

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Б2.В.03(П)
(индекс практики)

ПРОГРАММА ПРАКТИКИ

Производственная практика (технологическая (проектно-технологическая практика)) 3
(наименование практики)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)

Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 4 ЗЕ

Распределение часов практики по семестрам

Семестр	7	Итого
Форма контроля	зачет с оценкой	
Вид занятий		
Самостоятельная работа под руководством преподавателя	1,8	1,8
Промежуточная аттестация	0,2	0,2
Контактная работа	2	2
Иные формы	142	142
Итого	144	144

Программу практики составил(и):

Власов И.А.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование программы практики:

☐

Отсутствует

☐

Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Программа практики составлена на основании ФГОС ВО и учебного плана
направления подготовки 09.03.03 Прикладная информатика

Срок действия программы практики до «31» августа 2027 г.

УТВЕРЖДЕНО

На заседании ИИиЭБ

(протокол заседания № 2 от «сентября» 2022г.)

Производственная практика (технологическая (проектно-технологическая практика)) 3

1. Цель практики

Цель – закрепление теоретических знаний, полученных студентами в процессе обучения в ВУЗе на основе практического применения их в практической деятельности, целенаправленного формирования профессиональных навыков, необходимых для последующего выполнения должностных обязанностей в области информационной безопасности.

2. Место практики в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная практика: «Техническая защита информации», «Аудит защищенности информационных систем», «Информационная безопасность компьютерных сетей».

Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее: «Обеспечение безопасности критической информационной инфраструктуры», «Безопасность веб-приложений», «Безопасность баз данных», «Мониторинг событий информационной безопасности».

3. Вид практики, способ и форма (формы) ее проведения

Вид практики: производственная практика (технологическая (проектно-технологическая практика)).

Форма проведения практики: дискретно.

4. Тип практики

технологическая (проектно-технологическая) практика

5. Место проведения практики

Промышленные предприятия г.о. Тольятти (отделы информационной безопасности).

6. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-1 Способен осуществлять оптимизацию управления жизненным циклом распределенных данных с учетом информационной безопасности	ПК-1.4 Демонстрирует понимание работы реляционной модели данных и принципов защиты информации при ее построении и эксплуатации	Знать: -технические каналы утечки информации - реляционную модель данных СЗИ
		Уметь: - получать информацию от сетевых сервисов
		Владеть: -методами количественного анализа процессов обработки,

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.1 Применяет методику, средства и инструменты для проведения мониторинга	поиска и передачи информации
		Знать: - способы и средства защиты информации от утечек по техническим каналам - средства и инструменты анализа защищенности
		Уметь: - измерять физические параметры сигнала и определять комплекс мер по защите сигнала от утечек - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть: - навыками работы с программно-аппаратными комплексами защиты информации по техническим каналам
ПК-8 Способен составлять технико-экономическое обоснование проектных решений и техническое задание на разработку программного обеспечения	ПК-8.6 Демонстрирует умение выстраивать процесс управления ИБ на основе риск - ориентированного подхода	Знать: - принципы и требования разработки безопасного ПО - модели представления системы информационной безопасности
		Уметь: - встроить в процесс управления ИБ мониторинг безопасной разработки
		Владеть: - методами оценки инвестиций в информационную безопасность
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.7 Демонстрирует умение разрабатывать ОРД	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь: - разрабатывать и пользоваться нормативными документами по защите информации - разрабатывать политику безопасности

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		Владеть: - навыками разработки ОРД на основе определения границ безопасности инфраструктуры

7. Структура и содержание практики

Вид учебной работы	Этапы практики	Семестр	Объем, ч.	Баллы	Формы текущего контроля (наименование оценочного средства)
ИФ	Ознакомление с нормативной документацией	7	2	-	-
ИФ	Ознакомление со сроками прохождения практики	7	1	-	-
ИФ	Практическое задание 1 Подписанный со стороны профильной организации договор по практике	7	2	10	Подписанный со стороны профильной организации договор по практике
ИФ	Ознакомление с общим рабочим графиком (планом) проведения практики	7	1	-	-
ИФ	Практическое задание 2 Индивидуальный график (план) проведения практики	7	10	5	Индивидуальный график (план) проведения практики
ИФ	Практическое задание 3 Анализ состава и использования технических средств защиты информации на предприятии	7	29	10	Раздел отчета по практике
ИФ	Практическое задание 4 Аудит информационных процессов в операционных системах Windows	7	29	10	Раздел отчета по практике
ИФ	Практическое задание 5 Межсетевое экранирование. Настройка МЭ.	7	29	15	Раздел отчета по практике
ИФ	Практическое задание 6 Выводы по результатам анализа защищенности сетевой инфраструктуры предприятия	7	39	50	Отчет по практике
СРП	Консультации с руководителем практики	7	1,8	-	-
ПА	Сдача зачета с оценкой	7	0,2	-	Вопросы к зачету
Форма (формы) отчетности по практике					Наличие оформленного отчета
Итого:			144	100	

8. Образовательные технологии

Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Самостоятельная работа. Индивидуальное задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
Формы и методы обучения		
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

9. Методические указания

Прохождение практики подразумевает выполнение практических заданий:

Ознакомление с нормативной документацией

Ознакомление со сроками прохождения практики

Практическое задание 1. При выполнении данного задания обучающиеся оформляют договор с организацией на прохождение практики. Итогом выполнения этого задания является - Подписанный со стороны профильной организации договор по практике.

Ознакомление с общим рабочим графиком (планом) проведения практики

Практическое задание 2. При выполнении данного задания обучающиеся составляют по программе практики индивидуальный график проведения практики. С указанием сроков выполнения всех заданий. Итогом выполнения данного задания является - Индивидуальный график (план) проведения практики.

Практическое задание 3. При выполнении данного задания обучающиеся собирают данные, анализируют и заполняют таблицу с характеристиками технических

средств защиты информации используемых на предприятии с примерами их использования.

Итогом выполнения данного задания является - Аналитический отчет с выполненным заданием.

Практическое задание 4. При выполнении данного задания учащиеся исследуют организацию аудита информационных процессов в сетевых операционных системах Windows.

Результаты исследования отдельных категорий аудита должны включать описание, как проводились исследования, примеры различных событий данной категории, интерпретацию информации, выдаваемой для отдельных событий, анализ связи отдельных событий, полученные результаты и сделанные выводы.

Итогом выполнения данного задания является - Аналитический отчет с выполненным заданием.

Практическое задание 5. При выполнении данного задания учащиеся изучают технологию анализа защищенности сетевой инфраструктуры предприятия, средства анализа защищенности сетевых протоколов и сервисов, применяемые технологии обнаружения атак, методы реагирования.

Итогом выполнения данного задания является – презентация на тему « Средства анализа защищенности сетевых протоколов и сервисов применяемых на предприятии за защиты сетевой инфраструктуры».

Практическое задание 6. При выполнении данного задания учащиеся готовят отчет по практике. В отчете кроме результатов анализа из задания №3, №4, №5 должны быть отражены:

- какие методы анализа сетевой информации применяются на предприятии.

Заключение должно содержать:

- краткие выводы по результатам практики или отдельных ее этапов;
- оценку полноты решений поставленных задач;
- разработку рекомендаций по конкретному использованию результатов практики.

10. Оценочные средства

10.1. Паспорт оценочных средств

Код контролируемой компетенции (или ее части)	Наименование оценочного средства
ПК-1; ПК-6; ПК-8; ПК-9	<i>Вопросы к зачету с оценкой № 1-60 Отчет по практике</i>

10.2. Типовые задания или иные материалы, необходимые для текущего контроля успеваемости

10.2.1. Договор по практике

(наименование оценочного средства)

Типовой(ые) пример(ы) задания(ий)

Поиск профильной организации, заключение договора, загрузка договора в курс.

Краткое описание и регламент выполнения

Обучающийся оформляет договор по практике.

Загружает в систему Росдистант.

Критерии оценки:

Наличие договора в контенте – задание выполнено.

Отсутствие договора в контенте – задание не выполнено.

10.2.2. Индивидуальный график проведения практики**Типовой(ые) пример(ы) задания(ий)**

Составление и согласование индивидуального графика (плана) проведения практики

Краткое описание и регламент выполнения

Обучающийся составляет индивидуальный график проведения практики

Обучающийся согласовывает индивидуальный график проведения практики с руководителем по практике и представителем от профильной организации.

Учащийся загружает индивидуальный график в контент.

Критерии оценки:

Наличие индивидуального графика (плана) проведения практики в контенте – задание выполнено.

Отсутствие индивидуального графика (плана) проведения практики в контенте – задание не выполнено.

10.2.3. Анализ состава и использования технических средств защиты информации на предприятии**Типовой(ые) пример(ы) задания(ий)**

. Обучающийся, используя полученные знания заполняет таблицу с характеристиками известных ему вирусов, или выявленных на предприятии.

Проведя анализ выбирает антивирусное ПО для реализации политики безопасности компании.

Краткое описание и регламент выполнения

1. Заполнить таблицу классификации известных вирусов.

Название	Среда обитания	Способ заражения среды обитания	Способ воздействия	Особенности алгоритма

2. Посетить сайты наиболее известных разработчиков антивирусных программ:
– Антивирус Касперского (<http://www.kaspersky.ru/>), – Доктор Web (<http://www.drweb.com/>), – NOD32 (<http://www.esetnod32.ru/>), – Avast! (<http://www.avast-russia.com/>).

3. Исходя из информации, представленной на сайтах разработчиков антивирусного ПО, проанализировать виды угроз, от которых гарантированно предоставляется защита. Анализ проводить по параметрам защиты от:

- 1) мошеннического ПО;
- 2) хакерских атак;
- 3) фишинга;

4) спама

. Результаты представить в виде статистической гистограммы, используя средства программного продукта MS Excel. На основе полученных результатов выбрать антивирусное ПО для реализации политики безопасности компании.

Привести обоснование выбора в виде сравнительного отчета выбранного продукта с остальными продуктами по следующим показателям:

- а) стоимость;
- б) надежность;
- в) устойчивость;
- г) простота использования;
- д) наличие специальных предложений

Критерии оценки:

Наличие выполненного задания в контенте – задание выполнено.

Отсутствие выполненного задания в контенте – задание не выполнено.

10.2.4. Аудит информационных процессов в операционных системах Windows

Типовые примеры заданий

1 Исследование организации аудита информационных процессов в сетевых операционных системах Windows.

Краткое описание и регламент выполнения

При выполнении данного задания обучающиеся:

1. Знакомятся с программой просмотра событий. Знакомятся с различными видами журналов, их структурой. Приводят отрывки журналов в отчете, дают интерпретацию отдельных записей журналов.
 2. Знакомятся с возможностями настройки журналов, параметрами фильтрации записей. Сохраняют журнал в текстовом виде и экспортируют его в Excel.
 3. Знакомятся с аудитом доступа к объектам. Устанавливают определенные права аудита на созданный ими каталог и вложенные в него файлы. Приводят их в отчете.
 4. Включают аудит входов в систему и событий входа в систему, исследуют события, отнесенные к данной категории аудита, дают интерпретацию информации, выдаваемой для отдельных событий. Проводят анализ связи отдельных событий, делают выводы по результатам анализа.
 5. Исследуют аудит управления учетными записями.
 6. Исследуют аудит использования привилегий.
 7. Исследуют аудит изменения политик.
 8. Знакомятся с аудитом системных событий
 9. Исследуют возможности аудита процессов.
- Обучающийся загружает задание в контент.

Критерии оценки:

Наличие выполненного задания в контенте – задание выполнено.

Отсутствие выполненного задания в контенте – задание не выполнено.

10.2.5. Анализ защищенности и обнаружение атак.

Типовые примеры заданий

1. Технология анализа защищенности сетевой инфраструктуры предприятия
2. Средства анализа защищенности сетевых протоколов и сервисов
3. Применяемые технологии обнаружения атак
4. Методы реагирования
- 5.

Краткое описание и регламент выполнения

При выполнении данного задания обучающиеся изучают:

- технологию анализа защищенности сетевой инфраструктуры предприятия, средства анализа защищенности сетевых протоколов и сервисов, применяемые технологии обнаружения атак, методы реагирования.

Итогом выполнения данного задания является – презентация на тему «Средства анализа защищенности сетевых протоколов и сервисов, применяемых на предприятии за защиты сетевой инфраструктуры».

Обучающийся загружает задание в контент.

Критерии оценки:

Наличие выполненного задания в контенте – задание выполнено.

Отсутствие выполненного задания в контенте – задание не выполнено.

10.3. Оценочные средства для промежуточной аттестации

10.3.1. Вопросы к промежуточной аттестации

№ п/п	Вопросы к зачету с оценкой
1.	Цели и задачи, решаемые СУИБ
2.	Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ
3.	Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ
4.	Внедрение процессов управления ИБ: этапы и последовательность
5.	Назовите критерии, согласно которым происходит выбор решения программно-аппаратных и технических средств защиты информации
6.	Обоснуйте необходимость участия пользователя в создании проектной документации в процессе создания ИС и ИТ
7.	Охарактеризуйте наиболее часто применяемые методы и варианты организации создания информационных систем и информационных технологий в управлении
8.	Охарактеризуйте понятие и определите назначение онтологии предметной области
9	Программные средства аудита ИБ
10	Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия
11	Мониторинг эффективности мер по обеспечению ИБ и процессов

	управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ
12	Угрозы ИБ и их источники
13	Анализ информационных рисков предприятия. Методы оценивания информационных рисков
14	Подготовка предприятий к проведению аудита ИБ
15	Задачи и содержание работ при проведении аудита ИБ
16	Планирование процедуры аудита ИБ
17	Алгоритм проведения аудита безопасности предприятия
18	Перечень и систематизация данных, необходимых для проведения аудита ИБ
19	Выработка рекомендаций и подготовка отчетных документов по результатам аудита
20	Экономическая оценка обеспечения ИБ
21	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
22	Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
23	Из каких четырех доменов состоит CobiT?
24	Порядок проведения аттестационных испытаний объектов вычислительной техники и автоматизированных систем в ходе аудита ИБ
25	Мониторинг работоспособности аппаратных компонент автоматизированных систем
26	Нормативно-правовые акты по организации и проведению аудита ИБ
27	Определить содержание отчёта и заключения по результатам аудита ИБ
28	Сформировать программу аудита ИБ для выбранных областей обеспечения ИБ объекта
29	Какие используются на предприятии методы и средства управления процессами передачи информации
30	Основные понятия, виды и источники информации, подлежащей защите
31	Виды анализа защищенности операционной системы
32	Виды систем обнаружения атак
33	Средства анализа защищенности сетевых протоколов и сервисов
34	Какие интерфейсы у межсетевого экрана прикладного уровня?
35	VPN - назначение
36	Способы сегментирования компьютерной сети
37	Виды компьютерных атак
38	Раскрыть цикл компьютерной атаки
39	Что такой пэйлоад, назначение, как применяется
40	Как определяются границы сетевой инфраструктуры
41	Что входит в содержание Политики ИБ
42	Для защиты от атак какого типа предназначена служба конфиденциальности?
43	Какие разделы политики являются общепринятыми?
44	Что такое Атака модификации
45	Какие системы будут защищены межсетевым экраном, если почтовый сервер компании разместить между маршрутизатором и экраном?
46	Какие стандартные события учитываются при аудите безопасности?
47	Играет ли порядок применения правил в межсетевом экране на функционирование сети?

48	Какие цели могут преследоваться при установке IDS?
49	Какими способами вредоносный код может проникнуть в организацию?
50	Какие шаги следует предпринять при обнаружении подозрительного трафика?
51	Какие основные меры необходимо предпринять для защиты сервера от атак злоумышленника через интернет?
52	Раскрыть сущность реляционной модели данных
53	Виды информации, получаемой от сетевых сервисов
54	Назначение и использование NetFloorAnalyzer
55	Перечислить технические каналы утечки информации ПЭМИН
56	СЗИ от ПЭМИН, назначение
57	Что такое безопасная разработка ПО, регламентирующие документы
58	Как в организации выстроить контроль разработки безопасного ПО?
59	Что отражается в ТЗ на разработку ИС с точки зрения ИБ?
60	Как в организации выстроить процесс контроля аутсорсинга на разработку ПО?

10.3.1. Вопросы к промежуточной аттестации

Форма проведения промежуточной аттестации	Критерии и нормы оценки	
	зачет с оценкой (по накопительному рейтингу)	«отлично»
		85-100 баллов
		«хорошо»
		70-84 баллов
	«удовлетворительно»	55-69 баллов
		«неудовлетворительно»
		0-54 баллов

11. Учебно-методическое и информационное обеспечение практики

11.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Нестеров С.А.	Основы информационной безопасности	учебное пособие	2022	эбс-Лань
2	Прохорова О. В.	Информационная безопасность и защита информации	учебное пособие	2022	эбс-Лань
3	Раков А.С., Маслов О.Н., Губарева О.Ю., Почепцов А.О., Гуреев В.О.	Техническая защита информации: учебное пособие	учебное пособие	2020	эбс-Лань
5	Горбачев, А. А.	Техническая защита информации. Поисковые приборы	учебное пособие	2022	эбс-Лань
6	Н.В. Скабцов	Аудит безопасности информационных систем	учебно-методическое пособие	2020	эбс-Лань

11.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	Ясенев В.Н.	Информационная безопасность	учебное пособие	2019	эбс-Лань

2.	Рагозин Ю. Н.	Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности	учебное пособие	2019	эбс-Лань
3.	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства	учебное пособие	2019	https://e.lanbook.com/book/1122

11.3. Перечень профессиональных баз данных и информационных справочных систем

- Нормативные правовые документы. [Электронный ресурс] Режим доступа: <http://www.consultant.ru>
 - Документы ФСТЭК [Электронный ресурс] Режим доступа: <http://www.fstec.ru/>
 - Электронная библиотечная система IPRbooks. [Электронный ресурс] Режим доступа: <http://www.iprbookshop.ru/>
 - Научная электронная библиотека [Электронный ресурс] Режим доступа: <http://elibrary.ru/defaultx.asp?>
 - Энциклопедия информационной безопасности. [Электронный ресурс] Режим доступа: <https://securelist.ru/enciklopediya>
 - Набор технологий и программ для работы в сети [Электронный ресурс] Режим доступа: <http://internetsecure.ru/>
 - Информационно-аналитический портал по безопасности [Электронный ресурс] Режим доступа: <http://www.anti-malware.ru/>
 - Национальный форум информационной безопасности [Электронный ресурс] Режим доступа: <http://www.infoforum.ru/>
 - Журнал «Защита информации. Инсайд» [Электронный ресурс] Режим доступа: <http://www.inside-zi.ru>
 - Портал «InformationSecurity» [Электронный ресурс] Режим доступа: <http://www.itsec.ru>
 - Журнал «Безопасность информационных технологий» [Электронный ресурс] Режим доступа: <https://bit.spels.ru/index.php/bit/index>
 - Библиотека ИБ – эксперта [Электронный ресурс] Режим доступа: <https://securitymedia.org/info/biblioteka-ib-eksperta.html>
 - Банк угроз ФСТЭК [Электронный ресурс] Режим доступа: <https://bdu.fstec.ru/threat-section/negatives>
 - Форум Античат [Электронный ресурс] Режим доступа: <https://forum.antichat.com>
 - Справочно-правовая система по законодательству Российской Федерации [Электронный ресурс]. Режим доступа: <http://www.garant.ru>
 - Информационно-правовая система по законодательству Российской Федерации [Электронный ресурс]. Режим доступа: <http://www.kodeks.ru>
 - WebofScience [Электронный ресурс]: мультидисциплинарная реферативная база данных. – Philadelphia: ClarivateAnalytics, 2016–. – Режим доступа: apps.webofknowledge.com. – Загл. с экрана. – Яз. рус., англ.
 - Scopus [Электронный ресурс]: реферативная база данных. – Netherlands: Elsevier, 2004–. – Режим доступа: scopus.com. – Загл. с экрана. – Яз. рус., англ.
 - Elibrary [Электронный ресурс]: научная электронная библиотека. – Москва: НЭБ, 2000–. – Режим доступа: elibrary.ru. – Загл. с экрана. – Яз. рус., англ.
 - SpringerLink [Электронный ресурс]: [база данных]. – Switzerland: SpringerNature, 1842–. – Режим доступа: link.springer.com. – Загл. с экрана. – Яз. англ.
 - ScienceDirect [Электронный ресурс]: коллекция электронных книг издательства Elsevier. – Netherlands: Elsevier, 2018–. – Режим доступа: sciencedirect.com. – Загл. с экрана. – Яз. англ.
 - Cambridgeuniversitypress [Электронный ресурс]: журналы издательства. – Cambridge: Cambridgeuniversitypress, 2018–. – Режим доступа: cambridge.org. – Загл. с экрана. – Яз. англ.
- NEICON [Электронный ресурс]: электронная информация: архив научных журналов. – Москва: НЭИКОН, 2002–. – Режим доступа: neicon.ru/resources/archive. – Загл. с экрана. – Яз. рус., англ.

11.4. Перечень программного обеспечения

№ п/ п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	Office Standart	- OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3	Консультант+	- Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

11.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по практике

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
4	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф