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

Б2.В.02(П)
(индекс практики)

ПРОГРАММА ПРАКТИКИ

Производственная практика (технологическая (проектно-технологическая практика)) 2
(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	6	**Итого**
Форма контроля / **Вид занятий**	зачет с оценкой	
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)) 2

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: «Технологии и методы социальной инженерии», «Криптографические методы защиты информации», «Программно-аппаратные средства защиты информации», «Защита информации от вредоносного программного обеспечения».

Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее: «Техническая защита информации», «Аудит защищенности информационных систем», «Информационная безопасность компьютерных сетей».

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**
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 Определяет свою роль в команде для достижения поставленной цели	Знать: Должностные обязанности согласно задачам проекта
		Уметь: Реализовывать полученные теоретические знания на практике
		Владеть: Методами командной разработки проектов ИБ в области защиты информации
ПК-7 Способен	ПК-7.5 Демонстрирует	

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
разрабатывать и внедрять организационные меры по защите информации на основе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации	навыки организации работы коллектива исполнителей, определение порядка выполнения работ по осуществлению правового, организационного и технического обеспечения защиты информации	Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь: применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах
		Владеть: навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности
ПК-8 Способен составлять технико-экономическое обоснование проектных решений и техническое задание на разработку программного обеспечения	ПК-8.5 Демонстрирует навыки построения как отдельных процессов управления ИБ, так и системы процессов в целом.	Знать: принципы построения и развития социальной инженерии, основы теории системного подхода при решении задач защиты информации
		Уметь: провести оценку проблемной ситуации в сфере социальной инженерии, выявить основные закономерности и тенденции применения форм и методов нарушителями
		Владеть: Владеет основами социнженерии, методами работы нарушителей с целью их выявления и нейтрализации

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	6	2	-	-
ИФ	Ознакомление со сроками прохождения практики	6	1	-	-
ИФ	Практическое задание 1 Подписанный со стороны профильной организации договор по практике	6	2	10	Подписанный со стороны профильной организации договор по практике
ИФ	Ознакомление с общим рабочим графиком (планом) проведения практики	6	1	-	-
ИФ	Практическое задание 2 Индивидуальный график (план) проведения практики	6	10	5	Индивидуальный график (план) проведения практики
ИФ	Практическое задание 3 Классификация вредоносного ПО, его обнаружение, нейтрализация. Составить характеристику вирусов.	6	29	10	Раздел отчета по практике
ИФ	Практическое задание 4 Исследование методов и способов социальной инженерии, которые помогут распознать и предотвратить ее.	6	29	10	Раздел отчета по практике
ИФ	Практическое задание 5 Межсетевое экранирование. Настройка МЭ.	6	29	15	Раздел отчета по практике
ИФ	Практическое задание 6 - выводы по результатам анализа функциональности и задач средств защиты информации предприятия - выводы по мероприятиям противодействия соц.инженении на предприятии	6	39	50	Отчет по практике
СРП	Консультации с руководителем практики	6	1,8	-	-
ПА	Сдача зачета с оценкой	6	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 используя полученные знания заполняют таблицу с характеристиками известных ему вирусов, или выявленных на предприятии.

Проведя анализ выбирают антивирусное ПО для реализации политики безопасности компании. Итогом выполнения данного задания является - Аналитический отчет с выполненным заданием.

Практическое задание 4. При выполнении данного задания учащиеся используют интернет-браузер для исследования случаев социальной инженерии, обобщают четыре примера, найденные в исследовании, используют способы распознавания социальной инженерии, описывают три примера, найденные в исследовании, устанавливают какие процедуры и методы, помогающие предотвратить социальную инженерию, применяются на предприятии

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

Практическое задание 5. При выполнении данного задания учащиеся производят настройку МЭ (напр. iptables) для блокирования «Brute force» атаки, анализируют влияние МЭ на угрозу подбора пароля, мониторят попытку подбора пароля.

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

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 СКЗИ внедрены на предприятии;
- состав программно-аппаратных СЗИ, использующихся 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
УК-3, ПК-8, ПК-7	*Вопросы к зачету с оценкой № 1-60* *Отчет по практике*

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. Классификация вредоносного ПО, его обнаружение, нейтрализация. Составить характеристику вируса

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. Исследование методов и способов социальной инженерии, которые помогут распознать и предотвратить ее

Типовые примеры заданий

1 Исследование случаев социальной инженерии (СИ)

2 Исследование способов распознавания социальной инженерии

3 Описание процедур, помогающих предотвратить СИ на предприятии

Краткое описание и регламент выполнения

При выполнении данного задания обучающиеся выполняют:

- используют интернет-браузер для исследования случаев социальной инженерии, обобщают четыре примера, найденные в исследовании;
- используют способы распознавания социальной инженерии, описывают три примера, найденные в исследовании;
- устанавливают какие процедуры и методы, помогающие предотвратить социальную инженерию, применяются на предприятии
- описывают эти методы.

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. Межсетевое экранирование. Настройка МЭ.

Типовые примеры заданий

Настройка МЭ на блокировку подбора пароля.

Краткое описание и регламент выполнения

При выполнении данного задания обучающиеся выполняют:

- настройку МЭ (напр. iptables) для блокирования «Brute force» атаки
- анализируют влияние МЭ на угрозу подбора пароля
- производят успешную атаку подбора пароля
- мониторят попытку подбора пароля
- результат сохраняют на скриншоте.

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.	Что называют «вредоносным программным обеспечением»?
2.	Какое наказание предусмотрено в УК РФ за распространение вредоносного программного обеспечения?
3.	Перечислите законы аналогичные статье 273 УК РФ, действующие за пределами РФ
4.	Что такое макровирус?
5.	Какие типы файлов заражают макровирусы?
6.	Как просмотреть код макрови руса?
7.	Как восстановить файл, зараженный макровирусом?
8.	Классификация по специфике алгоритма действия, примеры
9	Повысится ли устойчивость компьютера к воздействию вируса, если установить два антивирусных продукта одновременно?
10	Каковы внешние проявления наличия вируса в компьютере? Приведите примеры широко известных вирусов
11	Какие программы-доктора вы знаете?
12	Какие вирусы называются резидентными, и в чем особенность таких вирусов?
13	Дать характеристику вируса-невидимки
14	Что представляет «полная изоляция» вируса?
15	Характеристика сетевых вирусов
16	Чем опасны файлово-загрузочные вирусы?
17	Что такое логическая бомба?
18	Что такое ключ?
19	Что такое криптосистема?
20	Пояснить, что такое шифрование и в чём заключается сущность метода Цезаря
21	Пояснить, в чём заключается сущность метода перестановки.
22	Какие вы знаете основные алгоритмы шифрования?
23	Что такое электронная подпись?
24	Для чего используется механизм электронной подписи?
25	Какой метод шифрования использует электронная подпись?
26	Виды ЭП
27	Почему профилактика «троянских программ» связана с системным

	реестром?
28	Какие разделы и ключи реестра являются потенциальными местами запуска «троянских программ»?
29	Какие стандарты действуют на алгоритмы формирования и проверки электронной цифровой подписи в России?
30	В чем заключается проблема сертификации открытых ключей?
31	Каковы функции центра сертификации открытых ключей?
32	Что такое сертификат открытого ключа?
33	Какие задачи выполняет протокол ICMP?
34	Как сканирование может быть использовано злоумышленником?
35	Как определяется открытый порт на хосте?
36	Какие данные позволяют предположить проведение атаки?
37	Каким угрозам подвержены протоколы ARP, IP, TCP, FTP?
38	Какую информацию и на каких уровнях анализирует МЭ?
39	В чем разница между МЭ и СОВ?
40	Какие схемы интеграции МЭ и СОВ существуют? В чем их преимущества и недостатки?
41	Какой командой проверить надежность сетевого взаимодействия устройств?
42	Какие команды используются при сканировании хоста?
43	Таблицы межсетевого экрана Netfilter. Для чего они используются?
44	Как создавать правила для межсетевого экрана утилитой Iptables?
45	Что такое Web Application Firewall?
46	Что такое сетевая система обнаружения вторжений?
47	Чем отличаются пассивные и активные IDS?
48	Шифрование файла с помощью симметричного криптоалгоритма.
49	Методы и средства защиты информации от НСД в локальных ПЭВМ
50	Типы контроля безопасности: потоковый, контроль вывода, контроль доступа
51	Технологии доверенной загрузки операционной системы
52	Принципы сертификации средств защиты информации
53	Управление средствами аутентификации в Linux и Windows
54	Применение типовых моделей управления доступом в операционных системах
55	Как соотносятся матрица доступа и ролевой доступ?
56	Методы внедрения программных закладок
57	Реализация защиты от вредоносного программного кода
58	Механизмы статического скрытия вредоносного программного кода
59	Основные меры по защите от вирусов - шифровальщиков
60	Принцип действия, достоинства и недостатки аппаратных устройств на основе электронных (магнитных) идентификаторов

10.3.1. Вопросы к промежуточной аттестации

Форма проведения промежуточной аттестации	**Критерии и нормы оценки**	
зачет с оценкой (по	«отлично»	85-100 баллов
	«хорошо»	70-84 баллов

накопительному рейтингу)	«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	Попел А. Е.	Социальная инженерия: теория и практика	Уч пособие	2022	эбс-Лань
5	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации	учебное пособие	2022	эбс-Лань
6	Галатенко В.А.	Идентификация и аутентификация, управление доступом	Эл.ресурс	2021	http://citforum.ru/security/articles/galatenko/- (дата обращения - 17.10.2021)

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.	Фомина Н.А.	Использование методов социальной инженерии при мошенничестве в социальных сетях	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: ClarivateAnalitics, 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	Столы-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