

106

СМК  
Ф7.2.2.11.01./01/00

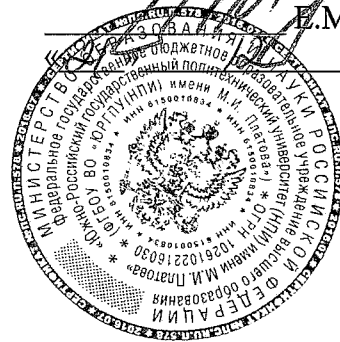
**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«ЮЖНО-РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ**  
**ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (НПИ) ИМЕНИ М.И. ПЛАТОВА»**

**УТВЕРЖДАЮ:**

Проректор по ОДЮРПУ (НПИ)

Е.М. Дьяконов

2016 г.



## **РАБОЧАЯ ПРОГРАММА**

**Б2.У.1**            **«Ознакомительная практика»**  
**10.05.02**        **«Информационная безопасность»**  
                      **Специализация: «Защита информации в системах связи и управления»**

Военный институт  
Кафедра    Информационная безопасность  
Курс        1  
Семестр    2

программа специалитета  
набор 2017 г.

**ИТОГО по дисциплине 3 /108 (ЗЕ / ч.)**  
**(с учетом ЗЕ/часов на экзамен)**

2016 г.

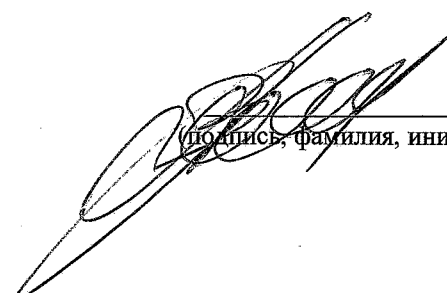
Рабочая программа составлена на основании рабочего учебного плана, утвержденного Ученым советом ЮРГПУ (НПИ) протоколом №4 от 21.12.2016 г.

Рабочую программу составил заведующий кафедрой ИБ к.в.н. доцент Баранов В.В.  
ученое звание, степень, должность, фамилия, инициалы

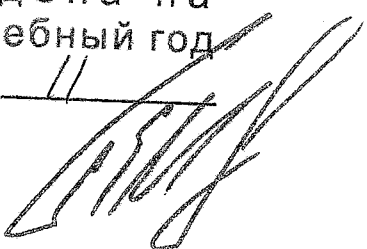
Рабочая программа обсуждена на заседании кафедры ИБ  
Наименование кафедры

Утверждена « 15 » мая 2017 г. Протокол № 13

Заведующий кафедрой ИБ

 / Баранов В.В. /  
(подпись, фамилия, инициалы)

Рабочая программа  
переутверждена на  
20 17 / 20 18 учебный год  
с обновлениями п. 11

Проректор по ОД 

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ.....	4
1. ВИД ПРАКТИКИ, СПОСОБЫ И ФОРМА ЕЕ ПРОВЕДЕНИЯ .....	4
2. ОБЪЕМ ПРАКТИКИ.....	4
3. ЦЕЛИ И ЗАДАЧИ. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ .....	4
4. СОДЕРЖАНИЕ ПРАКТИКИ.....	6
5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ .....	6
6. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ .....	6
7. ПРОИЗВОДСТВЕННАЯ РАБОТА И ПРИОБРЕТЕНИЕ КВАЛИФИКАЦИИ.....	8
8. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ .....	8
9. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРАКТИКЕ .....	8
10. ЛИТЕРАТУРА .....	14
11. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ИСПОЛЬЗУЕМЫЕ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ .....	16
12. МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ ПЕРЕД НАЧАЛОМ ПРАКТИКИ .....	16

## **ВВЕДЕНИЕ**

Ознакомительная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности) по специализации «Защита информации в системах связи и управления» является одним из важных этапов профессиональной подготовки студентов. Мероприятие организуется и проводится выпускающей кафедрой. Целенаправленная, активная работа студента во время Ознакомительной практики – обязательное условие успешной подготовки к будущей профессиональной деятельности. Одна из основных целей ознакомительной практики – познакомить студентов с обязанностями, которые выполняет специалист по защите информации в системах связи и управления, принципами работы с деловой документацией, а также с объектами информатизации, программно-аппаратными и техническими средствами защиты информации, защищенными информационными системами и др.

### **1. ВИД ПРАКТИКИ, СПОСОБЫ И ФОРМА ЕЕ ПРОВЕДЕНИЯ**

*Вид практики* - учебная.

*Тип практики* - ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности).

*Способ проведения практики* - стационарная или выездная.

*Форма проведения практики* - дискретная.

Место в структуре основной образовательной программы – Б2.У.1, обеспечивает ознакомление студентов с будущей профессиональной деятельностью на основе профессиональной подготовки, полученной в предшествующие семестры.

### **2. ОБЪЕМ ПРАКТИКИ**

Сроки проведения практики – 2-й семестр: с 8 по 21 июля, 2 недели.

Объем практики в академических часах – 108 час, 3 ЗЕТ.

### **3. ЦЕЛИ И ЗАДАЧИ. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ**

Ознакомительная практика студентов является составной частью их подготовки к профессиональной деятельности. За время обучения в университете студент обязан практически разобраться в сути процесса обеспечения защиты информации в системах связи и управления на всех уровнях – от уровня пользователя информационной системы до уровня администратора безопасности сети, начальника (сотрудника) отдела (службы) защиты информации.

Целями ознакомительной практики являются:

- ознакомление с предприятиями и организациями отрасли, обязанностями специалистов по защите информации в системах связи и управления, анализ основных направлений, форм и методов их деятельности;

- ознакомление с объектами информатизации, деловой документацией, программно-аппаратными и техническими средствами защиты информации, защищенными информационно-телекоммуникационными системами;

- получение первичных умений и навыков научно-исследовательской деятельности;

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин основной образовательной программы, получение необходимых первичных практических умений в соответствии с требованиями Федерального государственного образовательного стандарта к уровню подготовки выпускника.

Задачи практики:

- проверка, закрепление и углубление теоретических знаний, полученных при изучении дисциплин основной образовательной программы;

- профессиональная ориентация студентов, формирование у них полного представления о своей профессии, осознание ими собственных профессиональных качеств, интересов и склонностей;

- ознакомление с организационной структурой предприятий и организаций, принимающих студентов на практику, направлениями, формами и методами их деятельности;

- ознакомление и получение первичных умений работы с нормативно-правовыми актами, приказами, распоряжениями, указаниями и инструкциями, регламентирующими деятельность предприятий и организаций, принимающих студентов на практику, а также принимаемыми (издаваемыми) ими;

- ознакомление со структурой службы (отдела) информационной безопасности, обязанностями специалистов, получение представлений о роли и особенностях работы специалистов по защите информации;

- ознакомление с концепцией и политикой информационной безопасности предприятия (организации) и другими документами по информационной безопасности;

- ознакомление с конкретными объектами информатизации, их документацией, программно-аппаратными и техническими средствами защиты информации защищенных информационно-телекоммуникационных систем предприятия (организации);

- приобретение навыков профессионального общения:

- сбор и изучение практических материалов, необходимых для написания отчета, выполнения курсовых работ и проектов, выпускной квалификационной работы и в последующей профессиональной деятельности;

- подготовка студентов к осознанному и углубленному изучению общепрофессиональных и специальных дисциплин

Практика направлена на формирование следующих:

а) *компетенций*:

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 (ОК-5);

способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способность к самоорганизации и самообразованию (ОК-8);

способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств (ПК-3).

б) *первичных навыков*

- формулирования цели и задач научного исследования;

- выбора и обоснования методики научного исследования;

- сбора и изучения практических материалов, необходимых для написания отчета, выполнения курсовых работ и проектов, выпускной квалификационной работы и в последующей профессиональной деятельности;

- работы с офисными приложениями и прикладными программами, используемыми при проведении научных исследований и разработок;

- оформления результатов научного исследования (оформления отчета);

в) *первичных умений*

- соблюдать нормы профессиональной этики;

- работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

- коммуникации в устной и письменной формах для решения задач межличностного

и межкультурного взаимодействия в сфере профессиональной деятельности;

- оценивать технические возможности элементов и устройств информационно-телекоммуникационных систем и сетей предприятия;
- анализировать полученную информацию, нормативно-правовые акты по информационной безопасности;

#### **4. СОДЕРЖАНИЕ ПРАКТИКИ**

Во время прохождения ознакомительной практики студенты должны собрать материалы, необходимые для работы по направлению профессиональной деятельности.

Кроме этого, по согласованию с руководителем практики, студент должен проработать следующие вопросы.

По согласованию с руководителями ознакомительной практикой от кафедры и организации познакомиться с организационной структурой предприятия (организации), его задачами, направлениями, формами и методами деятельности.

Познакомиться с применяемыми на предприятии (организации) защищенными информационно-телекоммуникационными системами и сетями, средствами вычислительной техники, программным обеспечением.

Познакомиться с конкретными образцами технических и программно-аппаратных средств защиты информационно-телекоммуникационных сетей и систем, применяемыми в организации в целом и структурном подразделении, где он проходит практику, в частности, а также порядком их эксплуатации.

Познакомиться со структурой службы (отдела) информационной безопасности, обязанностями специалистов по защите информации.

Познакомиться с концепцией и политикой информационной безопасности предприятия (организации) и другими документами по информационной безопасности.

Познакомиться с конкретными объектами информатизации, их документацией, применяемыми в них методами и средствами обеспечения защиты информации.

Подготовить и защитить отчет по практике.

#### **5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ**

Материально-техническая база профильной организации должна обеспечивать качественный уровень проведения ознакомительной практики.

Используется материально-техническая база, которая включает телекоммуникационное оборудование и приборы, программные, программно-аппаратные и технические средства защиты информации, средства измерений, персональные компьютеры и другие виды вычислительной техники. Автоматизированные системы оснащены современными информационными технологиями, базами данных и программно-методическими комплексами для решения задач в области комплексной защиты информации в системах связи и управления.

#### **6. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ**

Каждый студент должен выполнить индивидуальное задание по направлению подготовки по изучению какого-либо направления профессиональной деятельности.

Индивидуальные задания определяются на основе анализа задач, решаемых профильной организацией, где студенты проходят эксплуатационную практику, а также специфике ее деятельности. В каждом случае задание формируется индивидуально.

Примеры индивидуальных заданий:

##### **1. Ознакомление с вопросами эксплуатации телекоммуникационного оборудования и приборов.**

- Познакомиться с порядком эксплуатации сетевого оборудования в организации.

- Познакомиться с порядком эксплуатации систем передачи информации в организации.
- Познакомиться с порядком эксплуатации антенно-фидерного оборудования в организации.
- Познакомиться с порядком эксплуатации средств защиты информации в информационных сетях организации.
- Познакомиться с порядком эксплуатации оборудования волоконно-оптических линий связи в организации.
- Познакомиться со структурой, составом оборудования, используемым программным обеспечением в локальной вычислительной сети организации (структурного подразделения).
- Познакомиться с составом телекоммуникационного оборудования и схемой организации связи организации (структурного подразделения).
- Познакомиться с порядком технического обслуживания телекоммуникационного оборудования в организации (структурном подразделении).

## **2. 1. Ознакомление с вопросами организации эксплуатации телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем**

- Познакомиться с порядком организации эксплуатации телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем в организации (структурном подразделении).
- Познакомиться с порядком разработки инструкций по эксплуатации телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем в организации (структурном подразделении).
- Познакомиться с порядком приемки и ввода в действие программных и технических средств и систем защиты информации в организации (структурном подразделении).
- Познакомиться с порядком организации эксплуатации волоконно-оптических линий связи в организации (структурном подразделении).
- Познакомиться с порядком организации эксплуатации антенно-фидерного оборудования в организации (структурном подразделении).
- Познакомиться с порядком организации эксплуатации средств защиты информации в компьютерных сетях организации.
- Познакомиться с порядком организации эксплуатации систем передачи информации в организации.

## **3. 1. Ознакомление с вопросами эксплуатации технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем в организации**

- Познакомиться с назначением, областью применения, основными возможностями средств антивирусной защиты в организации.
- Познакомиться с назначением, областью применения, основными возможностями технических средств защиты информации от утечек по АВАК в организации.
- Познакомиться с назначением, областью применения, основными возможностями технических средств защиты информации от утечек по ПЭМИН в организации.
- Познакомиться с назначением, областью применения, основными возможностями средств межсетевое экранирования в организации.
- Познакомиться с назначением, областью применения, основными возможностями средств разграничения доступа к оборудованию компьютерных сетей в организации.
- Познакомиться с назначением, областью применения, основными возможностями средств обнаружения вторжений в компьютерные сети в организации.
- Познакомиться с назначением, областью применения, основными возможностями средств идентификации и аутентификации в организации.

- Познакомиться с назначением, областью применения, основными возможностями средств операционной системы для защиты информации в организации.
- Познакомиться с назначением, областью применения, основными возможностями средств криптографической защиты в организации.

## 7. ПРОИЗВОДСТВЕННАЯ РАБОТА И ПРИОБРЕТЕНИЕ КВАЛИФИКАЦИИ

Студенты проходят ознакомительную практику в профильных организациях. Ознакомительная практика проводится только в организациях, которые имеют соответствующие лицензии на деятельность в области защиты информации (деятельность по технической защите конфиденциальной информации; деятельность с конфиденциальной информацией, со сведениями, составляющими государственную тайну; деятельность по оказанию услуг по защите государственной тайны и т.д.) в соответствии с ФЗ №99 "О лицензировании отдельных видов деятельности" от 04.05.2011 г. и иными нормативными и правовыми актами. Конкретные виды работ, выполняемых студентами на рабочих местах, согласовываются с руководителем практики от ЮРГПУ(НПИ). Приобретение квалификации не предусматривается.

## 8. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Отчет по практике и дневник являются основными документами, подтверждающими выполнение программы практики.

В дневнике отражаются все виды практики. На основании записи в дневнике практик каждый студент индивидуально составляет отчет по практике. В отчете отражаются вопросы, связанные с основной работой студента-практиканта на рабочем месте и детальной проработкой индивидуального задания, приводятся необходимые схемы, эскизы и другие научные или производственно-технические материалы.

Отчет студента проверяет и подписывает руководитель практики от кафедры, а в случае прохождения практики на предприятии его также проверяет и подписывает руководитель практики от предприятия. Данные руководители (руководитель) записывают в дневник отзыв в соответствии с компетенциями, освоенными в ходе прохождения практики и выставляют оценку. В графике прохождения практики должно быть учтено время на составление отчета и его защиту на предприятии.

Аттестация по практике - зачет с оценкой: отлично, хорошо, удовлетворительно, неудовлетворительно. Аттестация предусматривает защиту отчета перед руководителем практики от кафедры.

Требования к отчету: объем 10-30 листов формата А4, написанных шрифтом Times New Roman 14 с междустрочным интервалом 1,5.

## 9. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРАКТИКЕ

### 9.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер компетенции «ОК-5»	Формулировка компетенции «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»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		Этап формирования (семестр)
Индекс	Наименование	
Б1.В.ОД.6	Введение в специальность	1
Б1.В.ОД.11	Социальные проблемы информатизации	1
Б1.В.ДВ.1.1	Социально-психологические технологии инклюзивного образования	2
Б1.В.ДВ.1.2	Основы деловых коммуникаций и этикета	2



Б2. У1	Ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	2
Б1.Б.2	Философия	3
Б1.В.ОД.3	Социология и психология	4
Б2. У.2	Учебная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	4
Б2. П.1	Эксплуатационная № 1 (эксплуатационная практика)	6
Б1.Б.5	Основы управленческой деятельности	8
Б2.П.2	Эксплуатационная № 2 (эксплуатационная практика)	8
Б1.Б.22	Метрология и измерения в телекоммуникационных системах	8,9
Б2.П.3	Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности)	10
Б3	Государственная итоговая аттестация – подготовка и сдача государственного экзамена	11

Номер компетенции «ОК-6»	Формулировка компетенции «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		Этап формирования (семестр)
Индекс	Наименование	
Б1.В.ОД.11	Социальные проблемы информатизации	1
Б1.В.ДВ.1.1	Социально-психологические технологии инклюзивного образования	2
Б1.В.ДВ.1.2	Основы деловых коммуникаций и этикета	2
Б2. У.1	Ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	2
Б1.В.ОД.3	Социология и психология	4
Б2.У.2	Учебная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	4
Б2. П.1	Эксплуатационная № 1 (эксплуатационная практика)	6
Б1.Б.5	Основы управленческой деятельности	8
Б2.П.2	Эксплуатационная № 2 (эксплуатационная практика)	8
Б2.П.3	Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности)	10
Б3	Государственная итоговая аттестация – подготовка и сдача государственного экзамена	11

Номер компетенции «ОК-7»	Формулировка компетенции «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		Этап формирования (семестр)
Индекс	Наименование	
Б1.Б.16	Информатика	1
Б1.В.ДВ.1.2	Основы деловых коммуникаций и этикета	2
Б2.У.1	Ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	2

Б1.Б.3	Иностранный язык	1,2,3,4,5
Б2.У.2	Учебная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	4
Б2.П.1	Эксплуатационная № 1 (эксплуатационная практика)	6
Б1.В.ОД.7	Методы и средства защиты информации в системах электронного документооборота	8
Б2.П.2	Эксплуатационная № 2 (эксплуатационная практика)	8
Б2.П.3	Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности)	10
Б2.П.4	Научно-исследовательская работа (научно-исследовательская работа)	11
Б3	Государственная итоговая аттестация – подготовка и сдача государственного экзамена	11

Номер компетенции «ОК-8»	Формулировка компетенции «способность к самоорганизации и самообразованию»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		
Индекс	Наименование	Этап формирования (семестр)
Б1.В.ОД.6	Введение в специальность	1
Б1.В.ОД.12	Введение в основы инфокоммуникационных технологий	1
Б2.У.1	Ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	2
Б1.Б.2	Философия	3
Б2.У.2	Учебная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	4
Б2.П.1	Эксплуатационная № 1 (эксплуатационная практика)	6
Б2.П.2	Эксплуатационная № 2 (эксплуатационная практика)	8
Б1.В.ДВ.3.1	Методы научного творчества	9
Б2.П.3	Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности)	10
Б2.П.4	Научно-исследовательская работа (научно-исследовательская работа)	11
Б3	Государственная итоговая аттестация – подготовка и сдача государственного экзамена	11

Номер компетенции «ПК-3»	Формулировка компетенции «Способность оценивать технические возможности и выработать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		
Индекс	Наименование	Этап формирования (семестр)
Б2.У.1	Ознакомительная (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)	2
Б1.Б.11	Электроника и схемотехника	3,4

Б1.Б.33	Защита информации в компьютерных сетях	5
Б1.В.ОД.13	Основы волоконно-оптических линий связи	5,6
Б1.Б.13	Теория электрической связи	5,6,7
Б1.Б.20	Сети и системы передачи информации	6,7
Б1.Б.21	Аппаратные средства телекоммуникационных систем	7
Б1.Б.27	Техническая защита информации	7,8
Б1.Б.28	Программно-аппаратные средства обеспечения информационной безопасности	7,8
Б1.Б.23	Моделирование систем и сетей телекоммуникаций	8
Б1.В.ДВ.5.1	Защищенные мультисервисные сети	8,9
Б1.В.ДВ.5.2	Защищенные телекоммуникационные системы	8,9
Б1.Б.32	Защита информации в системах беспроводной связи	9
Б1.В.ОД.8	Мультимедийные технологии и протоколы	9
Б1.Б.29	Проектирование защищенных телекоммуникационных систем	10
Б1.В.ДВ.4.1	Проектирование мультисервисных сетей	10
Б1.В.ДВ.4.2	Проектирование телекоммуникационных систем	10
Б2. П.3	Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности)	10
Б2.П.5	Преддипломная (преддипломная практика)	11
Б3	Государственная итоговая аттестация – подготовка и сдача государственного экзамена	11

**9.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.**

Оценка сформированности компетенций в рамках промежуточной аттестации проводится при защите отчета по практике.

Номер компетенции	Показатели оценивания компетенций (знания и (или) умения и (или) навыки и (или) опыт деятельности, формируемые данной компетенцией)	Критерии оценивания компетенций на различных этапах их формирования		
		1-й уровень «УЗНАВАНИЕ»	2-й уровень «ВОСПРОИЗВЕДЕНИЕ»	3-й уровень «ПРИМЕНЕНИЕ»
ОК-5	<b>Знать</b> нормы профессиональной этики; <b>уметь</b> 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>владеть:</b> навыками формулирования цели и задач научного исследования; навыками выбора и обоснования методики научного исследования;	+	+	+

	навыками оформления результатов научного исследования			
ОК-6	<b>Знать</b> социальные, культурные и иные различия в коллективе; <b>уметь</b> работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	+	+	
ОК-7	<b>знать:</b> - иностранный язык в объеме, необходимом для профессиональной деятельности; - средства коммуникации в устной и письменной формах, в том числе в сети Интернет; <b>уметь</b> общаться с коллегами в устной и письменной формах для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности <b>владеть</b> навыками применения офисных приложений в профессиональной деятельности	+	+	+
ОК-8	<b>знать:</b> - основные источники информации, необходимой для профессиональной деятельности; - приемы самостоятельного освоения новых знаний и технологий в области комплексной защиты информации; <b>владеть</b> навыками сбора и изучения практических материалов, необходимых для написания отчета, выполнения курсовых работ и проектов, выпускной квалификационной работы и в последующей профессиональной деятельности	+		+
ПК-3	<b>Знать</b> области применения и основные возможности элементов и устройств телекоммуникационных систем и сетей; <b>уметь</b> оценивать технические возможности элементов и устройств телекоммуникационных систем и сетей	+	+	

#### Шкала оценивания компетенций:

«отлично» - обучающийся четко и в полном объеме изложил задачи и их реализацию при выполнении индивидуального задания по практике, проявил творческий подход при выполнении этих задач (учитывать отзыв о прохождении практики от руководителя практики от предприятия (организации)), изучил все общие вопросы, поставленные руководителем практики от кафедры;

«хорошо» - обучающийся правильно, но не в полном объеме изложил задачи и их реализацию при выполнении индивидуального задания по практике (учитывать отзыв о прохождении практики от руководителя практики от предприятия (организации)), изучил не все вопросы, поставленные руководителем практики от кафедры;

«удовлетворительно» - обучающийся, но не в полном объеме изложил задачи и их реализацию при выполнении индивидуального задания по практике (учитывать отзыв о прохождении практики от руководителя практики от предприятия (организации)), изучил не все вопросы, поставленные руководителем практики от кафедры;

«неудовлетворительно» - обучающийся, не выполнил индивидуальное задание по практике (учитывать отзыв о прохождении практики от руководителя практики от предприятия (организации)), изучил не все вопросы, поставленные руководителем практики от кафедры, или вообще не прошёл практику по неуважительной причине.

### 9.3. Типовые контрольные задания или иные материалы, необходимые для оценивания практических навыков

Контрольные задания и вопросы для оценивания результатов прохождения практики формирует руководитель в соответствии с той задачей, которую решал студент на практике.

*Примерный перечень вопросов для оценивания результатов прохождения практики*

1. Какова организационная структура и основные направления деятельности предприятия, на котором проходили практику?
2. Перечислите основные нормативно-правовые акты, на основе которых строит свою работу предприятие?
3. Перечислите основные нормативно-правовые акты, издаваемые на предприятии?
4. Какова структура службы (отдела) информационной безопасности предприятия?
5. Каковы роль и особенности работы специалистов по защите информации на предприятии?
6. Каково содержание концепции информационной безопасности предприятия (организации)?
7. Каково содержание политики информационной безопасности предприятия (организации)?
8. Какие частные политики информационной безопасности имеются на предприятии?
9. Какие документы разрабатываются и ведутся службой информационной безопасности?
10. С каким объектом информатизации вы знакомились, его задачи, структура, состав технических средств и программного обеспечения?
11. Какая документация разрабатывается и ведется на объекте информатизации?
12. Какие защищенные информационно-телекоммуникационные системы, сети созданы на предприятии, их назначение и состав?
13. Какие технические средства защиты информации применяются в ЗИС предприятия, их назначение и основные возможности?
14. Какие программно-аппаратные средства защиты информации применяются в ЗИС предприятия, их назначение и основные возможности?
15. Какое программное обеспечение применяется на предприятии, его назначение и основные возможности?
16. Какие цели и задач научного исследования ставили себе на время практики?
17. Какие методы научного исследования вы применяли во время практики? Обоснуйте их выбор.
18. Каков порядок оформления результатов научного исследования (отчета по научной работе)? Какими документами он определяется?
19. Какие инфокоммуникационные технологии применяются на предприятии? Их назначение и основные возможности.
20. Какие операционные системы используются на предприятии? Назовите их основные функции.
21. Какие периферийные устройства используются на предприятии? Назовите их основные функции.
22. Назовите основные компоненты операционной системы Windows.
23. Каковы основные возможности текстового процессора Microsoft Word?
24. Какие возможности предоставляет Центр управления безопасностью Microsoft Word?
25. Каковы основные возможности редактора электронных таблиц Microsoft Excel?
26. Назовите основные возможности применения Microsoft Excel для расчетов.
27. Каковы основные возможности программы Power Point?

28. Какие программные средства сжатия данных вы знаете? Какие из них применяются на предприятии, на котором вы проходили практику?

29. Какова структура ЛВС на объекте информатизации (в структурном предприятии), с которым вы знакомились в ходе практики?

30. Каким образом на предприятии осуществлялся доступ к сети Интернет? Какие способы осуществления доступа вы знаете? Охарактеризуйте их.

## 10. ЛИТЕРАТУРА

### Основная учебная литература

1. Кудинов Ю.И. Основы современной информатики [Электронный ресурс]: учебное пособие / Ю.И. Кудинов, Ф.Ф. Пашенко. – Электрон. дан. – СПб. Лань, 2011. – 256 с. – Режим доступа: <https://e.lanbook.com/book/91902>.

2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / Шаньгин В.Ф. – Электрон. дан. – СПб. Лань, 2012. – 592 с. – Режим доступа: <http://e.lanbook.com/book>.

3. Величко В.В., Катунин Г.П., Шувалов В.П. Основы инфокоммуникационных технологий Издательство – Горячая линия-Телеком, - М., 2016– 724 с:ил.

4. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: <http://e.lanbook.com/book/5170>.

### Дополнительная учебная литература

#### Учебные издания

5. Сафонов В.О. Основы современных операционных систем. [Электронный ресурс]: учебное пособие/ В.О. Сафонов. – М.: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. – 584 с.: ил.– (основы информационных технологий). – Режим доступа: <http://www.knigafund.ru/books/178696/read>.

6. Лебедько, Е.Г. Теоретические основы передачи информации. [Электронный ресурс] - СПб. : Лань, 2011. - 352 с.- Режим доступа: <http://e.lanbook.com/book/1543>.

7. Давыдов А.Е., Максимов Р.Е., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем: научно-техническое издание/– Москва: ОАО «Воентелеком», 2015. – 520 с.

8. Новиков В.К., Галушкин И.Б., Аксенов С.В.; под общей редакцией В. К. Новикова. Информационная безопасность и защита информации. Организационно-правовые основы. - М.: Горячая линия-Телеком, 2016 г.-312 стр.

9. Работа в Microsoft Word 2007/ О.В. Спиридонов. [Электронный ресурс]: – М.: Национальный Открытый Университет «ИНТУИТ», 2008. – 346 с. – Режим доступа: <http://www.knigafund.ru/books/177184/read>

10. Работа в Microsoft Excel 2010/О.В. Спиридонов. [Электронный ресурс]: -М.: Национальный Открытый Университет «ИНТУИТ», 2011. – 438 с. – Режим доступа: <http://www.knigafund.ru/books/176821/read>

11. Microsoft Power Point 2010/ В.П. Молочков. [Электронный ресурс]: -М.: Национальный Открытый Университет «ИНТУИТ», 2011. –241 с.– Режим доступа: <http://www.knigafund.ru/books/177124/read>

#### Официальные издания

12. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert>

13. ГОСТ 29099-91. Сети вычислительные локальные. Термины и определения. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert>.

14. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

455 Л

технологий. Часть 1. Введение и общая модель. <http://www.lib.npi-tu.ru/textpert>

15. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. <http://www.lib.npi-tu.ru/textpert>.

16. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. <http://www.lib.npi-tu.ru/textpert>

17. ГОСТ Р ИСО/МЭК ТО 1546-2008. Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert>

18. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert>

19. ГОСТ Р 51188-98. Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert> .

20. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert> .

21. ГОСТ Р ИСО/МЭК 7498-4-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert> .

22. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert> .

23. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс]. - Режим доступа: <http://www.lib.npi-tu.ru/textpert> .

24. Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Электронный ресурс]. - Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-25-iyulya-1997-g>

25. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. - Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g4>.

26. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс]. - Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g3>.

### **Методические указания к лабораторным и практическим занятиям**

27. Рожков В.И. Информатика [Электронный ресурс]: учебно-методическое пособие к лабораторным работам/Чамлай С.В. – Новочеркасск: ЮРГПУ (НПИ), 2015. – 67 с. – Режим доступа: <http://lib.npi-tu.ru/books/1299a7f46d819e512da34af494c8852121.pdf>.
28. Система защиты информации ViPNet. Практикум. Учебно-методическое пособие/ Под ред. доктора пед. наук, профессора А. О. Чефрановой. – М.: Горячая линия - Телеком, 2016 г. – 346 с.
29. Технология ViPNet. Практикум/ Под ред. профессора А. О. Чефрановой. – М.: Горячая линия - Телеком, 2016 г. – 456 с.
30. Гусев В.В. Программно-аппаратные комплексы ViPNet/Под ред. профессора А.О. Чефрановой. - 3-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2016. – 110 с.
31. Удостоверяющий центр ViPNet. Практикум. – М.: ИнфоТеКС, 2015. – 163 с.
32. А.О. Чефранова, А.В. Белов. Межсетевое экранирование. Учебно-методическое пособие. – М.: 11-формат, 2015. – 46 с.
33. Программно-аппаратный комплекс ViPNet IDS. Практикум. – М.: ИнфоТеКС, 2015. – 64 с.
34. ПАК ViPNet Coordinator HW. Руководство администратора [Электронный ресурс]. – М.: ИнфоТеКС, 2011. – 245 с. – Режим доступа: [https://www.infotecs.ru/downloads/product\\_docs.php?id\\_product=190](https://www.infotecs.ru/downloads/product_docs.php?id_product=190).
35. Программно-аппаратный комплекс ViPNet IDS. Руководство администратора. [Электронный ресурс]. – М.: ИнфоТеКС, 2015. – 329 с. – Режим доступа: [https://files.infotecs.ru/\\_dl/sess/vipnet\\_ids/docs/ViPNet\\_IDS\\_Adminguide\\_Ru\\_1.0.pdf](https://files.infotecs.ru/_dl/sess/vipnet_ids/docs/ViPNet_IDS_Adminguide_Ru_1.0.pdf).
36. Ермаков А.Е. Основы конфигурирования корпоративных сетей Cisco [Электронный ресурс]: учебное пособие. – М.: ФБГОУ «Учебно-методический центр на железнодорожном транспорте», 2013 г. – 248 с. – Режим доступа: <http://www.knigafund.ru/books/173404>.
37. Колегов, Д.Н. Лабораторный практикум по основам построения защищенных компьютерных сетей [Электронный ресурс]: учебное пособие. – Электрон. дан. – Томск: ТГУ (Национальный исследовательский Томский государственный университет), 2013. — 140 с. — Режим доступа: [http://e.lanbook.com/books/element.php?pl1\\_id=44913](http://e.lanbook.com/books/element.php?pl1_id=44913).

### **Интернет-ресурсы**

38. Пользовательская документация АПКШ "Континент" 3.7. [Электронный ресурс]. Режим доступа: [http://www.securitycode.ru/products/apksh\\_kontinent/documentation](http://www.securitycode.ru/products/apksh_kontinent/documentation). – Загл. с экрана.
39. Документация на СЗИ от НСД Secret Net. [Электронный ресурс]. – Режим доступа: [http://www.securitycode.ru/products/secret\\_net/documentation/](http://www.securitycode.ru/products/secret_net/documentation/). – Загл. с экрана.

## **11. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ИСПОЛЬЗУЕМЫЕ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ**

1. Microsoft Windows 7, 8, 10 Enterprise, лицензия V4640039.
2. Microsoft Office 2010, 2013, 2016 Professional, лицензия V4640039.
3. ПО ViPNet, лицензии lic\_11208\_30.08.2017\_893308-1.itcslic, lic\_11209\_30.08.2017\_893428-1.itcslic
4. Kaspersky Endpoint Securite 10 Standart, лицензия 17E0160122123732623108.

## **12. МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ ПЕРЕД НАЧАЛОМ ПРАКТИКИ**

Студенты до начала практики должны пройти инструктаж о порядке прохождения практики и общий инструктаж по обеспечению безопасности жизнедеятельности. Допуск к



работе на объектах практики осуществляется после проведения обязательных инструктажей по технике безопасности и охране труда: вводного и на рабочем месте с оформлением установленной документации.

В случае прохождения практики на предприятии, перед отъездом на практику студент должен пройти медицинскую комиссию, оформить медицинскую справку установленного образца (если это требуется по месту прохождения практики), получить на кафедре командировочное удостоверение, программу практики, дневник практик и выписку из приказа по практике (направление - письмо руководителю предприятия). Взять с собой паспорт, студенческий билет, страховое свидетельство государственного пенсионного страхования, ИНН, страховой медицинский полис, а ранее работавшим - трудовую книжку.

Студенты до начала практики получают задание от своего руководителя по практике.