

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»**

УТВЕРЖДАЮ

Первый проректор, проректор по  
учебной работе

\_\_\_\_\_ А.Е. Рудин

«30» 06 2020 года

**Блок 2**

**ПРОГРАММА ПРАКТИКИ**

Кафедра: **20** Интеллектуальных систем и защиты информации  
*Код* *Наименование кафедры*

Направление подготовки: **10.03.01 Информационная безопасность**

Профиль подготовки: **Безопасность компьютерных систем (в коммерческих структурах)**

Уровень образования: **Бакалавриат**

**План учебного процесса**

Индекс	Наименование практик (по видам и типам)	Трудоём- кость, ЗЕТ	Очное обучение		Очно-заочное обучение		Заочное обучение	
			Номер семестра	Часы	Номер семестра	Часы	Номер семестра	Часы
<b>Б2.П</b>	<b>Производственная практика:</b>							
Б2.В.0 2.03(П д)	Преддипломная практика (научно-исследовательская работа)	6	8	216				

Рабочая программа практики составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки

и на основании учебного плана № 1/1/704

## Б2.П ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

**Б2.В.02.03(ПД)**

**Преддипломная практика (научно-исследовательская работа)**

(Индекс и название практики согласно учебному плану)

### 1.1. Вид производственной практики

- Преддипломная практика

### 1.2. Тип практики

- Научно-исследовательская работа

### 1.3. Способ и форма проведения практики

- Способ проведения практики

Стационарная                       Выездная

- Форма проведения практики

Непрерывно                       Дискретно по видам практик                       Дискретно по периодам проведения практик

Для инвалидов и лиц с ограниченными возможностями здоровья выбор мест прохождения практики учитывает особенности их психофизического развития, индивидуальные возможности, состояние здоровья и требования по доступности.

### 1.4. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы:

Код компетенции	Формулировка компетенции	Этап формирования
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Второй
<p><b>Планируемые результаты обучения</b></p> <p>Знать:</p> <p>1) Логiku функционирования сети и ее основных информационных сервисов</p> <p>Уметь:</p> <p>1) применять мировые информационные системы в учебной и трудовой деятельности</p> <p>Владеть:</p> <p>1) навыками применения в своей работе мировых информационных ресурсов</p>		
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Второй
<p><b>Планируемые результаты обучения</b></p> <p>Знать:</p> <p>1) основные характеристики устройств хранения, обработки и передачи информации</p> <p>Уметь:</p> <p>1) ориентироваться в особенностях применяемых программно-аппаратных, технических и инженерно-технических комплектов</p> <p>Владеть:</p> <p>1) Опытom применения методов и средств выявления угроз безопасности</p>		

ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Второй
<b>Планируемые результаты обучения</b> Знать: 1) Методы разработки, анализа и проектирования ПО Уметь: 1) Оценивать риски Владеть: 1) Навыками выявления требований архитектурного проекта программного средства		
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты	Второй
<b>Планируемые результаты обучения</b> Знать: 1) операционные системы персональных ЭВМ Уметь: 1) формулировать и настраивать политику безопасности Владеть: 1) навыками применения методики анализа сетевого трафика		
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Второй
<b>Планируемые результаты обучения</b> Знать: 1) основные особенности эксплуатации программных, программно-аппаратных и технических средств защиты информации Уметь: 1) осуществлять организационно-правовое обеспечение информационной безопасности объекта защиты Владеть: 1) навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны		
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Второй
<b>Планируемые результаты обучения</b> Знать: законы, технологии, правила аттестации объекта информатизации. Уметь: проводить аттестацию объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации Владеть: Навыками разработки технологической документации		
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Второй
<b>Планируемые результаты обучения</b> Знать: места уязвимости программного обеспечения и программно-аппаратных средств защиты Уметь: определять направления использования аппаратного и программного обеспечения		

определенного класса для решения служебных задач Владеть: навыками выявления и уничтожения компьютерных вирусов		
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Второй
<b>Планируемые результаты обучения</b> Знать: 1) методы и средства проектирования подсистем и средств обеспечения информационной безопасности Уметь: 1) проводить обоснование соответствующих проектных решений Владеть: 1) технологиями системного анализа при ведении проектной деятельности		
ПК-8	Способность оформлять рабочую документацию с учетом действующих нормативных и методических документов	Второй
<b>Планируемые результаты обучения</b> Знать: 1) нормы и методы оформления документов. Уметь: 1) оформлять рабочую техническую документацию Владеть: 1) навыками оформления документации в области информационной безопасности		
ПК-9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Второй
<b>Планируемые результаты обучения</b> Знать: 1) технологические процессы обработки информации Уметь: 1) применять методы представления и обработки знаний для решения научных и прикладных задач Владеть: 1) навыками работы с базами данных и базами знаний		
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Второй
Знать: 1) виды и формы функционирования вредоносного программного обеспечения Уметь: 1) обосновывать правила безопасной эксплуатации программного обеспечения Владеть: 1) навыками проведения организационных технических и программных мероприятий по защите информации		
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Второй

<b>Планируемые результаты обучения</b>		
Знать: 1) Методологии разработки программного обеспечения		
Уметь: 1) Применять методологии разработки программного обеспечения		
Владеть: 1) Навыками разработки регламентов обмена информацией в команде разработчиков		
ПК-12	Способность принимать участие в проведении экспериментальных исследований	первый
<b>Планируемые результаты обучения</b>		
Знать: 1) виды численных методов для анализа функций, для решения задач линейной алгебры		
Уметь: 1) выбирать численные методы для анализа функций		
Владеть: 1) навыками конфигурирования основных численных методов		
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Второй
<b>Планируемые результаты обучения</b>		
Знать: 1) Основные процессы СУИБ		
Уметь: 1) Использовать методы анализа рисков информационной безопасности		
Владеть: 1) Опытном использовании подходов к управлению службой защиты информации		
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	Первый
<b>Планируемые результаты обучения</b>		
Знать: 1) теорию организации и функционирования малого бизнеса в области информационных технологий		
Уметь: 1) формировать предложения по совершенствованию управлением малым коллективом		
Владеть: 1) навыками применения экономических и административных методов управления малыми коллективам		
ПК-15	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Первый
<b>Планируемые результаты обучения</b>		
Знать: 1) правила эксплуатации средств вычислительной техники, измерительных приборов или технологического оборудования		
Уметь: 1) использовать на практике методы анализа организационно-технического уровня изучаемого		

аппаратного и программного обеспечения инструментальных систем и их компонентов Владеть: 1) опытом работы с методами и средствами анализа и моделирования современных вычислительных объектов		
ПСК-1	способность проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики	Первый
<b>Планируемые результаты обучения</b> Знать: 1) Методологии разработки программного обеспечения для разработки совместного анализа Уметь: 1) Применять методологии разработки программного обеспечения для разработки совместного анализа Владеть: 1) Навыками разработки регламентов обмена информацией в команде разработчиков		
ПСК-2	способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов	Первый
<b>Планируемые результаты обучения</b> Знать: 1) Методологии разработки программного обеспечения Уметь: 1) Применять методологии разработки программного обеспечения Владеть: 1) Навыками разработки регламентов обмена информацией в команде разработчиков		

### 1.5. Место практики в структуре образовательной программы

#### Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Информатика (ОПК-7)
- Базы данных (ОПК-7)
- Информационные технологии (ОПК-7)
- Защита информации в компьютерных системах (ОПК-7)
- Защита информации в Internet (ОПК-7)
- Безопасность корпоративных компьютерных сетей (ОПК-7)
- Основы управления информационной безопасностью (ОПК-7)
- Основы информационной безопасности (ПК-9)
- Учебная практика (практика по получению первичных профессиональных умений и навыков) (ПК-9)
- Комплексная защита информации на предприятии (ПК-9)
- Теория вероятностей и математическая статистика (ПК-11)
- Алгебраические методы информационной безопасности (ПК-11)

#### Влияние практики на последующую образовательную траекторию обучающегося

Прохождение данной практики необходимо обучающемуся для успешного освоения следующих дисциплин (практик) по данному направлению подготовки:

- Государственная итоговая аттестация (ОПК-7, ПК-9, ПК-11)

### 1.6. Содержание практики

Наименование и содержание разделов (этапов)	Объем (часы)
Раздел 1. Систематизация материалов по теме выпускной квалификационной работы	

Наименование и содержание разделов (этапов)	Объем (часы)
Этап 1. Собеседование о целях и задачах преддипломной производственной практики студента	20
Этап 2. Обоснование актуальности, предметности, степень разработанности, теоретико-методологических основ, авторского видения раскрытия темы выпускной квалификационной работы в сфере информационной безопасности	20
Раздел 2. Научно-исследовательская работа.	
Этап 3. Разработка моделей и методик проведения исследований в предметной области, согласно темы выпускной квалификационной работы	50
Этап 4. Алгоритмизация и компьютерная реализация разработанных методик проведения исследований в предметной области, согласно темы выпускной квалификационной работы	40
Раздел 3. Оформление отчета	
Этап 5. Обобщение материалов научного исследования по теме выпускной квалификационной работы. Формулирование выводов.	30
Этап 6. Оформление отчета по практике и других сопутствующих документов (отзыв руководителя практики).	30
Этап 7. Подготовка к защите отчета. Сдача зачета по практике.	20
Текущий контроль (Собеседование по разделам)	2
Промежуточная аттестация (зачет с оценкой)	4
<b>ВСЕГО:</b>	<b>216</b>

### 1.7. Формы отчетности по практике

Дневник практиканта, согласно принятой в СПГУПТД форме, включает в себя: задание на практику, краткий отчёт, отзыв руководителя практики, календарный план-график преддипломной практики, выводы и предложения, сделанные студентом в ходе прохождения практики. Отчёт по преддипломной практике выполняется обучающимся индивидуально, объём составляет 12-15 страниц машинописного текста.

### 1.8. Учебная литература

#### а) основная учебная литература

1. Чуянов А.Г. Обеспечение информационной безопасности в компьютерных системах [Электронный ресурс] : учебное пособие / А.Г. Чуянов, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2012. — 204 с. — 978-5-88651-535-0. — Режим доступа: <http://www.iprbookshop.ru/36015.html>
2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа:
3. Артемов А.В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов. — Электрон. текстовые данные. — Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 256 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/33430.html>
4. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
5. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: <http://www.iprbookshop.ru/52209.html>
6. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 с. — 978-5-374-00301-7. — Режим доступа: <http://www.iprbookshop.ru/10677.html>



7. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс] : учебно-методический комплекс / Ю.Н. Сычев. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 342 с. — 978-5-374-00602-5. — Режим доступа: <http://www.iprbookshop.ru/14642.html>
  8. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: <http://www.iprbookshop.ru/33857.html>
  9. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: <http://www.iprbookshop.ru/43183.html>
  10. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — 978-5-7422-4331-1. — Режим доступа: <http://www.iprbookshop.ru/43960.html>
- б) дополнительная учебная литература
1. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 с. — 978-89838-487-6. — Режим доступа: <http://www.iprbookshop.ru/6991.html>
  2. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс] : монография / А.А. Смирнов. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2012. — 159 с. — 978-5-238-02259-8. — Режим доступа: <http://www.iprbookshop.ru/15425.html>
  3. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс] : учебное пособие / А.Н. Кубанков, Н.Н. Куняев. — Электрон. текстовые данные. — М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — 978-5-89172-850-9. — Режим доступа: <http://www.iprbookshop.ru/47262.html>
  4. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 35 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/61737.html>
  5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/62945.html>
  6. Смышляев А.Г. Информационная безопасность. Лабораторный практикум [Электронный ресурс] : учебное пособие / А.Г. Смышляев. — Электрон. текстовые данные. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/66655.html>
  7. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 с. — 978-5-00094-297-0. — Режим доступа: <http://www.iprbookshop.ru/66771.html>
  8. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 335 с. — 978-5-4383-0136-3. — Режим доступа: <http://www.iprbookshop.ru/66797.html>
  9. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2012. — 98 с. — 9965-756-05-8. — Режим доступа: <http://www.iprbookshop.ru/67055.html>

10. Михайлов В.Ю. Дискретная математика и модели кодирования в задачах информационной безопасности [Электронный ресурс] : учебное пособие / В.Ю. Михайлов, Р.Б. Мазепа, Е.О. Карпухин. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 160 с. — 978-5-4383-0140-0. — Режим доступа: <http://www.iprbookshop.ru/68587.html>

11. Информационная безопасность при управлении техническими системами [Электронный ресурс] : учебное пособие / С.А. Баркалов [и др.]. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 528 с. — 978-5-4383-0133-2. — Режим доступа: <http://www.iprbookshop.ru/68589.html>

12. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

#### 1.9. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для проведения практики

1. [Электронно-библиотечная система IPRbooks.](http://www.iprbookshop.ru) (<http://www.iprbookshop.ru>)
2. [Электронная библиотека учебных изданий СПбГУПТД](http://publish.sutd.ru) (<http://publish.sutd.ru>)
3. Сайт Федерального института промышленной собственности (<http://www1.fips.ru>)
4. Сайт Федеральной службы по интеллектуальной собственности (Роспатент) (<http://www.rupto.ru>)

#### 1.10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Microsoft Office Standart 2016 Russian Open No Level Academic)
2. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

#### 1.11. Материально-техническая база, необходимая для проведения практики

1. Стандартно оборудованная аудитория
2. Видеопроектор
3. Компьютеры с возможностью выхода в Интернет

#### 1.12. Фонд оценочных средств для проведения промежуточной аттестации по практике

##### 1.12.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства*	Представление оценочного средства в фонде
ОПК-7/второй	Интерпретирует основные принципы функционирования сети и ее основных информационных сервисов в мировом информационном пространстве	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	использует мировые информационные системы для поиска, обработки информации при решении прикладных задач		
	Рассматривает основные технологические принципы функционирования мировых информационных ресурсов на основе глобальной сети Internet		
ПК-1/второй	Раскрывает составляющие средств информатизации и описывает их функционал	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Сравнивает характеристики средств защиты информации		
	Компонует информацию о средствах защиты информации для выявления угроз		
ПК-2/второй	Обосновывает использование программного обеспечения при решении профессиональных задач	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства*	Представление оценочного средства в фонде
	Составляет перечень рисков, несущих угрозу защищаемой информации Анализирует требования программного средства для обеспечения защиты объекта информатизации		
ПК-3/второй	Воспроизводит основные принципы функционирования и характеристики операционных систем Определяет и формулирует политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе Применяет методику анализа сетевого трафика, контролирует работу средств обнаружения несанкционированных вторжений	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
ПК-4/второй	Описывает технологии, методы и модели проектирования, разработки, тестирования, отладки и внедрения приложений для информатизации различных аспектов деятельности Систематизирует нормативно-правовую документацию, связанную с обеспечением защиты информации Осуществляет анализ современных систем защиты информации	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
ПК-5/второй	формулирует основные понятия в области аттестации объекта информатизации по требованиям безопасности рассматривает участников стандартной схемы аттестации и этапы аттестации в соответствии с нормативными документами составляет перечень документации для проведения аттестации объекта информатизации	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
ПК-6/второй	формулирует направления, методы и средства защиты информации от утечки, хищения, искажения, подделки, несанкционированного уничтожения, копирования и блокирования  выбирает, строит и анализирует показатели защищенности программно-аппаратных средств защиты информации  настраивает средства обнаружения вторжений и антивирусные системы	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
ПК-7/второй	Дает характеристику основных этапов проектирования систем безопасности Доказывает эффективность применения программно-аппаратных, инженерных и технических средств обеспечения информационной безопасности Производит оценку проблемы с применением методов системного анализа	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
ПК-8/второй	Раскрывает методики оформления служебных документов Компонует основную информацию для последующей разработки технической документации Использует комплект типовых документов по информационной безопасности	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства*	Представление оценочного средства в фонде
ПК-9/второй	определяет процессы обработки информации для решения задач профессиональной деятельности	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	использует и обосновывает выбор методов представления и обработки знаний		
	демонстрирует результат поиска информации в различных базах данных и базах знаний при принятии конкретного технического решения		
ПК-10/второй	Раскрывает механизмы действия вредоносных программ.	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Анализирует объект защиты с помощью методик представленных в нормативно-технических документах.		
	Аргументированно использует различные методы защиты информации при решении профессиональной задачи.		
ПК-11/второй	Описывает основные приемы и этапы разработки программного обеспечения для решения профессиональных задач	Отчет по преддипломной практике	Перечень вопросов (4 вопроса)
	Исследует современные методики разработки комплекса программ по обеспечению информационной безопасности		
	Исследует информационные потоки по обработке информации		
ПК-12/первый	Знает численные методы для анализа функций, для решения задач линейной алгебры и решения задач аппроксимации и нахождения экстремумов	Отчет по преддипломной практике	Перечень вопросов (4 вопроса)
	Использует численные методы для анализа функций, численные методы, связанные с задачами линейной алгебры и применяет численные методы, связанные с задачами аппроксимации и нахождения экстремумов		
	Владеет основными численными методами и схемами, связанными с вычислением производных и интегралов и основными численными методами и схемами, связанными с задачами линейной алгебры		
ПК-13/второй	Описывает основные этапы построения системы управления информационной безопасностью	Отчет по преддипломной практике	Перечень вопросов (4 вопроса)
	Осуществляет оценку рисков на основе модели угроз и уязвимостей и на основе модели информационных потоков		
	Предлагает организационно-технические мероприятия по защите информации на предприятии		
ПК-14/первый	перечисляет и соотносит известные теории организации и функционирования малого бизнеса в профессиональной сфере	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Предлагает мероприятия по изменению организационной структуры предприятия в рамках разработки проекта на предприятии		
	выбирает и обосновывает свой выбор экономических или административных		

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства*	Представление оценочного средства в фонде
	методов управления коллективом, в рамках разработки профессионального проекта		
ПК-15/первый	Излагает правила безопасности при использовании технологического оборудования для решения профессиональных задач	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Планирует использование программно-аппаратных средств для обеспечения комплексной защиты в соответствии с требованиями нормативно-правовых документов		
	Предлагает алгоритм моделирования систем защиты на предприятии с учетом требований ФТЭК		
ПСК-1/первый	Знает основы нечеткого моделирования	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Представляет информационные системы и начальное обучение пользователей с применением нечеткого моделирования		
	Осуществляет презентацию информационной системы и начальное обучение пользователей		
ПСК-2/первый	Знает методологии разработки программного обеспечения	Отчет по преддипломной практике	Перечень вопросов (3 вопроса)
	Умеет применять методологии разработки программного обеспечения		
	Владеет навыками разработки регламентов обмена информацией в команде разработчиков		

Описание шкал и критериев оценивания сформированности компетенций на установленных этапах их формирования по результатам прохождения практики

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
86 - 100	5 (отлично)	Обучающийся соблюдал сроки прохождения практики; отчетные материалы полностью соответствуют программе практики и имеют практическую ценность; индивидуальное задание выполнено полностью и на высоком уровне, получен положительный отзыв от предприятия; качество оформления отчета и презентации соответствуют требованиям. В процессе защиты отчета обучающийся дал полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области.
75 – 85	4 (хорошо)	Обучающийся соблюдал сроки прохождения практики; отчетные материалы в целом соответствуют программе практики, содержат стандартные выводы и рекомендации практиканта; индивидуальное задание выполнено, получен положительный отзыв от предприятия; качество оформления отчета и презентации соответствуют требованиям. В процессе защиты отчета обучающийся дал полный ответ, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный.
61 – 74		Обучающийся соблюдал сроки прохождения практики; отчетные материалы в целом соответствуют программе практики, содержат стандартные выводы и рекомендации практиканта; индивидуальное задание в целом выполнено с несущественными ошибками, получен положительный отзыв от предприятия; качество оформления отчета и / или презентации имеют несущественные ошибки. В процессе защиты отчета обучающийся дал стандартный ответ, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.
51 - 60	3 (удовлетво-	Обучающийся соблюдал сроки прохождения практики; отчетные материалы в целом соответствуют программе практики, собственные выводы и

	нительно)	рекомендации практиканта по итогам практики отсутствуют; индивидуальное задание выполнено с существенными ошибками, получен неудовлетворительный отзыв от предприятия; качество оформления отчета и / или презентации имеют многочисленные несущественные ошибки. В процессе защиты отчета обучающийся дал ответ с существенными ошибками или пробелами в знаниях по некоторым разделам практики. Демонстрирует понимание содержания практики в целом, без углубления в детали.
40 – 50		Обучающийся нарушал сроки прохождения практики; отчетные материалы в целом соответствуют программе практики, собственные выводы и рекомендации практиканта по итогам практики отсутствуют; индивидуальное задание выполнено с существенными ошибками, получен неудовлетворительный отзыв от предприятия; качество оформления отчета и / или презентации имеют многочисленные существенные ошибки. В процессе защиты отчета обучающийся продемонстрировал слабое понимание сущности практической деятельности, допустил существенные ошибки или пробелы в ответах сразу по нескольким разделам программы практики, незнание (путаницу) важных терминов.
17 – 39	2 (неудовлетворительно)	Обучающийся систематически нарушал сроки прохождения практики; отчетные материалы частично не соответствуют программе практики; не смог справиться с практической частью индивидуального задания, получен неудовлетворительный отзыв от предприятия; качество оформления отчета и / или презентации не соответствует требованиям. В процессе защиты отчета обучающийся продемонстрировал неспособность ответить на вопрос без помощи преподавателя, незнание значительной части принципиально важных практических элементов, многочисленные грубые ошибки.
1 – 16		Обучающийся систематически нарушал сроки прохождения практики; отчетные материалы не соответствуют программе практики; не смог справиться с индивидуальным заданием, получен неудовлетворительный отзыв от предприятия; отчет к защите не представлен.
0		Обучающийся практику не проходил.

### 1.12.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций по результатам прохождения практики

Перечень контрольных вопросов (заданий, иных материалов), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопроса (задания, оценочного материала)
1	Формулирование целей и задач ВКР
2	Обоснование актуальности и предметности темы ВКР
3	Обоснование степени разработанности и применяемых методов, согласно теме ВКР
4	Виды моделей, применяемых в информационной безопасности
5	Типы методик проведения исследований, применяемые в информационной безопасности
6	Виды алгоритмов и методы их разработки в сфере информационной безопасности
7	Виды компьютерных программ и методы их разработки в сфере информационной безопасности
8	Описание структуры отчета по практике

Типовые контрольные задания по результатам прохождения производственной практики

**Задание 1.** Формирование регламента поиска патентной документации, согласно тематике ВКР

**Задание 2.** Формирование перечня нормативно-технической литературы, согласно тематике ВКР

### 1.12.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

- **Условия допуска обучающегося к сдаче зачета по практике и порядок ликвидации академической задолженности**

Проведение аттестации регламентируется локальными нормативными актами «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся» и

«Положение о практике обучающихся, осваивающих образовательные программы высшего образования в СПбГУПТД».

Обучающиеся, не прошедшие практику по уважительной причине, проходят практику по индивидуальному графику.

Обучающиеся, не прошедшие практику без уважительной причины или получившие оценку «неудовлетворительно», считаются лицами, имеющими академическую задолженность, и ликвидируют ее в соответствии с порядком ликвидации академической задолженности согласно ЛНА «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся».

- **Форма проведения промежуточной аттестации по практике**

устная  письменная  компьютерное тестирование  иная

- **Особенности проведения зачета по практике**

Аттестация проводится на выпускающей кафедре на основании анализа содержания отчета по практике, собеседования, отзывов руководителей практики и оценки, выставленной обучающемуся на базе практики.

Если практика проводилась на выпускающей кафедре СПбГУПТД, оценку в отзыве проставляет руководитель практики от выпускающей кафедры. Если практика проводилась в профильной организации (структурном подразделении СПбГУПТД), оценку в отзыве проставляет руководитель практики от профильной организации (руководитель структурного подразделения СПбГУПТД).

Процедура оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности) обучающегося, характеризующих этап (ы) формирования каждой компетенции (или ее части) осуществляется в процессе аттестации по критериям оценивания сформированности компетенций с переводом баллов, полученных обучающимся, из одной шкалы в другую согласно п.1.12.1 программы практики.

Для успешного прохождения аттестации по практике обучающемуся необходимо получить оценку «удовлетворительно» при использовании традиционной шкалы оценивания и (или) не менее 40 баллов при использовании шкалы БРС.

Для оценивания результатов прохождения практики и выставления зачета с оценкой в ведомость и зачетную книжку используется традиционная шкала оценивания, предполагающая выставление оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

По результатам аттестации оценку в ведомости и зачетной книжке проставляет руководитель практики от выпускающей кафедры или заведующий выпускающей кафедрой.