

УТВЕРЖДАЮ  
Первый проректор, проректор по  
УР

\_\_\_\_\_ А.Е.Рудин

## Программа практики

**Б2.В.01(П)** Производственная практика (проектно-технологическая практика)

Учебный план: 2024-2025 10.04.01 ИИТА ПСЗИНП ОО №2-1-159.plx

Кафедра: **20** Интеллектуальных систем и защиты информации

Направление подготовки:  
(специальность) 10.04.01 Информационная безопасность

Профиль подготовки: Проектирование систем защиты информации на предприятии  
(специализация)

Уровень образования: магистратура

Форма обучения: очная

### План учебного процесса

Семестр		Контактная работа обучающихся	Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Практ. занятия				
4	УП	66	293,75	0,25	10	Зачет с оценкой
	ПП	66	293,75	0,25	10	
Итого	УП	66	293,75	0,25	10	
	ПП	66	293,75	0,25	10	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1455

Составитель (и):

кандидат технических наук, Доцент

\_\_\_\_\_

Зурахов В. С.

От выпускающей кафедры:

Заведующий кафедрой

\_\_\_\_\_

Макаров Авинир

Геннадьевич

Методический отдел:

\_\_\_\_\_

## 1 ВВЕДЕНИЕ К ПРОГРАММЕ ПРАКТИКИ

**1.1 Цель практики:** Сформировать компетенции обучающегося в области проектно-технологической деятельности в области информационной безопасности

**1.2 Задачи практики:**

- закрепление теоретических знаний, полученных в процессе обучения;
- приобретение социально-личностных компетенций, необходимых для работы в профессиональной среде

**1.3 Требования к предварительной подготовке обучающегося:**

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

- Защищенные информационные системы
- Информационно-аналитические системы безопасности
- Организация и технологии защиты персональных данных
- Управление информационной безопасностью
- Криптографические средства защиты информации

## 2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ПРОХОЖДЕНИЯ ПРАКТИКИ

<b>УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий</b>
<b>Знать:</b> стандарты и методики проектирования систем безопасности
<b>Уметь:</b> анализировать и выбирать наиболее эффективные и рентабельные методы защиты разнородной информации в организации
<b>Владеть:</b> опытом обоснования и синтезе проектных решений в области защиты информации в организации
<b>УК-2: Способен управлять проектом на всех этапах его жизненного цикла</b>
<b>Знать:</b> методы представления и описания результатов проектной деятельности
<b>Уметь:</b> обосновывать практическую и теоретическую значимость полученных результатов
<b>Владеть:</b> навыками управления проектами в области, соответствующей профессиональной деятельности; навыками распределения заданий и побуждением других к достижению целей;
<b>ПК-2: Способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой</b>
<b>Знать:</b> принципы формирования и реализации политики безопасности информации в автоматизированных системах
<b>Уметь:</b> анализировать требования к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации
<b>Владеть:</b> опытом формирования разделов технических заданий на создание систем защиты информации
<b>ПК-3: Способен вводить в эксплуатацию и сопровождать системы защиты информации в организации</b>
<b>Знать:</b> порядок организации технического обслуживания и ремонта технических, программных (программно-технических) средств защиты информации
<b>Уметь:</b> осуществлять разработку программы и методики предварительных испытаний системы защиты информации и организации приемочных испытаний системы защиты информации
<b>Владеть:</b> Владеть - навыками организации проведения специальных исследований и специальных проверок технических средств обработки информации ограниченного доступа и опытной эксплуатации и доработки системы защиты информации

## 3 СОДЕРЖАНИЕ ПРАКТИКИ

Наименование и содержание разделов (этапов)	Семестр	Контактная работа	СР (часы)	Форма текущего контроля
		Пр. (часы)		
Раздел 1. Подготовительный этап	4			0
Этап 1. Оформление на предприятие. Инструктаж по технике безопасности. Выбор и анализ предметной области		6	25	

Этап 2. Выбор способов и методов поиска, обработки и хранения производственной информации. Формирование технического задания.	6	25	
Раздел 2. Выбор объекта исследования			
Этап 3. Сбор производственного и графического материала в соответствии с заданием	4	25	Пр
Этап 4. Анализ и обработка собранной производственной информации. (формирование критериев анализа, оценка соответствия нормативным документам и проч.)	6	25	
Раздел 3. Реализация проекта			
Этап 5. Подготовка требуемого инструментального окружения и документов для проектирования/моделирования систем/подсистем защиты информации	8	31	О
Этап 6. Выполнение необходимых расчетов и разработка алгоритмов в соответствии с заданием	8	31	
Раздел 4. Анализ ключевых показателей проектируемой системы информационной безопасности			
Этап 7. Построение системы/подсистемы защиты информации на предприятии.	8	30	О
Этап 8. Тестирование спроектированной системы/подсистемы, оценка соответствию внутренним нормативным документам предприятия и законодательной базе РФ	8	30	
Раздел 5. Заключительный этап			
Этап 9. Подготовка отчета	4	25	Пр
Этап 10. Формирование отчетной документации	4	25	
Этап 11. Создание презентации и подготовка к защите проекта	4	21,75	
Итого в семестре	66	293,75	
Промежуточная аттестация (Зачет с оценкой)	0,25		
<b>Всего контактная работа и СР по дисциплине</b>	<b>66,25</b>	<b>293,75</b>	

#### 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

##### 4.1 Описание показателей, критериев и системы оценивания результатов обучения

###### 4.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
УК-1	Описывает стандарты и методики проектирования систем безопасности. Убедительно обосновывает с юридической, технической и экономической точки зрения выбранные методы защиты информации в организации. Анализирует, оптимизирует и синтезирует новые проектные решения.
УК-2	Излагает методы представления и описания результатов проектной деятельности. Проявляет управленческие способности при работе в коллективе, формирует план работы проектной команды учитывая компетенции и психологические особенности участников. Оформляет отчетные документы на высоком научном и техническом уровне, структурирует и визуализирует результаты проектной деятельности, эффективно и всесторонне ее представляет и презентует
ПК-2	Прописывает и успешно реализует алгоритм разработки политик безопасности в автоматизированных системах учитывая их функционал и специфику. Наглядно демонстрирует и протоколирует процесс выявления угроз через системный и сравнительный анализ автоматизированных систем.

	Формирует эффективное техническое задание, качество распределяет время и трудозатраты при планировании личного графика и в рабочей команде.
ПК-3	<p>Прописывает программу и инструментарий тестирования технических и программных средств защиты информации.</p> <p>Реализует алгоритм проверки системы защиты информации или ее отдельных подсистем на наличие уязвимостей, эффективность работы и соответствие необходимым нормативным документам.</p> <p>Предлагает новые проектные решения по итогу проведенных испытаний по модернизации, оптимизации или обслуживанию системы защиты информации</p>

#### 4.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций
	Устное собеседование
5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.
4 (хорошо)	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.
3 (удовлетворительно)	Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов.
2 (неудовлетворительно)	<p>Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки.</p> <p>Попытка использования неразрешенных технических устройств или подсказки другого человека (вне зависимости от успешности такой попытки).</p>

#### 4.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

##### 4.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 4	
1	Как произведен анализ предметной области?
2	Какие факторы повлияли на структуру проекта?
3	Какие технологии выбраны для реализации проекта и почему?
4	Опишите последовательность сбора требований к проекту.
5	Какие методы сбора требований были задействованы?
6	Какова сущность и значение информации в развитии современного общества?
7	Какие документы необходимо изучить, чтобы оформить научно-техническую документацию?
8	Как была построена схема тестирования системы/подсистемы?
9	Какие сторонние сервисы используются в проекте и для чего?
10	С какими информационными объектами были ознакомлены на практике?
11	Дайте определения следующим терминам: информационная безопасность, угроза, уязвимость, риск, методика определения риска.
12	Какие нормативные и проектные документы необходимы для выполнения проекта?
13	Как правильно провести технико-экономическое обоснование системы защиты информации?
14	Структура предприятия, его информационной системы
15	Каков списочный состав предприятия?
16	Каковы цели и задачи проектно-технологической практики?
17	Опишите использование информации отделом информационной безопасности
18	Опишите порядок доступа к служебной информации на предприятии
19	Изложите порядок обследования предприятия на наличие информационных угроз
20	В соответствии с каким принципом рассчитывается сумма возможных затрат на разработку и обслуживание системы защиты информации на предприятии?

#### 4.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

##### 4.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

##### 4.3.2 Форма проведения промежуточной аттестации по практике

Устная  Письменная  Компьютерное тестирование  Иная

##### 4.3.3 Требования к оформлению отчётности по практике

Формой отчётности являются письменный отчёт и дневник.

Форма отчёта предусматривает обязательные к заполнению разделы:

- титульный лист,
- содержание отчёта,
- описание конкретной профильной организации, в которой обучающийся проходил практику: структура, организационная форма, направление деятельности и регулирующие ее нормативные документы, производственные стандарты и пр.,
- изложение сути пройденной практики: объем и вид выполненной работы, возникшие при этом проблемы и пути их разрешения, обозначение результатов практики и т. д.,
- приложения.

При прохождении практики в профильной организации заполняется дневник.

Дневник должен содержать:

- титульный лист,
- задание на практику,
- описание выполняемых работ,
- график прохождения практики,
- отзыв руководителя практики от профильной организации.

Отчет должен быть оформлен в соответствии с ГОСТ 7.32. Объем отчета не более 40 листов.

##### 4.3.4 Порядок проведения промежуточной аттестации 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.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

### 5.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
<b>5.1.1 Основная учебная литература</b>				
Галатенко, В. А.	Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	<a href="https://www.iprbooks.hop.ru/97562.html">https://www.iprbooks.hop.ru/97562.html</a>
Моргунов, А. В.	Информационная безопасность	Новосибирск: Новосибирский государственный технический университет	2019	<a href="https://www.iprbooks.hop.ru/98708.html">https://www.iprbooks.hop.ru/98708.html</a>
<b>5.1.2 Дополнительная учебная литература</b>				
Батоврин В. К.	Системная и программная инженерия. Словарь-справочник	Саратов: Профобразование	2017	<a href="http://www.iprbookshop.ru/63956.html">http://www.iprbookshop.ru/63956.html</a>

Ружников, В. А., Вержаковская, М. А., Аронов, В. Ю.	Экономика программной инженерии	Самара: Поволжский государственный университет телекоммуникаций и информатики	2016	<a href="http://www.iprbookshop.ru/73844.html">http://www.iprbookshop.ru/73844.html</a>
Соловьев, Н. А., Юркевская, Л. А.	Введение в программную инженерию	Оренбург: Оренбургский государственный университет, ЭБС АСВ	2017	<a href="http://www.iprbookshop.ru/71267.html">http://www.iprbookshop.ru/71267.html</a>

## 5.2 Перечень профессиональных баз данных и информационно-справочных систем

Зарубежные базы данных ограниченного доступа:

Scopus - база данных рефератов и цитирования URL: <http://www.scopus.com/>

ScienceDirect - 4 коллекции: Chemistry, Engineering, Materials Science, Physics and Astronomy URL: <http://www.sciencedirect.com/>

Российские базы данных ограниченного доступа:

Кодекс URL: <http://www.kodeks.ru/>

РОСПАТЕНТ URL: <http://www1.fips.ru/>

ВИНИТИ URL: <http://www2.viniti.ru/>

eLIBRARY.ru URL: <http://www.eLIBRARY.ru/>

КонсультантПлюс (правовые документы) URL: <http://www.consultant.ru/>

## 5.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows

MicrosoftOfficeProfessional

## 5.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по практике

Аудитория	Оснащение
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду