

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: 2026

Общая трудоемкость: 5 ЗЕ

**Распределение часов практики по семестрам**

Семестр	6	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	178	178
<b>Итого</b>	<b>180</b>	<b>180</b>

Программу практики составил(и):

Старший преподаватель института инженерной и экологической безопасности Додонов  
А.В.

---

(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» декабря 2031 г.**

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

---

(протокол заседания № 1 от «01» сентября 2025 г.).

## **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: «Компьютерные сети», «Основы моделирования и проектирования программного обеспечения», «Основы управления информационной безопасностью», «Организация обработки персональных данных в организации», «Программирование на Java (Джава) 2», «Программирование на .Net (ДотНет) 2».

Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее: «Криптографические методы защиты информации», «Технологии и методы социальной инженерии», «Программно-аппаратные средства защиты информации», «Компьютерная криминалистика», «Защита информации от вредоносного программного обеспечения».

### **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**

<b>Формируемые и контролируемые компетенции (код и наименование)</b>	<b>Индикаторы достижения компетенций (код и наименование)</b>	<b>Планируемые результаты обучения</b>
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: свою роль в команде для достижения поставленной цели Уметь: определять свою роль в команде для достижения поставленной цели Владеть: навыками определения своей роли в команде для достижения поставленной цели

<b>Формируемые и контролируемые компетенции</b> (код и наименование)	<b>Индикаторы достижения компетенций</b> (код и наименование)	<b>Планируемые результаты обучения</b>
ПК-7 Способен разрабатывать и внедрять организационные меры по защите информации на основе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации	ПК-7.5 Демонстрирует навыки организации работы коллектива исполнителей, определение порядка выполнения работ по осуществлению правового, организационного и технического обеспечения защиты информации	Владеть: Навыками составления документации на разработку ИС
		Знать: Принципы работы с источниками информации
		Уметь: Подбирать нужную информацию
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.	Владеть: Навыками научного поиска, создания научных текстов
		Знать: Законодательство РФ и Нормативные документы регуляторов
		Уметь: Формулировать заключения по проведенным мероприятиям ИБ

## 7. Структура и содержание практики

Вид учебной работ	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	37	-	-
ИФ	Практическое задание 2 Индивидуальный график (план) проведения практики	6	10	5	Индивидуальный график (план) проведения практики
ИФ	Практическое задание 3 Анализ сети предприятия, выявление точек проникновения злоумышленника.	6	29	10	Раздел отчета по практике
ИФ	Практическое задание 4 Настройка ACL или правил межсетевого экрана.	6	29	10	Раздел отчета по практике
ИФ	Практическое задание 5 Изучение локальных нормативных актов предприятия в части обработки ПДн, разработка недостающих.	6	29	15	Раздел отчета по практике
ИФ	Практическое задание 6 Написание отчёта по практике.	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:			180	100	

## 8. Образовательные технологии

<b>Технология традиционного обучения</b> – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Самостоятельная работа. Индивидуальное задание.	Наглядные, словесные, практические.
<b>Технология модульного обучения</b> – 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.
<b>Информационные технологии</b> – 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		
<b>Дистанционное обучение</b>	<b>Сетевая технология</b> – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. <b>CD-технология</b> – 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. Обучающийся анализирует сеть, используя инструменты сканирования (Nmap, Wireshark), документирует архитектуру, выявляет

точки проникновения и предлагает решения по устранению или минимизации этих точек. Итогом выполнения задания является отчёт, включающий в себя схему сети, рекомендации по сегментации и настройкам сетевых устройств.

Практическое задание 4. Обучающийся анализирует сетевой трафик, определяет признаки целевого приложения (порт, протокол, сигнатуры), настраивает правила фильтрации на сетевом оборудовании (коммутатор, маршрутизатор, межсетевой экран) для блокировки или ограничения трафика определённого приложения/протокола и проверяет их работоспособность путём запуска выбранного приложения и попытки передачи данных.

Итогом выполнения данного задания является отчёт с выявленными признаками целевого приложения, конфигурацией правил, а также скриншотами или логами проверки работоспособности правил.

Практическое задание 5. Обучающийся анализирует внутренние документы организации, касающиеся обработки персональных данных, проводит оценку комплектности документов в соответствии с законодательством Российской Федерации и в случае выявления несоответствия разрабатывает проект недостающего документа.

Итогом выполнения задания является отчёт, включающий в себя таблицу соответствия локальных нормативных актов требованиям законодательства, а также проект документа, регламентирующего обработку персональных данных.

Практическое задание 6. При выполнении данного задания учащиеся готовят отчет по практике. В отчёт необходимо включить результаты выполненных заданий 3, 4, 5.

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**

<b>Код контролируемой компетенции (или ее части)</b>	<b>Наименование оценочного средства</b>
УК-3, ПК-8, ПК-7	<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 сети предприятия, выявление точек проникновения злоумышленника**

#### **Типовой(ые) пример(ы) задания(ий)**

Обучающийся анализирует сеть на предмет потенциальных точек проникновения, используя инструменты сканирования (Nmap, Nessus) и методы анализа трафика. На основе результатов предлагаются решения для минимизации рисков.

#### **Краткое описание и регламент выполнения**

Обучающийся начинает с сканирования периметра сети с помощью инструментов Nmap или Nessus, чтобы выявить открытые порты и сервисы, доступные извне. Например, обнаруживается, что сервер с устаревшей версией ПО имеет критическую уязвимость, позволяющую удалённо выполнить произвольный код. Таким же образом производится сканирование внутренних узлов сети для построения схемы сети.

Далее проводится анализ внутренней сети через Wireshark или tcpdump для выявления аномалий в трафике. Выясняется, что устройства IoT (например, камеры) используют незашифрованные протоколы и доступны из всех сегментов сети, что создаёт риск распространения атаки. Проверка системы удалённого доступа (например, RDP или SSH) с помощью Hydra или Medusa показывает отсутствие двухфакторной аутентификации, что упрощает brute-force атаки.

Для поиска уязвимостей в веб-сервисах обучающийся применяет Burp Suite или OWASP ZAP, что позволяет обнаружить возможность SQL-инъекций через незащищённые формы веб-приложений. На основе анализа обучающийся предлагает закрыть неиспользуемые порты на межсетевом экране; обновить ПО и настроить автоматические обновления для веб-сервера; внедрить сегментацию сети через VLAN и 802.1X для изоляции IoT-устройств.

В результате выполнения задания студент должен предоставить отчёт с описанием схемы сети, описанием выявленных уязвимостей, перечнем использованных



инструментов (Nmap, Wireshark), а также рекомендациям по настройке сегментации и сетевых устройств.

**Критерии оценки:**

Наличие выполненного задания в контенте – задание выполнено.

Отсутствие выполненного задания в контенте – задание не выполнено.

**10.2.4. Настройка ACL или правил межсетевого экрана.**

**Типовые примеры заданий**

Обучающийся анализирует сетевой трафик, определяет признаки целевого приложения (порт, протокол, сигнатуры), настраивает правила фильтрации на сетевом оборудовании (коммутатор, маршрутизатор, межсетевой экран) для блокировки или ограничения трафика определённого приложения/протокола и проверяет их работоспособность путём запуска выбранного приложения и попытки передачи данных.

**Краткое описание и регламент выполнения**

Обучающийся начинает с захвата трафика с помощью Wireshark или tcpdump, пытаясь выявить целевое приложение. Например, обнаруживается, что приложение использует UDP-порт 51413 и характерные строки в пакетах (например, BitTorrent protocol). Далее анализируется топология сети: определяется, через какой маршрутизатор или фаервол проходит трафик. Например, выясняется, что трафик торрент-клиента проходит через Cisco ISR 4451. На сетевом оборудовании настраиваются правила фильтрации: `access-list 101 deny udp any any eq 51413`.

Проверка работоспособности правила проводится путём запуска торрент-клиента и добавления тестового торрента. Если правило было корректным образом настроено, попытки подключения к пирам будут блокироваться.

В отчёте о выполнении задания обучающийся указывает выявленные признаки целевого приложения из дампа трафика, конфигурацию правил сетевого оборудования для блокировки этого приложения, а также скриншоты или логи, подтверждающие работоспособность настроенных правил.

**Критерии оценки:**

Наличие выполненного задания в контенте – задание выполнено.

Отсутствие выполненного задания в контенте – задание не выполнено.

**10.2.5. Изучение локальных нормативных актов предприятия в части обработки ПДн, разработка недостающих.**

**Типовые примеры заданий**

Изучение внутренних документов организации, регулирующих обработку персональных данных (ПДн), оценка их соответствия требованиям законодательства РФ (152-ФЗ), разработка проекта недостающего документа при выявлении пробелов.

**Краткое описание и регламент выполнения**

При выполнении данного задания обучающиеся выполняют:

- анализ существующих документов по обработке ПДн в организации;

- выявление несоответствия комплектности или состава документов в соответствии с 152-ФЗ;
- разработку проекта недостающих или изменение несоответствующих законодательству документов.

Например, студент изучил «Политику обработки персональных данных» организации и обнаружил отсутствие раздела об отзыве согласия субъектом персональных данных. Обучающийся разрабатывает проект раздела, согласовывает положения раздела с ответственными лицами в организации и передаёт проект на утверждение. В отчёте по заданию студент оформляет таблицу соответствия локальных нормативных актов требованиям законодательства, а также проект разработанных документов или изменений в них.

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**

<b>№ п/п</b>	<b>Вопросы к зачету с оценкой</b>
1.	Перечислите Источники угроз НСД в ИСПДн
2.	По режиму обработки персональных данных в информационной системе информационные системы подразделяются на два вида. Назовите, какие
3.	К каким видам нарушения безопасности информации может привести реализация угроз НСД?
4.	Что понимается под угрозами безопасности ПДн при их обработке в ИСПДн?
5.	Как могут быть реализованы угрозы безопасности ПДн?
6.	Перечислите источники угроз, реализуемые за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения.
7.	Какая угроза считается актуальной?
8.	Какие показатели применяются для оценки возможности реализации угрозы?
9.	Что понимается под уровнем исходной защищенности ИСПДн?
10.	Что понимается под частотой (вероятностью) реализации угрозы?
11.	Перечислите вербальные показатели опасности для рассматриваемой ИСПДн.
12.	Какое значение имеет вербальный показатель, если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных?
13.	Каковы правила выбора из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн?
14.	Перечислите показатели опасности угрозы
15.	Для каких дальнейших действий необходимо составление перечня актуальных угроз?
16.	При наличии каких условий необходим 3-й уровень защищенности персональных данных?
17.	При наличии каких условий необходим 4-й уровень защищенности персональных данных?
18.	При наличии каких условий необходим 2-й уровень защищенности персональных данных?

19	Какое основное требование к средствам защиты информации установлено в Приказе №21?
20	Что должны обеспечивать меры по идентификации и аутентификации субъектов доступа и объектов доступа?
21	Что должны обеспечивать меры по антивирусной защите?
22	Что включает в себя выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных?
23	В каких случаях применяются компенсирующие меры?
24	Какого класса применяются средства вычислительной техники для обеспечения 3 уровня защищенности персональных данных?
25	Что является основным документом, обеспечивающим защиту персональных данных
26	Кто является субъектом права на семейную тайну
27	Как осуществляется допуск к работе с государственной тайной для организаций
28	В каких случаях возможно ограничение права гражданина на тайну переписки, телефонных и иных переговоров
29	Под какую статью УК РФ попадает такое киберпреступление, как неправомерный доступ к компьютерной информации
30	Для чего нужна идентификация
31	Что НЕ относится к обработке персональных данных
32	Что относится к свойствам обезличенных данных
33	Кто должен соблюдать конфиденциальность персональных данных
34	В каком случае персональные данные НЕ перестают считаться конфиденциальными
35	В каком случае НЕ нужно писать согласие на обработку персональных данных
36	Что относится к биометрическим данным
37	Чем должен руководствоваться работодатель при определении объема и содержания обрабатываемых персональных данных работника
38	Чем характеризуется неавтоматизированная обработка данных
39	Что относится к особой категории данных согласно Конвенции о защите физических лиц при автоматизированной обработке персональных данных
40	В каком случае субъект персональных данных имеет право подать жалобу на оператора
41	Может ли работодатель сообщать персональные данные работника третьим лицам
42	Что обязательно должно быть указано в Уведомлении в Роскомнадзор о начале обработки персональных данных
43	Что относится к мерам внешней защиты персональных данных
44	Каков срок уничтожения персональных данных
45	В каком случае НЕ нужно отправлять в Роскомнадзор Уведомление об обработке персональных данных
46	Кто назначает лицо, ответственное за организацию обработки персональных данных
47	Какова периодичность плановых проверок в отношении операторов персональных данных
48	Кто несет ответственность за распространение персональных данных
49	Какая часть политики информационной безопасности определяет важность ОБИ, роль сотрудников, нормативно-правовые основы
50	Для чего нужна подсистема предотвращения утечки информации
51	Как называется подсистема, которая предназначена для поддержания в

	актуальном состоянии организационно-распорядительных документов по обеспечению ИБ
52	Что отражает обобщенная информационная модель системы защиты
53	Что такое границы информационной системы
54	Что выполняется на первом этапе проведения аудита систем информационной безопасности. Каких средств достаточно для эффективного предотвращения попыток несанкционированного доступа к данным
55	Цели и задачи управления ИБ
56	Ключевые процессы СУИБ
57	Механизм взаимодействия и применения стандартов системы управления ИБ
58	Существующие стандарты и методологии по управлению ИБ.
59	Задачи, функции, права и ответственность руководителя и руководителей подразделений службы защиты информации.
60	Персонал предприятия как объект защиты.
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 макровируса?
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 скрывания 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 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	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	<a href="http://citforum.ru/security/articles/galatenko/">http://citforum.ru/security/articles/galatenko/</a> - (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.	Яснев 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	<a href="https://e.lanbook.com/book/1122">https://e.lanbook.com/book/1122</a>

### 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](https://apps.webofknowledge.com). – Загл. с экрана. – Яз. рус., англ.
  - Scopus [Электронный ресурс]: реферативная база данных. – Netherlands: Elsevier, 2004–. – Режим доступа: [scopus.com](https://scopus.com). – Загл. с экрана. – Яз. рус., англ.
  - Elibrary [Электронный ресурс]: научная электронная библиотека. – Москва: НЭБ, 2000–. – Режим доступа: [elibrary.ru](http://elibrary.ru). – Загл. с экрана. – Яз. рус., англ.
  - SpringerLink [Электронный ресурс]: [база данных]. – Switzerland: SpringerNature, 1842–. – Режим доступа: [link.springer.com](https://link.springer.com). – Загл. с экрана. – Яз. англ.
  - ScienceDirect [Электронный ресурс]: коллекция электронных книг издательства Elsevier. – Netherlands: Elsevier, 2018–. – Режим доступа: [sciencedirect.com](https://sciencedirect.com). – Загл. с экрана. – Яз. англ.
  - Cambridgeuniversitypress [Электронный ресурс]: журналы издательства. – Cambridge: Cambridgeuniversitypress, 2018–. – Режим доступа: [cambridge.org](https://cambridge.org). – Загл. с экрана. – Яз. англ.
- NEICON [Электронный ресурс]: электронная информация: архив научных журналов. – Москва: НЭИКОН, 2002–. – Режим доступа: [neicon.ru/resources/archive](http://neicon.ru/resources/archive). – Загл. с экрана. – Яз. рус., англ.

#### 11.4. Перечень программного обеспечения

<b>№ п/ п</b>	<b>Наименование ПО</b>	<b>Реквизиты договора (дата, номер, срок действия)</b>
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

<b>№ п/п</b>	<b>Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)</b>	<b>Перечень основного оборудования</b>
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