

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)



УТВЕРЖДАЮ

Проректор по ОД

Н.Н. Маливанов

«26» апреля 2017 г.

Регистрационный номер 4050-17/65

**РАБОЧАЯ ПРОГРАММА**

дисциплины (модуля)

**«Введение в профессиональную деятельность»**

Индекс по учебному плану: **Б1.Б.12**

Направление: **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**


Казань 2017 г.

Рабочая программа составлена на основе Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации от «1» декабря 2016 г. № 1515 и в соответствии с учебным планом направления 10.03.01 «Информационная безопасность», утвержденным Ученым советом КНИТУ-КАИ «29» апреля 2015 г., протокол № 4, с изменениями от «28» декабря 2016 г., протокол № 9.

Рабочая программа дисциплины (модуля) разработана к.т.н., доцентом кафедры СИБ Александровой Л.А. 

Утверждена на заседании кафедры СИБ, протокол №1 от 20 января 2017 г.

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

Рабочая программа дисциплины (модуля)	Наименование подразделения	Дата	№ протокола	Подпись
СОГЛАСОВАНА	Кафедра СИБ	20.01.2017	1	 заведующий кафедрой СИБ
ОДОБРЕНА	Учебно-методическая комиссия института КТЗИ	23.01.2017	1	 председатель УМК ИКТЗИ
СОГЛАСОВАНА	Научно-техническая библиотека			 директор ИТБ
СОГЛАСОВАНА	УМУ			 начальник УМУ



## РАЗДЕЛ 1. ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 1.1. Цель изучения дисциплины (модуля)

Основной целью изучения дисциплины является раскрытие основных положений федерального государственного образовательного стандарта по специальности, подготовка к профессиональной деятельности в области обеспечения информационной безопасности телекоммуникационных систем

### 1.2. Задачи дисциплины (модуля)

Основными задачами дисциплины являются:

- 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.

### 1.3. Место дисциплины (модуля) в структуре ОП ВО

Дисциплина «Введение в профессиональную деятельность» изучается в первом семестре и входит в состав базовой части блока «Б1. Дисциплины (модули)».

### 1.4. Объем дисциплины (модуля) (с указанием трудоемкости всех видов учебной работы)

Таблица 1

Объем дисциплины (модуля) для очной формы обучения

Виды учебной работы	Общая трудоемкость		Семестр	
	в ЗЕ	в час	1	
			в ЗЕ	в час
<b>Общая трудоемкость дисциплины (модуля)</b>	<b>2</b>	<b>72</b>	<b>2</b>	<b>72</b>
<i>Аудиторные занятия</i>	<i>0,5</i>	<i>18</i>	<i>0,5</i>	<i>18</i>
Лекции	0,5	18	0,5	18
Лабораторные работы				
Практические занятия				
<b>Самостоятельная работа студента</b>	<b>1,5</b>	<b>54</b>	<b>1,5</b>	<b>54</b>
Проработка учебного материала	1,5	54	1,5	54
Курсовой проект				
Курсовая работа				
Подготовка к промежуточной аттестации				
Промежуточная аттестация:	<b>Зачет</b>			



## 1.5. Планируемые результаты обучения

Таблица 2

### Формируемые компетенции

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)	Уровни освоения составляющих компетенций		
	Пороговый	Продвинутый	Превосходный
<b>ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</b>			
<b>Знание</b> - основных квалификационных характеристик специалиста по защите информации, основных задач и принципов информационной безопасности общества, государства, личности, основных информационных источников в области обеспечения информационной безопасности.	Иметь представление об основах социальной значимости будущей профессии, основных задачах информационной безопасности общества, государства, личности, информационных источниках в области обеспечения информационной безопасности	Знание основ социальной значимости будущей профессии, основных задач информационной безопасности, информационных источников в области обеспечения информационной безопасности	Знание социальной значимости будущей профессии, основных задач информационной безопасности общества, государства, личности, информационных источников в области обеспечения информационной безопасности
<b>Умение</b> - Умение донести до общества, отдельных личностей проблемы информационной безопасности не только физических, но и юридических лиц.	Умение формулировать мотивацию к выполнению простейшей профессиональной деятельности	Умение формулировать проблемы и мотивацию к выполнению простейшей профессиональной деятельности	Умение донести до общества, отдельных личностей проблемы и мотивацию к выполнению профессиональной деятельности
<b>Владение</b> - навыками выявления проблем информационной безопасности и определения приоритета решаемых задач.	Владение навыками аргументирования основных проблем информационной безопасности	Владение навыками аргументирования проблем информационной безопасности	Владение навыками аргументирования проблем информационной безопасности и определения приоритета решаемых задач



## РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) И ТЕХНОЛОГИЯ ЕЕ ОСВОЕНИЯ

### 2.1. Структура дисциплины (модуля), ее трудоемкость

Распределение фонда времени по видам занятий

Таблица 3

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-5.3	Тесты
Тема 1.2. Квалификационная характеристика специалиста	4/1	2/1	–	–	2	ОК-5.3	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-5.3	Тесты
Тема 2.2. Задачи и принципы построения защищенных информационных систем	6/1	2/1	–	–	4	ОК-5.3	Тесты
Тема 2.3. Информационная безопасность телекоммуникационных систем	12/1	2/1	–	–	10	ОК-5.3 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-5.3 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-5.3 ОК-5.У ОК-5.В	Тесты, отчет о выполнении самостоятельной работы
Зачет						ОК-5.3 ОК-5.У ОК-5.В	ФОС ПА - комплексное задание
ИТОГО:	72/9	18/9	–	–	54		

Матрица компетенций по разделам РП

Наименование раздела (тема)	Формируемые компетенции (составляющие компетенций)		
	ОК-5		
	ОК-5.3	ОК-5.У	ОК-5.В
Раздел 1			
Тема 1.1.	*		
Тема 1.2.	*		
Раздел 2			
Тема 2.1.	*		
Тема 2.2.	*		
Тема 2.3.	*	*	*
Раздел 3			
Тема 3.1.	*	*	*
Тема 3.2.	*	*	*

## 2.2. Содержание дисциплины (модуля)

### *Раздел 1. Социальная значимость специалиста информационной безопасности*

#### *Тема 1.1. Сущность и значение специальности*

Подготовка специалистов в области ИБ, актуальность введения специальностей по направлению «Информационная безопасность», направления и специальности высшего образования. Сущность и отличительные особенности специальности, характеристика ее составляющих; взаимосвязь специальности с другими специальностями в области информационной безопасности.

**Литература:** [1, стр.3-10].

#### *Тема 1.2. Квалификационная характеристика специалиста*

Объекты профессиональной деятельности специалиста. Виды профессиональной деятельности, место специальности в области науки и техники; объекты и виды профессиональной деятельности выпускника по специальности; требования Государственного образовательного стандарта к уровню подготовки специалиста;

Задачи в области экспериментально-исследовательской, проектной, управленческой и эксплуатационной деятельности по защите информации, к решению которых должен быть подготовлен специалист.

**Литература:** [1, стр.11-17].

### *Раздел 2.. Защита информации и информационная безопасность*



### ***Тема 2.1. Основные понятия в области систем обеспечения информационной безопасности и защиты информации***

Защита информации, информационная безопасность. Информационное общество, особенности и проблемы информационной безопасности телекоммуникационных систем.

Угрозы ИБ, атаки, риски в системах защиты информации. Каналы утечки информации.

**Литература:** [1, стр.40-80], [2, стр.156-164].

### ***Тема 2.2. Задачи и принципы построения защищенных информационных систем***

Задачи целостности, доступности, достоверности, конфиденциальности, аутентификации источника, протоколируемости. Виды аутентификации. Модели парольной аутентификации. Принципы построения защищенной информационной системы. Концепция защищенной информационной системы. Направления защиты.

**Литература:** [1, стр.104-106], [2, стр.156-164].

### ***Тема 2.3. Информационная безопасность телекоммуникационных систем***

Прообразы вычислительных сетей. Глобальные и локальные сети. Сетевые протоколы, среда передачи данных, коммуникационные подсети. Виды топологии сети (преимущества и недостатки с позиций информационной безопасности). Цифровая подпись и технологии ее использования. Виды компьютерных преступлений с использованием телекоммуникационных сетей.

**Литература:** [2, стр.203-290].

## ***Раздел 3. Правовая защита информационной безопасности***

### ***Тема 3.1. Роль правовой защиты в сфере информационной безопасности***

Направления защиты: организационная, инженерно-техническая, правовая. Роль правовой защиты и ее нормативно-методическое наполнение.

**Литература:** [2, стр.8-14].

### ***Тема 3.2. Уголовная и административная ответственность за нарушение информационной безопасности***

Нормативно-методическая база правовой защиты информации. Основные законы сферы информационной безопасности. Модели компьютерных преступлений, модели злоумышленников. Преступления сферы информационной безопасности, уголовная и административная ответственность.

**Литература:** [2, стр.8-42].

## **2.3. Курсовой проект / курсовая работа**

Курсовое проектирование по дисциплине в соответствии с учебным планом не предусмотрено.

## РАЗДЕЛ 3. ОЦЕНОЧНЫЕ СРЕДСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) И КРИТЕРИИ ОЦЕНОК ОСВОЕНИЯ КОМПЕТЕНЦИЙ

### 3.1. Оценочные средства для текущего контроля

Фонд оценочных средств для проведения текущего контроля (ФОС ТК) является составной частью РП дисциплины (модуля) и хранится на кафедре.

Фонд оценочных средств текущего контроля

№ п/п	Наименование раздела (модуля)	Вид оценочных средств	Примечание
1	2	3	4
1.	Социальная значимость специалиста информационной безопасности	ФОС ТК-1	Тест текущего контроля дисциплины по первому разделу (модулю) (ФОС ТК-1)
2.	Защита информации и информационная безопасность	ФОС ТК-2	Тест текущего контроля дисциплины по второму разделу (модулю) (ФОС ТК-2)
3.	Правовая защита информационной безопасности	ФОС ТК-3	Отчет о выполнении самостоятельной работы. Тест текущего контроля дисциплины по второму разделу (модулю) (ФОС ТК-3)

#### Типовые оценочные средства для текущего контроля

##### Типовые тестовые задания

МС Что такое ООП?

- Набор организационно- методических документов correct
- Документ-программа обучения специалиста incorrect
- Образовательная обучающая программа incorrect
- Организационный документ incorrect

МА Квалификация выпускника ?

- бакалавр correct
- магистр incorrect
- специалист incorrect
- техник по защите incorrect

МА Статьи Уголовного кодекса о компьютерных нарушениях распространяются на:

- любую информацию incorrect,
- только на гостайну incorrect,
- на информацию, охраняемую законом correct,
- на информацию, хранящуюся на серверах предприятий incorrect



### ***Типовые вопросы по самостоятельной работе***

1. Что такое модель и как описать модель компьютерного преступления и модель злоумышленника?
2. Какие объекты и субъекты защиты в созданных моделях.

### **3.2. Оценочные средства для промежуточного контроля.**

Фонд оценочных средств для проведения промежуточной аттестации (ФОС ПА) является составной частью РП дисциплины, разработан в виде отдельного документа в соответствии с положением о ФОС ПА.

#### **Первый этап: типовые тестовые задания**

МА Найдите верные высказывание:

- идентификация выполняется перед аутентификацией correct
- авторизация выполняется вместо аутентификации incorrect
- идентификация и аутентификация - это процессы проверки подлинности пользователя, объекта, процесса incorrect
- авторизация процесс, который выполняется за процессом аутентификации correct

#### **Второй этап: контрольные вопросы**

1. Объекты и субъекты модели компьютерного преступления
2. Угрозы и уязвимости модели компьютерного преступления.
3. Возможные инциденты.

### **3.3. Форма и организация промежуточной аттестации по итогам освоения дисциплины**

По итогам освоения дисциплины проводится зачет: **тестирование** и(или) **письменный ответ на контрольные вопросы** и(или) **защита выполненной самостоятельной работы**.

**Тестирование** ставит целью оценить пороговый уровень освоения обучающимися заданных результатов, а также знаний и умений, предусмотренных компетенциями.

Для оценки превосходного и продвинутого уровня усвоения компетенций проводится **второй этап**.

### 3.4. Критерии оценки промежуточной аттестации

Результаты промежуточного контроля заносятся в АСУ «Деканат» в баллах.

Таблица 5

Система оценки промежуточной аттестации

Описание оценки в требованиях к уровню и объему компетенций	Выражение в баллах	Словесное выражение
Освоен превосходный уровень усвоения компетенций	от 86 до 100	Зачтено
Освоен продвинутый уровень усвоения компетенций	от 71 до 85	Зачтено
Освоен пороговый уровень усвоения компетенций	от 51 до 70	Зачтено
Не освоен пороговый уровень усвоения компетенций	до 51	Не зачтено



## **РАЗДЕЛ 4. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

### **4.1. Учебно-методическое обеспечение дисциплины (модуля)**

#### **4.1.1. 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.

#### **4.1.2. Дополнительная литература**

1. Абзалов А.Р. Правовая защита информации : учеб. пособие /А. Р. Абзалов [и др.] ; Мин-во образования и науки РФ, ФГБОУ ВПО КНИТУ-КАИ им. А.Н. Туполева. - Казань: Изд-во КГТУ им. А.Н. Туполева, 2011. - 98 с.

2. Основы управления информационной безопасностью: учеб. пособие для студ. вузов /А. П. Курило [и др.]. - М. : Горячая линия - Телеком, 2014. - 244 с.

#### **4.1.3. Методическая литература к выполнению практических и/или лабораторных работ**

Практические и лабораторные работы не предусмотрены.

#### **4.1.4. Методические рекомендации для студентов, в том числе по выполнению самостоятельной работы**

Изучение лекционного материала выполняется с использованием личных записей студента и рекомендованной литературы. В результате самоподготовки студент должен ответить на контрольные вопросы по разделам курса, приведенным в рабочей программе дисциплины.

В соответствии с программой курса студент должен выполнить самостоятельную работу и по результатам ее выполнения оформить отчет. Самостоятельная работа засчитывается после защиты отчета. При сдаче отчета студент должен дать развернутые ответы на контрольные вопросы.

#### **4.1.5. Методические рекомендации для преподавателей**

Изучение дисциплины производится последовательно в соответствии с тематическим планом. Выполнению каждой лабораторной работы и самостоятельному изучению материала предшествует лекция по соответствующей теме.

Для успешного усвоения материала каждому студенту предоставляются в электронном виде материалы, отражающие основные положения теоретических основ и практических методов, изучаемых в дисциплине.

В качестве оценочных средств текущего контроля успеваемости и промежуточной аттестации предлагается использовать тесты и контрольные вопросы.



## **4.2. Информационное обеспечение дисциплины (модуля)**

### **4.2.1. Основное информационное обеспечение**

1. Александрова Л.А. Введение в профессиональную деятельность. [Электронный ресурс]: курс дистанц. обучения по направлению подготовки специалистов 10.03.01. «Информационная безопасность» ФГОСЗ+ / 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](https://bb.kai.ru:8443/webapps/blackboard/execute/announcement?method=search&context=course&course_id=_11834_1&handle=cp_announcements&mode=cpview)

### **4.2.2. Дополнительное справочное обеспечение**

1. Александрова Л.А. Дополнительные электронные ресурсы по дисциплине «Введение в профессиональную деятельность» [Электронный ресурс]: курс дистанц. обучения по направлению подготовки специалистов 10.03.01. «Информационная безопасность» ФГОСЗ+ / КНИТУ-КАИ, Казань, 2016 – Доступ по логину и паролю. URL: [https://bb.kai.ru:8443/webapps/blackboard/execute/announcement?method=search&context=course\\_entry&course\\_id=\\_2383\\_1&handle=announcements\\_entry&mode=view](https://bb.kai.ru:8443/webapps/blackboard/execute/announcement?method=search&context=course_entry&course_id=_2383_1&handle=announcements_entry&mode=view)

## **4.3. Кадровое обеспечение**

### **4.3.1. 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.

### **4.3.2. 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.

### **4.3.3. 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.



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

В табличной форме указывается наименование основных и специализированных учебных лабораторий/аудиторий/кабинетов с перечнем специализированной мебели и технических средств обучения, средств измерительной техники и др., необходимых для освоения заданных компетенций.

Таблица 6

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

### 5.1. Лист регистрации изменений, вносимых в рабочую программу дисциплины (модуля)


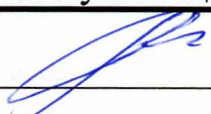
## Лист регистрации изменений

[illegible]



**5.2. Лист утверждения рабочей программы дисциплины (модуля) на учебный год**

Рабочая программа дисциплины(модуля) утверждена на ведение учебного процесса в учебном году:

Учебный год	«Согласовано» Заведующий кафедрой, реализующей дисциплину	«Согласовано» Председатель УМК института, в состав которого входит выпускающая кафедра
2016 / 2017		
2017 / 2018		
2018 / 2019		
2019 / 2020		
2020 / 2021		