК-5.У  ОК-5.В | | Тесты,  отчет о выполнении самостоятельной работы | |
| Зачет |  | |  | |  | |  | |  | | ОК-5.З  ОК-5.У  ОК-5.В | | *ФОС ПА - комплексное задание* | |
| ИТОГО: | 72/9 | | 18/9 | | – | | – | | 54 | |  | |  | |

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

### 4.1. Основная литература

1. Введение в информационную безопасность : учеб. пособие для студ. вузов / А. А. Малюк [и др.] ; под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2014. - 288 с.

2. Мельников В.П. Защита информации: учебник /В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе – М.:Академия, 2014. – 304 с.

### 4.2. Основное информационной обеспечение дисциплины (модуля)

1. Александрова Л.А. Введение в профессиональную деятельность. [Электронный ресурс]: курс дистанц. обучения по направлению подготовки специалистов 10.03.01. «Информационная безопасность» ФГОС3+ / КНИТУ-КАИ, Казань, 2016 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/announcement?method=search&context=course&course\_id=\_11834\_1&handle=cp\_announcements&mode=cpview

## 5. Материально-техническое обеспечение дисциплины (модуля)

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование раздела (темы)  дисциплины | Наименование учебной лаборатории, аудитории, класса *(с указанием номера аудитории и учебного здания)* | Перечень лабораторного оборудования, специализированной мебели и технических средств обучения | Количество  единиц |
| Разделы 1-3 | 7 зд., ауд. 425, 429м, 429 | Проекционный экран размера не менее 100 см ×150 см | 1 |
| Проектор, предназначенный для проведения презентаций и лекций в аудиториях на 20 человек | 1 |
| Персональный компьютер преподавателя для обеспечения работы проектора, подключенный к локальной и глобальной вычислительным сетям, с установленным пакетом прикладных программ Microsoft Office 2010 (или выше). | 1 |

## 6. Кадровое обеспечение дисциплины (модуля)

**6.1. 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.

**6.2. 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.

**6.3. 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.