МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор института автоматики и информационных технологий

_____ Ю.Ю. Громов
«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.О.01.01(У) Ознакомительная практика
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование)

Специализация

Безопасность открытых информационных систем
(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***
(наименование кафедры)

Составитель:

		И.А. Дьяков
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

	И.А. Дьяков
подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Практика входит в состав обязательной части образовательной программы.

Таблица 1.1 - Результаты обучения по практике

Код, наименование индикатора	Результаты обучения по практике
УК-3 Способен организовывать и руководить работой команды, разрабатывать командную стратегию для достижения поставленной цели	
ИД7-(УК-3) Владеет первичными навыками организации и руководства работой команды, выработки командной стратегии для достижения поставленной цели	владение способностью понимать социальную значимость своей будущей профессии
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства для решения задач профессиональной деятельности	
ИД7-(ОПК-2) Владеет навыками применения программных средств системного и прикладного назначений, в том числе отечественного производства для решения задач профессиональной деятельности	владение первичными навыками поиска, изучения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная.
Тип практики: ознакомительная.
Способ проведения практики: стационарная; выездная.
Форма проведения практики: дискретно.

Объем практики составляет 3 зачетных единицы, продолжительность - 108 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	2 семестр
Контактная работа	**19**
консультации	18
промежуточная аттестация	1
Самостоятельная работа	**89**
Всего	**108**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить особенности информации, обрабатываемой в информационной системе организации, способы обеспечения её конфиденциальности, целостности и доступности;
- ознакомиться с документами по организации защиты информации, техническими и программно-аппаратными средствами обеспечения информационной безопасности;
- приобрести опыт самоорганизации и самообразования; работы в коллективе; поиска информации в компьютерных системах, сетях, библиотечных фондах; оформления отчётов о научных исследованиях; освоения новых образцов программных, технических средств и информационных технологий; поиска, изучения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.

Каждый обучающийся получает также индивидуальное задание, связанное с:

- изучением и практическим освоением современных информационных технологий;
- поиском информации в компьютерных системах, сетях, библиотечных фондах;
- систематизацией и обобщением научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин– Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 702 с. – Режим доступа: http://www.iprbookshop.ru/63594.html. – ЭБС «IPRbooks».
2. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ В.И. Васильев–Электрон. текстовые данные. –М.: Машиностроение, 2013. – 172 с. – Режим доступа: http://www.iprbookshop.ru/18519.html. – ЭБС «IPRbooks».
3. Паршин, К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс]: учебное пособие/ К.А. Паршин– Электрон. текстовые данные. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015. – 96 с. – Режим доступа: http://www.iprbookshop.ru/45291.html. – ЭБС «IPRbooks»

4.2 Периодическая литература

1. Журнал «Вопросы защиты информации». Способ доступа к архиву изданий: http://izdat.ntckompas.ru/editions/for_readers/archive/?SECTION_ID=155
2. Журнал «Проблемы информационной безопасности. Компьютерные системы» Способ доступа к архиву изданий: http://jisp.ru/o-zhurnale/arxiv-nomerov/
3. Журнал «Информация и безопасность». Способ доступа к архиву изданий: http://kafedrasib.ru/index.php/informatsiya-bezopasnost/arkhiv-vypuskov

4.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru
Справочно-правовая система «Консультант+» http://www.consultant-urist.ru
Справочно-правовая система «Гарант» http://www.garant.ru
База данных Web of Science https://apps.webofknowledge.com/
База данных Scopus https://www.scopus.com
Портал открытых данных Российской Федерации https://data.gov.ru
База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata
База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/
База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
Базы данных Министерства экономического развития РФ http://www.economy.gov.ru
База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata
Электронная база данных «Издательство Лань» https://e.lanbook.com
Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru
База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru
База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru
Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф
Национальный портал онлайн обучения «Открытое образование» https://openedu.ru
Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Наряду с решением основных задач, в процессе проведения учебной практики желательно ознакомить студентов с историей развития информационных технологий, базовыми информационными технологиями и их местом в системах автоматизированного управления.

Основными мероприятиями учебной практики являются:

– ознакомление с информационной системой и подсистемой информационной безопасности предприятий (организаций, учреждений) г. Тамбова;

– ознакомление с особенностями работы и функциональными обязанностями должностных лиц по обеспечению информационной безопасности;

– ознакомление с современными техническими, программными и аппаратными средствами обеспечения информационной безопасности;

– ознакомление с современными методами обеспечения совместимости, переносимости и масштабируемости информационных систем;

– ознакомление с технологиями и средствами обеспечения защищённого электронного документооборота;

– изучение документации по организационному обеспечению информационной безопасности;

– изучение документов по правовому обеспечению информационной безопасности;

– личное участие в подготовке сообщений и разработке презентаций на заданные темы;

– личное участие в разработке простейших программ для ЭВМ.

В процессе учебной практики возможно использование следующих технологий образовательного процесса:

1. Технология презентации знаний (основана на поведении преподавателя, в которой преобладает приоритет и опора на методические приёмы преподнесения знаний).

2. Технократическая технология (приоритет отдается использованию технических средств, особенно персонального компьютера). Система формализации знаний, запрограммированных форм и методов проведения занятий, жесткого регламента.

3. Технология адаптивного типа (предполагает регулярную корректировку форм занятий и стилей обучения).

4. Технология социально-психологического типа (использование социально-психологических характеристик восприятия личностью и группой определенного объема знаний и методов обучения, восприятия преподавателя студентами и т.д.).

5. Технология креативного обучения (используется творческий потенциал личности, способность к творчеству, к неординарному восприятию материала и т.д.). Основное– постановка проблем, обсуждение их содержания.

6. Технология самообразования (самостоятельное освоение отдельных вопросов, роль руководителя – консультационная).

Руководитель практики может по своему усмотрению изменять конкретное содержание проводимых мероприятий в пределах, определенных рабочей программой учебной практики с учетом реального уровня знаний студентов и новых информационных материалов, представляющих ценность при решении отдельных задач практики.

Для более эффективного проведения практики рекомендуется предоставлять студентам раздаточный материал со всеми, необходимыми для эффективного решения поставленных задач графическими и методическими материалами. При возможности могут быть использованы мультимедийные приложения (презентации, фильмы и др.).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Помещения для выполнения индивидуальных заданий на практику.	Мебель: учебная мебель	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643;
Помещения для выполнения индивидуальных заданий на практику. Компьютерный класс.	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства: экран, проектор, компьютер	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ТОГБУ «Региональный информационно-технический центр»	г. Тамбов, ул. Советская, 118
2.	Межвидовой центр подготовки и боевого применения войск РЭБ (в/ч 61460)	г. Тамбов-6
3.	ФГУП Тамбовский завод «Октябрь»	г. Тамбов, ул. Бастионная, 1
4.	ТОГБУ «Медицинский информационно-аналитический центр»	г. Тамбов-4, д.20/1443

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	1 семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет;

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД7-(УК-3) Владеет первичными навыками органи-зации и руководства работой команды, выработки командной стратегии для достижения поставленной цели

Результаты обучения	Контрольные мероприятия
владение способностью понимать социальную значимость своей будущей профессии	Зач01

ИД7-(ОПК-2) Владеет навыками применения программных средств системного и прикладного назначений, в том числе отечественного производства для решения задач профессиональной деятельности

Результаты обучения	Контрольные мероприятия
владение первичными навыками поиска, изучения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности	Зач01

Вопросы к защите отчета по практике Зач01

1. Назовите федеральные законы РФ, регулирующие вопросы информационной безопасности.
2. Как Вы понимаете социальную значимость своей будущей профессии?
3. Какие морально-нравственные принципы и нормы профессиональной этики способствуют повышению информационной безопасности в организации?
4. Какие методы используются в организациях для повышения эффективности и качества работы сотрудников?
5. Как информационная безопасность способствует защите интересов личности, общества и государства?
6. Назовите известные Вам способы предупреждения и конструктивного разрешения конфликтных ситуаций в процессе профессиональной деятельности.
7. Приведите сравнительную характеристику известных Вам поисковых систем.
8. Опишите влияние формулировки поискового запроса на результаты поиска информации в компьютерных сетях.

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике, в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Оценка «неудовлетворительно» выставляется обучающемуся, если он не представил на защиту отчет по практике, в целом соответствующий установленным требованиям, либо при ответах на вопросы не дал удовлетворительных ответов.

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор ИАИТ

_____ Ю.Ю.Громов

«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.О.02.01(П) Научно-исследовательская работа

(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем

(шифр и наименование)

специализация

Безопасность открытых информационных систем

(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***

(наименование кафедры)

Составитель:

к.т.н.		И.С. Касатонов
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

		И.А. Дьяков
	подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Практика входит в состав обязательной части образовательной программы.

Таблица 1.1 - Результаты обучения по практике

Код, наименование индикатора	Результаты обучения по практике
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы её совершенствования на основе самооценки и самообразования в течение всей жизни	
ИД-4-(УК-6) Владеет первичными навыками определения и реализации приоритетов собственной деятельности и способами её совершенствования на основе самооценки и самообразования	Владеет способностью к самоорганизации и самообразованию
ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	
ИД4-(ОПК-8) Владеет навыками применения методов системного анализа для моделирования и исследования бизнес-процессов предметной области	Имеет опыт применения методов системного анализа в области защиты информации в автоматизированных системах

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Тип практики: научно-исследовательская работа
Способ проведения практики: стационарная; выездная.
Форма проведения практики: дискретно.

Объем практики составляет 3 зачетных единицы, продолжительность - 108 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	8 семестр
Контактная работа	**19**
консультации	18
промежуточная аттестация	1
Самостоятельная работа	**89**
Всего	**108**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить оргструктуру предприятия, технологию организации и выполнения НИР, основные параметры используемых аппаратно-программных средств и особенности технологического процесса на предприятии;
- применить методы научных исследований в профессиональной деятельности, в том числе в области защиты информации в автоматизированных системах;
- разработать и предложить современные способы защиты информации от негативных воздействий;
- приобрести опыт анализа информационных систем на предмет защиты информации, разработки способов обеспечения информационной безопасности.

Каждый обучающийся получает также индивидуальное задание, связанное с

- изучением заданного объекта информатизации на предмет угроз информационной безопасности и анализом уязвимостей автоматизированной информационной системы в аспекте выбранного направления научных исследований;
- измерением (экспериментальным исследованием) оценок уязвимостей автоматизированной информационной системы в аспекте выбранного направления научных исследований;
- систематизацией и обобщением полученных результатов с целью разработки обоснованных предложений (рекомендаций) по защите информации в рамках заданного объекта информатизации.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 544 c. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html

2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 c. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html

4.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

Базы данных Министерства экономического развития РФ http://www.economy.gov.ru

База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

Электронная база данных «Издательство Лань» https://e.lanbook.com

Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru

База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru

База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
3	4	5
Помещения для выполнения индивидуальных заданий на практику. Лаборатория 6С.	Мебель: Технические средства:	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643; MATLAB R2013b/ прикладное/ Лицензия №537913 бессрочная Договор №43759/VRN3 от 07.11.2013г./ключей 100 Пакет расширения MATLAB Simulink/ прикладное/ Лицензия №537913 бессрочная Договор №43759/VRN3 от 07.11.2013г./ключей 10 Astra Linux Special Edition/ базовое/ Лицензионный договор №РБТ-14/1640-01-ВУЗ/ключей 100 CodeGear RAD Studio 2007 Professional/ прикладное/ Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г./ ключей 30
Помещения для выполнения индивидуальных заданий на практику. Компьютерный класс.	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства: экран, проектор, компьютер	

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	8 семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет;

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД-4-(УК-6) Владеет первичными навыками определения и реализации приоритетов собственной деятельности и способами её совершенствования на основе самооценки и самообразования

Результаты обучения	Контрольные мероприятия
Владеет способностью к самоорганизации и самообразованию	Зач01

Вопросы к защите отчета по практике Зач01

1. Нормы профессиональной этики
2. Понятие и специфика профессиональной деятельности.

ИД4-(ОПК-8) Владеет навыками применения методов системного анализа для моделирования и исследования бизнес-процессов предметной области

Результаты обучения	Контрольные мероприятия
Имеет опыт применения методов системного анализа в области защиты информации в автоматизированных системах	Зач01

Вопросы к защите отчета по практике Зач01

1. Типовые теоретические методы научных исследований.
2. Основы методологии научных исследований.
3. Краткая характеристика элементов (структурных составляющих) методологии научных исследований.
4. Типовые методы системного анализа.
5. Особенности системного анализа в области защиты информации

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Результаты защиты отчета по практике оцениваются максимально 100 баллами.

Критерии оценивания на защите отчета по практике

Показатель	Количество баллов
Соблюдение рабочего графика (плана) проведения практики	5
Отзыв руководителя практики от профильной организации	10
Качество оформления отчета по практике	5
Полнота выполнения задания на практику	10
Качество ответов на вопросы на защите	70
Всего	100

Итоговая оценка выставляется с использованием следующей шкалы

Оценка	Набрано баллов
«отлично»	81-100
«хорошо»	61-80

«удовлетворительно»	41-60
«неудовлетворительно»	0-40

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор Института автоматики и информационных технологий

_____ Ю.Ю. Громов
«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.О.02.02(П) Технологическая практика
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование)

Специализация

Безопасность открытых информационных систем
(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***
(наименование кафедры)

Составитель:

к.т.н., доцент		А.В.Яковлев
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

	И.А. Дьяков
подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Дисциплина входит в состав обязательной части образовательной программы.

Таблица 1.1 - Результаты обучения по практике

ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	
ИД-6 (ОПК-5.1) Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах
	Владеет способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем
ОПК-5.2 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	
ИД-3 (ОПК-5.2) Владеет основами разработки и эксплуатации систем защиты информации открытых информационных систем	Владеет основами разработки проектных решений по защите информации в открытых информационных системах
	Владеет основами разработки эксплуатационной документации на системы защиты информации открытых информационных систем
ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	
ИД-3 (ОПК-5.3) Владеет способностью осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в от-	Владеет способностью осуществлять контроль обеспечения информационной безопасности открытых информационных систем

крытых информационных системах	Владеет способностью проводить верификацию данных в открытых информационных системах
ПК-6 Способен обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
ИД-4 (ПК-6) Владеет способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Владеет способностью обеспечить интенсификацию использования информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
	Владеет способностью обеспечить увеличение доли полезного машинного времени в общем бюджете времени работы ЭВМ автоматизированной системы с учетом требований информационной безопасности

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Тип практики: технологическая.
Способ проведения практики: стационарная; выездная.
Форма проведения практики: дискретно.

Объем практики составляет 6 зачетных единиц, продолжительность - 216 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	В семестр
Контактная работа	**37**
консультации	36
промежуточная аттестация	1
Самостоятельная работа	**179**
Всего	**216**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить оргструктуру предприятия, технологию производства, основные параметры оборудования, номенклатуру выпускаемой продукции, средства, меры и практики обеспечения информационной безопасности автоматизированной системы предприятия;
- приобрести первичный опыт обслуживания системы защиты информации в автоматизированной системе предприятия, обеспечения защиты информации в автоматизированной системе в процессе ее эксплуатации, внедрения системы защиты информации автоматизированной системы.

Каждый обучающийся получает также индивидуальное задание, связанное с:

- анализом угроз информационной безопасности и уязвимостей в автоматизированной системе предприятия;
- способностью разрабатывать и реализовывать политику информационной безопасности автоматизированной системы предприятия;
- разработкой проектных решений по защите информации в автоматизированной системе предприятия;
- разработкой эксплуатационной документации на систему защиты автоматизированной системы предприятия;
- осуществлением контроля обеспечения информационной безопасности автоматизированной системы предприятия;
- проведением верификации данных в автоматизированной системе предприятия;
- обеспечением интенсификации использования информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
- обеспечением увеличения доли полезного машинного времени в общем бюджете времени работы ЭВМ автоматизированной системы с учетом требований информационной безопасности.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/86938.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 c. — ISBN 978-5-7782-3918-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98708.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

4. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77317.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

5. Информационная безопасность : учебное пособие / Кирколуп сост., Е. М. Скурыдина. — Барнаул : Алтайский государственный педагогический университет, 2017. — 313 c. — ISBN 978-5-88210-898-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102889.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

6. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Новосибирск : Новосибирский государственный университет экономики и управления «НИНХ», 2018. — 84 c. — ISBN 978-5-7014-0841-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95200.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/95200

7. Грекул, В. И. Управление внедрением информационных систем : учебное пособие / В. И. Грекул, Г. Н. Денищенко, Н. Л. Коровкина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 277 c. — ISBN 978-5-4497-0910-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102073.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

8. Нестеров, С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 250 c. — ISBN 978-5-4497-0300-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89416.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

9. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95150.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

4.2 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

Базы данных Министерства экономического развития РФ http://www.economy.gov.ru

База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

Электронная база данных «Издательство Лань» https://e.lanbook.com

Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru

База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru

База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику (при необходимости), утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643;
Научно-исследовательская лаборатория «Безопасность открытых информационных систем»	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование.	
Компьютерный класс	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ГБУЗ «ТОДКБ»	392000, г. Тамбов, ул. Рылеева, д. 80
2.	ГБУЗ «ТОМИАЦ»	392004, г. Тамбов, ул. Тамбов-4, д. 20/144
3.	МКУ «РЦДО»	392008, г. Тамбов, ул. Советская, д. 182
4.	ООО «Максоком»	392000, г. Тамбов, ул. Державинская, д. 16, корпус А
5.	ООО «ПМК Бухгалтер»	392000, г. Тамбов, ул. Студенецкая набережная, д. 20
6.	ООО «Портал-68»	392000, г. Тамбов, ул. Коммунальная, д. 21а
7.	ООО «Русагро-Тамбов» филиал «Жердевский»	393671, Тамбовская обл., г. Жердевка, ул. Интернациональная, 1А
8.	ПАО «Пигмент»	392000, г. Тамбов, ул. Монтажников, д. 1
9.	ТОГБУ «Региональный информационно-технический центр»	392000, г. Тамбов, ул. Советская, д. 118
10.	ТОГБУЗ «ГКБ им. Арх. Луки г. Тамбова»	392000, г. Тамбов, ул. Гоголя, д. 6
11.	ТОГУП «Водгазхоз»	392000, г. Тамбов, ул. Студенецкая, д. 3

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	В семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД-6 (ОПК-5.1) Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

Результаты обучения	Контрольные мероприятия
Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах	Зач01
Владеет способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения доступности информации
2. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения целостности информации
3. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения конфиденциальности информации
4. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Ошибки при проектировании, разработке и эксплуатации программно-аппаратного обеспечения
5. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Преднамеренные действия по внесению уязвимостей в ходе проектирования, разработки и эксплуатации программно-аппаратного обеспечения
6. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Неправильные настройки оборудования и ПО
7. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Несанкционированное внедрения и использование неучтенных программ
8. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Внедрение вредоносных программ
9. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Несанкционированные неумышленные действия пользователей
10. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Сбои в работе оборудования и ПО
11. Разработка и реализация политики информационной безопасности открытых информационных систем. Общие требования по обеспечению информационной безопасности
12. Разработка и реализация политики информационной безопасности открытых информационных систем. Объекты, подлежащие защите
13. Разработка и реализация политики информационной безопасности открытых информационных систем. Основные принципы обеспечения информационной безопасности

14. Разработка и реализация политики информационной безопасности открытых информационных систем. Цели и задачи обеспечения информационной безопасности
15. Разработка и реализация политики информационной безопасности открытых информационных систем. Угрозы безопасности информации
16. Разработка и реализация политики информационной безопасности открытых информационных систем. Техническая политика в области обеспечения безопасности информации
17. Разработка и реализация политики информационной безопасности открытых информационных систем. Меры, методы и средства обеспечения безопасности информации

ИД-3 (ОПК-5.2) Владеет основами разработки и эксплуатации систем защиты информации открытых информационных систем

Результаты обучения	Контрольные мероприятия
Владеет основами разработки проектных решений по защите информации в открытых информационных системах	Зач01
Владеет основами разработки эксплуатационной документации на системы защиты информации открытых информационных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Проектирование системы защиты информации информационной системы
2. Разработка эксплуатационной документации на систему защиты информации открытой информационной системы
3. Макетирование и тестирование системы защиты информации открытой информационной системы
4. Описание структуры системы защиты информации открытой информационной системы
5. Описание состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств
6. Описание правил эксплуатации системы защиты информации открытой информационной системы

ИД-3 (ОПК-5.3) Владеет способностью осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Результаты обучения	Контрольные мероприятия
Владеет способностью осуществлять контроль обеспечения информационной безопасности открытых информационных систем	Зач01
Владеет способностью проводить верификацию данных в открытых информационных системах	Зач01

Вопросы к защите отчета по практике Зач01

1. Контроль использования в информационной системе технологий беспроводного доступа
2. Контроль использования в информационной системе мобильных технических средств
3. Контроль использования в информационной системе за запуском компонентов программного обеспечения
4. Контроль использования в информационной системе за установкой компонентов программного обеспечения
5. Контроль перемещения машинных носителей информации за пределы контролируемой зоны

6. Контроль использования интерфейсов ввода (вывода)
7. Контроль ввода (вывода) информации на машинные носители информации
8. Контроль подключения машинных носителей информации
9. Контроль уничтожения (стирания) информации с машинных носителей при их передаче между пользователями, в сторонние организации для ремонта или утилизации,
10. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации
11. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
12. Контроль состава технических средств, программного обеспечения и средств защиты информации
13. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
14. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
15. Контроль целостности информации, содержащейся в базах данных информационной системы
16. Контроль содержания информации, передаваемой из информационной системы и исключение неправомерной передачи информации из информационной системы
17. Верификация данных, вводимых в информационную систему
18. Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях
19. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
20. Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации
21. Контроль физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены
22. Контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами
23. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода
24. Контроль санкционированного и исключение несанкционированного использования технологий передачи речи
25. Контроль санкционированной и исключение несанкционированной передачи видеоинформации
26. Контроль целостности программного обеспечения, загружаемого и исполняемого с машинных носителей информации, доступных только для чтения

ИД-4 (ПК-6) Владеет способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

Результаты обучения	Контрольные мероприятия
Владеет способностью обеспечить интенсификацию использования информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Зач01
Владеет способностью обеспечить увеличение доли полезного машинного	Зач01

Результаты обучения	Контрольные мероприятия
времени в общем бюджете времени работы ЭВМ автоматизированной системы с учетом требований информационной безопасности	

Вопросы к защите отчета по практике Зач01

1. Эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
2. Эффективное использование информационно-технологических ресурсов на различных уровнях автоматизированной системы
3. Интенсификация использования информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
4. Использование по времени как критерий эффективности использования информационно-технологических ресурсов автоматизированной системы
5. Использование по мощности как критерий эффективности использования информационно-технологических ресурсов автоматизированной системы
6. Оптимизационные задачи использования информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
7. Обоснование варианта архитектуры автоматизированной системы на основе многокритериальной задачи принятия решений.
8. Структура машинного времени работы ЭВМ автоматизированной системы
9. Календарный фонд машинного времени работы ЭВМ автоматизированной системы
10. Режимный фонд машинного времени работы ЭВМ автоматизированной системы
11. Внережимный фонд машинного времени работы ЭВМ автоматизированной системы
12. Располагаемый фонд машинного времени работы ЭВМ автоматизированной системы
13. Резерв машинного времени работы ЭВМ автоматизированной системы
14. Производительный фонд машинного времени работы ЭВМ автоматизированной системы
15. Эффективный фонд машинного времени работы ЭВМ автоматизированной системы
16. Показатели эффективности использования машинного времени работы ЭВМ автоматизированной системы

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике, в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Оценка «неудовлетворительно» выставляется обучающемуся, если он не представил на защиту отчет по практике, в целом соответствующий установленным требованиям, либо при ответах на вопросы не дал удовлетворительных ответов.

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор Института автоматики и информационных технологий

_____ Ю.Ю. Громов
«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.О.02.03(П) Преддипломная практика
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование)

Специализация

Безопасность открытых информационных систем
(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***
(наименование кафедры)

Составитель:

к.т.н., доцент		А.В. Яковлев
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

	И.А. Дьяков
подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Дисциплина входит в состав обязательной части образовательной программы.

Таблица 1.1 - Результаты обучения по практике

Код, наименование индикатора	Результаты обучения по практике
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	
ИД-4 (ОПК-5) Владеет методами обеспечения информационной безопасности объектов информатизации	Владеет средствами обеспечения информационной безопасности объектов информатизации
	Владеет мерами обеспечения информационной безопасности объектов информатизации
	Владеет практиками обеспечения информационной безопасности объектов информатизации
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю	
ИД-4 (ОПК-6) Владеет первичными навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю	Владеет первичными навыками обслуживания систем защиты информации в автоматизированных системах
	Владеет первичными навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации
	Владеет первичными навыками внедрения систем защиты информации автоматизированных систем
ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	
ИД-5 (ОПК-8) Умеет применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Умеет применять методы эмпирического уровня при проведении разработок в области защиты информации в автоматизированных системах
	Умеет применять методы экспериментально-теоретического уровня при проведении разработок в области защиты информации в автоматизированных системах

	Умеет применять методы теоретического уровня при проведении разработок в области защиты информации в автоматизированных системах
ОПК-9 Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	
ИД-10 (ОПК-9) Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий
	Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития средств технической защиты информации
	Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации
ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	
ИД-6 (ОПК-5.1) Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах
	Владеет способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем
ОПК-5.2 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	
ИД-3 (ОПК-5.2) Владеет основами разработки и эксплуатации систем защиты информации открытых информационных систем	Владеет основами разработки проектных решений по защите информации в открытых информационных системах
	Владеет основами разработки эксплуатационной документации на системы защиты информации открытых информационных систем
ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	

ИД-3 (ОПК-5.3) Владеет способностью осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	Владеет способностью осуществлять контроль обеспечения информационной безопасности открытых информационных систем
	Владеет способностью проводить верификацию данных в открытых информационных системах

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Тип практики: преддипломная.
Способ проведения практики: стационарная; выездная.
Форма проведения практики: дискретно.

Объем практики составляет 15 зачетных единиц, продолжительность - 540 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	В семестр
Контактная работа	**91**
консультации	90
промежуточная аттестация	1
Самостоятельная работа	**449**
Всего	**540**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить оргструктуру предприятия, технологию производства, основные параметры оборудования, номенклатуру выпускаемой продукции, средства, меры и практики обеспечения информационной безопасности автоматизированной системы предприятия;
- приобрести первичный опыт обслуживания системы защиты информации в автоматизированной системе предприятия, обеспечения защиты информации в автоматизированной системе в процессе ее эксплуатации, внедрения системы защиты информации автоматизированной системы.

Каждый обучающийся получает также индивидуальное задание, связанное с:

- изучением методов научных исследований при проведении разработок в области защиты информации в автоматизированных системах;
- приобретением умения решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;
- анализом угроз информационной безопасности и уязвимостей в автоматизированной системе предприятия;
- способностью разрабатывать и реализовывать политику информационной безопасности автоматизированной системы предприятия;
- разработкой проектных решений по защите информации в автоматизированной системе предприятия;
- разработкой эксплуатационной документации на систему защиты автоматизированной системы предприятия;
- осуществлением контроля обеспечения информационной безопасности автоматизированной системы предприятия;
- проведением верификации данных в автоматизированной системе предприятия.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/86938.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 c. — ISBN 978-5-7782-3918-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98708.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

4. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77317.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

5. Информационная безопасность : учебное пособие / Кирколуп сост., Е. М. Скурыдина. — Барнаул : Алтайский государственный педагогический университет, 2017. — 313 c. — ISBN 978-5-88210-898-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102889.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

6. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Новосибирск : Новосибирский государственный университет экономики и управления «НИНХ», 2018. — 84 c. — ISBN 978-5-7014-0841-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95200.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/95200

7. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 c. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101992.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

8. Басыня, Е. А. Сетевая информационная безопасность и анонимизация : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2016. — 76 c. — ISBN 978-5-7782-3107-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/91519.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

9. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Ин-

формационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 c. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

4.2 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

Базы данных Министерства экономического развития РФ http://www.economy.gov.ru

База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

Электронная база данных «Издательство Лань» https://e.lanbook.com

Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru

База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru

База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику (при необходимости), утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643;
Научно-исследовательская лаборатория «Безопасность открытых информационных систем»	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование.	
Компьютерный класс	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ГБУЗ «ТОДКБ»	392000, г. Тамбов, ул. Рылеева, д. 80
2.	ГБУЗ «ТОМИАЦ»	392004, г. Тамбов, ул. Тамбов-4, д. 20/144
3.	МКУ «РЦДО»	392008, г. Тамбов, ул. Советская, д. 182
4.	ООО «Максоком»	392000, г. Тамбов, ул. Державинская, д. 16, корпус А
5.	ООО «ПМК Бухгалтер»	392000, г. Тамбов, ул. Студенецкая набережная, д. 20
6.	ООО «Портал-68»	392000, г. Тамбов, ул. Коммунальная, д. 21а
7.	ООО «Русагро-Тамбов» филиал «Жердевский»	393671, Тамбовская обл., г. Жердевка, ул. Интернациональная, 1А
8.	ПАО «Пигмент»	392000, г. Тамбов, ул. Монтажников, д. 1
9.	ТОГБУ «Региональный информационно-технический центр»	392000, г. Тамбов, ул. Советская, д. 118
10.	ТОГБУЗ «ГКБ им. Арх. Луки г. Тамбова»	392000, г. Тамбов, ул. Гоголя, д. 6
11.	ТОГУП «Водгазхоз»	392000, г. Тамбов, ул. Студенецкая, д. 3

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	В семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД-4 (ОПК-5) Владеет методами обеспечения информационной безопасности объектов информатизации

Результаты обучения	Контрольные мероприятия
Владеет средствами обеспечения информационной безопасности объектов информатизации	Зач01
Владеет мерами обеспечения информационной безопасности объектов информатизации	Зач01
Владеет практиками обеспечения информационной безопасности объектов информатизации	Зач01

Вопросы к защите отчета по практике Зач01

1. Физические средства обеспечения информационной безопасности объектов информатизации
2. Аппаратные средства обеспечения информационной безопасности объектов информатизации
3. Программные средства обеспечения информационной безопасности объектов информатизации
4. Организационные средства обеспечения информационной безопасности объектов информатизации
5. Правовые средства обеспечения информационной безопасности объектов информатизации
6. Морально-этические средства обеспечения информационной безопасности объектов информатизации
7. Меры обеспечения информационной безопасности объектов информатизации. Защита информации от случайных воздействий
8. Меры обеспечения информационной безопасности объектов информатизации. Защита информации от преднамеренных воздействий
9. Меры обеспечения информационной безопасности объектов информатизации. Защита компьютерной информации от копирования
10. Меры обеспечения информационной безопасности объектов информатизации. Защита информации от вредоносных программных средств
11. Практики обеспечения информационной безопасности объектов информатизации

ИД-4 (ОПК-6) Владеет первичными навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю

Результаты обучения	Контрольные мероприятия
Владеет первичными навыками обслуживания систем защиты информации в автоматизированных системах	Зач01
Владеет первичными навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации	Зач01
Владеет первичными навыками внедрения систем защиты информации автоматизированных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем
2. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем
3. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем
4. Диагностика систем защиты информации автоматизированных систем
5. Администрирование систем защиты информации автоматизированных систем
6. Управление защитой информации в автоматизированных системах
7. Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
8. Мониторинг защищенности информации в автоматизированных системах
9. Аудит защищенности информации в автоматизированных системах
10. Установка и настройка средств защиты информации в автоматизированных системах
11. Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
12. Анализ уязвимостей внедряемой системы защиты информации
13. Внедрение организационных мер по защите информации в автоматизированных системах
14. Тестирование систем защиты информации автоматизированных систем

ИД-5 (ОПК-8) Умеет применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах

Результаты обучения	Контрольные мероприятия
Умеет применять методы эмпирического уровня при проведении разработок в области защиты информации в автоматизированных системах	Зач01
Умеет применять методы экспериментально-теоретического уровня при проведении разработок в области защиты информации в автоматизированных системах	Зач01
Умеет применять методы теоретического уровня при проведении разработок в области защиты информации в автоматизированных системах	Зач01

Вопросы к защите отчета по практике Зач01

1. Методы эмпирического уровня. Наблюдение
2. Методы эмпирического уровня. Описание
3. Методы эмпирического уровня. Измерение
4. Методы эмпирического уровня. Эксперимент
5. Методы эмпирического уровня. Сравнение
6. Методы экспериментально-теоретического уровня. Эксперимент
7. Методы экспериментально-теоретического уровня. Анализ и синтез
8. Методы экспериментально-теоретического уровня. Индукция и дедукция
9. Методы экспериментально-теоретического уровня. Моделирование
10. Методы экспериментально-теоретического уровня. Гипотетический метод
11. Методы экспериментально-теоретического уровня. Логический метод
12. Методы теоретического уровня. Формализация
13. Методы теоретического уровня. Аксиоматизация
14. Методы теоретического уровня. Гипотетико-дедуктивный метод

ИД-10 (ОПК-9) Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Результаты обучения	Контрольные мероприятия
Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий	Зач01
Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития средств технической защиты информации	Зач01
Умеет решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации	Зач01

Вопросы к защите отчета по практике Зач01

1. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Антивирусы
2. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Межсетевые экраны
3. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Авторизация и разграничение доступа
4. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Системы обнаружения и предотвращения атак
5. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Сканеры безопасности
6. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий. Системы контроля содержимого и антиспама
7. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития средств технической защиты информации. Механические средства
8. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития средств технической защиты информации. Электромеханические средства
9. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития средств технической защиты информации. Электронные средства
10. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Адресация, протоколы, порты
11. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Статическая маршрутизация
12. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Универсальный идентификатор ресурсов
13. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Служба FTP, протокол FTP, протокол TFTP
14. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Служба WWW, протокол HTTP

15. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Служба DNS
16. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Служба Telnet, служба SSH, протокол SSH
17. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Регистратуры InterNet, автономные системы, обратные домены, служба Whois
18. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Электронная почта, формат сообщения, протокол SMTP
19. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Электронная почта, протоколы POP3 и IMAP4
20. Решение задач профессиональной деятельности с учётом текущего состояния и тенденций развития сетей и систем передачи информации. Динамическая маршрутизация, протоколы RIP и OSPF

ИД-6 (ОПК-5.1) Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

Результаты обучения	Контрольные мероприятия
Владеет навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах	Зач01
Владеет способностью разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения доступности информации
2. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения целостности информации
3. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Угрозы нарушения конфиденциальности информации
4. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Ошибки при проектировании, разработке и эксплуатации программно-аппаратного обеспечения
5. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Преднамеренные действия по внесению уязвимостей в ходе проектирования, разработки и эксплуатации программно-аппаратного обеспечения
6. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Неправильные настройки оборудования и ПО
7. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Несанкционированное внедрения и использование неучтенных программ
8. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Внедрение вредоносных программ
9. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Несанкционированные неумышленные действия пользователей

10. Анализ угроз информационной безопасности и уязвимостей в открытых информационных системах. Сбои в работе оборудования и ПО
11. Разработка и реализация политики информационной безопасности открытых информационных систем. Общие требования по обеспечению информационной безопасности
12. Разработка и реализация политики информационной безопасности открытых информационных систем. Объекты, подлежащие защите
13. Разработка и реализация политики информационной безопасности открытых информационных систем. Основные принципы обеспечения информационной безопасности
14. Разработка и реализация политики информационной безопасности открытых информационных систем. Цели и задачи обеспечения информационной безопасности
15. Разработка и реализация политики информационной безопасности открытых информационных систем. Угрозы безопасности информации
16. Разработка и реализация политики информационной безопасности открытых информационных систем. Техническая политика в области обеспечения безопасности информации
17. Разработка и реализация политики информационной безопасности открытых информационных систем. Меры, методы и средства обеспечения безопасности информации

ИД-3 (ОПК-5.2) Владеет основами разработки и эксплуатации систем защиты информации открытых информационных систем

Результаты обучения	Контрольные мероприятия
Владеет основами разработки проектных решений по защите информации в открытых информационных системах	Зач01
Владеет основами разработки эксплуатационной документации на системы защиты информации открытых информационных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Проектирование системы защиты информации информационной системы
2. Разработка эксплуатационной документации на систему защиты информации открытой информационной системы
3. Макетирование и тестирование системы защиты информации открытой информационной системы
4. Описание структуры системы защиты информации открытой информационной системы
5. Описание состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств
6. Описание правил эксплуатации системы защиты информации открытой информационной системы

ИД-3 (ОПК-5.3) Владеет способностью осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Результаты обучения	Контрольные мероприятия
Владеет способностью осуществлять контроль обеспечения информационной безопасности открытых информационных систем	Зач01
Владеет способностью проводить верификацию данных в открытых информационных системах	Зач01

Вопросы к защите отчета по практике Зач01

1. Контроль использования в информационной системе технологий беспроводного доступа
2. Контроль использования в информационной системе мобильных технических средств
3. Контроль использования в информационной системе за запуском компонентов программного обеспечения
4. Контроль использования в информационной системе за установкой компонентов программного обеспечения
5. Контроль перемещения машинных носителей информации за пределы контролируемой зоны
6. Контроль использования интерфейсов ввода (вывода)
7. Контроль ввода (вывода) информации на машинные носители информации
8. Контроль подключения машинных носителей информации
9. Контроль уничтожения (стирания) информации с машинных носителей при их передаче между пользователями, в сторонние организации для ремонта или утилизации,
10. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации
11. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
12. Контроль состава технических средств, программного обеспечения и средств защиты информации
13. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
14. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
15. Контроль целостности информации, содержащейся в базах данных информационной системы
16. Контроль содержания информации, передаваемой из информационной системы и исключение неправомерной передачи информации из информационной системы
17. Верификация данных, вводимых в информационную систему
18. Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях
19. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
20. Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации
21. Контроль физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены
22. Контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами
23. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода
24. Контроль санкционированного и исключение несанкционированного использования технологий передачи речи
25. Контроль санкционированной и исключение несанкционированной передачи видеоинформации

26. Контроль целостности программного обеспечения, загружаемого и исполняемого с машинных носителей информации, доступных только для чтения

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике, в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Оценка «неудовлетворительно» выставляется обучающемуся, если он не представил на защиту отчет по практике, в целом соответствующий установленным требованиям, либо при ответах на вопросы не дал удовлетворительных ответов.

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор института Автоматики и информационных технологий

_____ Ю.Ю. Громов
«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.В.01.01(У) Учебно-лабораторный практикум
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование)

Специализация

Безопасность открытых информационных систем
(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***
(наименование кафедры)

Составитель:

		Ю.В. Кулаков
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

	И.А. Дьяков
подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Практика входит в состав части образовательной программы, формируемой участниками образовательных отношений.

Таблица 1.1 - Результаты обучения по практике

Код, наименование индикатора	Результаты обучения по практике
ПК-5 Способен проводить контроль защищённости информации от утечки по техническим каналам и от несанкционированного доступа	
ИДЗ-(ПК-5) Владеет основами проведения экспериментально-исследовательских работ с использованием современных программно-технических комплексов измерения параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации	Применяет на практике современные программно-технические комплексы измерения параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации
	Анализирует результаты проведения экспериментально-исследовательских работ по измерению параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная.
Тип практики: учебно-лабораторный практикум.
Способ проведения практики: стационарная.
Форма проведения практики: дискретно.

Объем практики составляет 3 зачетных единицы, продолжительность - 108 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	6 семестр
Контактная работа	**19**
консультации	18
промежуточная аттестация	1
Самостоятельная работа	**89**
Всего	**108**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить особенности проведения экспериментально-исследовательских работ по измерению параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации;
- ознакомиться с документами по организации специальных исследований, современными программно-аппаратными комплексами проведения экспериментально-исследовательских работ по измерению параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации;
- приобрести опыт самоорганизации и самообразования; работы в коллективе; поиска информации в компьютерных системах, сетях, библиотечных фондах; оформления отчётов о научных исследованиях; освоения новых образцов программных, технических средств и информационных технологий; поиска, изучения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.

Каждый обучающийся получает также индивидуальное задание, связанное с:

- изучением и практическим освоением современных программно-аппаратных комплексов проведения экспериментально-исследовательских работ по измерению параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации;
- поиском информации в компьютерных системах, сетях, библиотечных фондах;
- систематизацией и обобщением научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин– Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 702 с. – Режим доступа: http://www.iprbookshop.ru/63594.html. – ЭБС «IPRbooks».

2. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ В.И. Васильев–Электрон. текстовые данные. –М.: Машиностроение, 2013. – 172 с. – Режим доступа: http://www.iprbookshop.ru/18519.html. – ЭБС «IPRbooks».

3. Паршин, К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс]: учебное пособие/ К.А. Паршин– Электрон. текстовые данные. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015. – 96 с. – Режим доступа: http://www.iprbookshop.ru/45291.html. – ЭБС «IPRbooks»

4.2 Периодическая литература

1. Журнал «Вопросы защиты информации». Способ доступа к архиву изданий: http://izdat.ntckompas.ru/editions/for_readers/archive/?SECTION_ID=155
2. Журнал «Проблемы информационной безопасности. Компьютерные системы» Способ доступа к архиву изданий: http://jisp.ru/o-zhurnale/arxiv-nomerov/
3. Журнал «Информация и безопасность». Способ доступа к архиву изданий: http://kafedrasib.ru/index.php/informatsiya-bezopasnost/arkhiv-vypuskov

4.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru
Справочно-правовая система «Консультант+» http://www.consultant-urist.ru
Справочно-правовая система «Гарант» http://www.garant.ru
База данных Web of Science https://apps.webofknowledge.com/
База данных Scopus https://www.scopus.com
Портал открытых данных Российской Федерации https://data.gov.ru
База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata
База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/
База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
Базы данных Министерства экономического развития РФ http://www.economy.gov.ru
База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata
Электронная база данных «Издательство Лань» https://e.lanbook.com
Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru
База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru
База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Наряду с решением основных задач, в процессе проведения учебной практики желательно ознакомить студентов с историей развития информационных технологий, базовыми информационными технологиями и их местом в системах автоматизированного управления.

Основными мероприятиями учебной практики являются:

– ознакомление с информационной системой и подсистемой информационной безопасности предприятий (организаций, учреждений) г. Тамбова;

– ознакомление с особенностями работы и функциональными обязанностями должностных лиц по обеспечению информационной безопасности;

– ознакомление с современными техническими, программными и аппаратными средствами обеспечения информационной безопасности;

– ознакомление с современными методами обеспечения совместимости, переносимости и масштабируемости информационных систем;

– ознакомление с технологиями и средствами обеспечения защищённого электронного документооборота;

– изучение документации по организационному обеспечению информационной безопасности;

– изучение документов по правовому обеспечению информационной безопасности;

– личное участие в подготовке сообщений и разработке презентаций на заданные темы;

– личное участие в разработке простейших программ для ЭВМ.

В процессе учебной практики возможно использование следующих технологий образовательного процесса:

1. Технология презентации знаний (основана на поведении преподавателя, в которой преобладает приоритет и опора на методические приёмы преподнесения знаний).

2. Технократическая технология (приоритет отдается использованию технических средств, особенно персонального компьютера). Система формализации знаний, запрограммированных форм и методов проведения занятий, жесткого регламента.

3. Технология адаптивного типа (предполагает регулярную корректировку форм занятий и стилей обучения).

4. Технология социально-психологического типа (использование социально-психологических характеристик восприятия личностью и группой определенного объема знаний и методов обучения, восприятия преподавателя студентами и т.д.).

5. Технология креативного обучения (используется творческий потенциал личности, способность к творчеству, к неординарному восприятию материала и т.д.). Основное– постановка проблем, обсуждение их содержания.

6. Технология самообразования (самостоятельное освоение отдельных вопросов, роль руководителя – консультационная).

Руководитель практики может по своему усмотрению изменять конкретное содержание проводимых мероприятий в пределах, определенных рабочей программой учебной практики с учетом реального уровня знаний студентов и новых информационных материалов, представляющих ценность при решении отдельных задач практики.

Для более эффективного проведения практики рекомендуется предоставлять студентам раздаточный материал со всеми, необходимыми для эффективного решения поставленных задач графическими и методическими материалами. При возможности могут быть использованы мультимедийные приложения (презентации, фильмы и др.).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Помещения для выполнения индивидуальных заданий на практику.	Мебель: учебная мебель	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643;
Помещения для выполнения индивидуальных заданий на практику. Компьютерный класс.	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства: экран, проектор, компьютер	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ТОГБУ «Региональный информационно-технический центр»	г. Тамбов, ул. Советская, 118
2.	Межвидовой центр подготовки и боевого применения войск РЭБ (в/ч 61460)	г. Тамбов-6
3.	ФГУП Тамбовский завод «Октябрь»	г. Тамбов, ул. Бастионная, 1
4.	ТОГБУЗ «Медицинский информационно-аналитический центр»	г. Тамбов-4, д.20/1443
5.	Региональный учебно-научный центр по вопросам информационной безопасности	г. Тамбов, Советская, 106

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	6 семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет;

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД3-(ПК-5) Владеет основами проведения экспериментально-исследовательских работ с использованием современных программно-технических комплексов измерения параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации

Результаты обучения	Контрольные мероприятия
Применяет на практике современные программно-технические комплексы измерения параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации	Зач01
Анализирует результаты проведения экспериментально-исследовательских работ по измерению параметров технических каналов утечки информации и локализации технических средств образования каналов утечки информации	Зач01

Вопросы к защите отчета по практике Зач01

1. Назовите современные программно-технические комплексы измерения параметров технических каналов утечки информации. локализации технических средств образования каналов утечки информации и их возможности.
2. Назовите современные программно-технические комплексы локализации технических средств образования каналов утечки информации и их возможности.
3. Преднезначение и возможности нелинейных локаторов.
4. Преднезначение и возможности индикаторов поля.
5. Предназначение и возможности поисковых приёмников.

Практические задания к защите отчёта по практике Зач01

1. Подготовить к работе ПАК «Сигурд» и измерить уровень побочных электромагнитных излучений тестового компьютера.
2. Подготовить к работе ПАК «Трап» и измерить разборчивость речи на границе контролируемой зоны выделенного помещения.
3. Подготовить к работе нелинейный локатор «Катран» и локализовать местоположение закладного устройства.
4. Подготовить к работе ПАК «RS Digital Mobile» и локализовать местоположение радиомикрофона.

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, дал исчерпывающие ответы на заданные вопросы и правильно выполнил практическое задание.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и уверенно отве-

чал на заданные вопросы и выполнил практическое задание, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике, в целом соответствующий установленным требованиям, при ответах на некоторые вопросы и выполнении практического задания допускал существенные ошибки.

Оценка «неудовлетворительно» выставляется обучающемуся, если он не представил на защиту отчет по практике, в целом соответствующий установленным требованиям, либо при ответах на вопросы не дал удовлетворительных ответов, либо не смог выполнить практическое задание.

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

УТВЕРЖДАЮ

Директор Института автоматики и информационных технологий

_____ Ю.Ю. Громов
«_13_» _____*февраля*_____ 20_25_ г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.В.02.01(П) Проектно-технологическая практика
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование)

специализация

Безопасность открытых информационных систем
(наименование профиля образовательной программы)

Формы обучения: ***очная***

Кафедра: ***Информационные системы и защита информации***
(наименование кафедры)

Составитель:

к.т.н., доцент		А.И. Елисеев
степень, должность	подпись	инициалы, фамилия

Заведующий кафедрой

		И.А. Дьяков
	подпись	инициалы, фамилия

Тамбов 2025

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

Цель прохождения практики – достижение планируемых результатов обучения (таблица 1.1), соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Практика входит в состав части образовательной программы, формируемой участниками образовательных отношений.

Таблица 1.1 - Результаты обучения по практике

Код, наименование индикатора	Результаты обучения по практике
ПК-4 Способен участвовать в разработке и проектировании программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированной системы	
ИД5-(ПК-4) Владеет способностью участвовать в разработке и проектировании программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированной системы	Владеет способностью участвовать в разработке проектных решений программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированной системы
	Владеет способностью участвовать в разработке эксплуатационной документации на программно-аппаратные и технические (в том числе криптографические) средства защиты информации автоматизированной системы
	Владеет способностью участвовать в разработке программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированных систем
	Владеет способностью тестировать программно-аппаратные и технические (в том числе криптографических) средства защиты информации автоматизированных систем

Результаты обучения по практике достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ВИД, ТИП, ОБЪЁМ ПРАКТИКИ, СПОСОБ И ФОРМА ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Тип практики: проектно-технологическая практика.
Способ проведения практики: стационарная; выездная.
Форма проведения практики: дискретно.

Объем практики составляет 3 зачетные единицы, продолжительность – 108 часов.

Ниже приведено распределение общего объема практики (в академических часах в соответствии с утвержденным учебным планом).

Виды работ	Форма обучения
	Очная
	4 семестр
Контактная работа	**19**
консультации	18
промежуточная аттестация	1
Самостоятельная работа	**89**
Всего	**108**

3. СОДЕРЖАНИЕ ПРАКТИКИ

В ходе практики обучающиеся должны:

- пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда;
- ознакомиться с правилами внутреннего трудового распорядка организации, на базе которой обучающийся проходит практику;
- изучить оргструктуру предприятия, системы, средства, меры и практики обеспечения информационной безопасности автоматизированной системы предприятия;
- приобрести первичный опыт тестирование систем защиты информации автоматизированных систем, разработки проектных решений по защите информации в автоматизированных системах, разработки эксплуатационной документации на системы защиты информации автоматизированных систем, разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.

Каждый обучающийся получает также индивидуальное задание, связанное с:

- проведением анализа программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;
- выявлением основных угроз безопасности информации в автоматизированных системах;
- систематизацией научно-технической информации в области современных информационных технологий и обеспечения защиты информации;
- разработкой моделей автоматизированных систем и подсистем безопасности автоматизированных систем;
- разработкой предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах;
- формированием требований по защите информации, включая использование математического аппарата для решения прикладных задач;
- проектированием, моделированием, исследованием автоматизированных систем и подсистем информационной безопасности автоматизированных систем;
- разработкой модели автоматизированных систем и систем защиты информации автоматизированных систем;
- разработкой и документированием программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации;
- проведением комплексного тестирования аппаратных и программных средств.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1 Учебная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/86938.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 c. — ISBN 978-5-7782-3918-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98708.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

4. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77317.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

5. Информационная безопасность : учебное пособие / Кирколуп сост., Е. М. Скурыдина. — Барнаул : Алтайский государственный педагогический университет, 2017. — 313 c. — ISBN 978-5-88210-898-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102889.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей

6. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Новосибирск : Новосибирский государственный университет экономики и управления «НИНХ», 2018. — 84 c. — ISBN 978-5-7014-0841-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95200.html (дата обращения: 18.05.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/95200

7. Грекул, В. И. Управление внедрением информационных систем : учебное пособие / В. И. Грекул, Г. Н. Денищенко, Н. Л. Коровкина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 277 c. — ISBN 978-5-4497-0910-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102073.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

8. Нестеров, С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 250 c. — ISBN 978-5-4497-0300-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89416.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

9. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва: Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95150.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей

4.2 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

Базы данных Министерства экономического развития РФ http://www.economy.gov.ru

База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

Электронная база данных «Издательство Лань» https://e.lanbook.com

Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru

База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru

База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Ресурсы электронной информационно-образовательной среды университета представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде Тамбовского государственного технического университета».

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте университета в разделе «Университет»-«Сведения об образовательной организации»-«Материально-техническое обеспечение и оснащенность образовательного процесса».

Сведения о лицензионном программном обеспечении, используемом в образовательном процессе, представлены на официальном сайте университета в разделе «Образование»-«Учебная работа»-«Доступное программное обеспечение».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

В первый день практики руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику (при необходимости), утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблоном отчета по практике, принять задание на практику к исполнению.

В первый день практики обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности профильной организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- выполнить индивидуальное задание;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений для прохождения практики	Оснащенность специальных помещений для прохождения практики	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	MS Office, Windows / Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643;
Научно-исследовательская лаборатория «Безопасность открытых информационных систем»	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование.	
Компьютерный класс	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ГБУЗ «ТОДКБ»	392000, г. Тамбов, ул. Рылеева, д. 80
2.	ГБУЗ «ТОМИАЦ»	392004, г. Тамбов, ул. Тамбов-4, д. 20/144
3.	МКУ «РЦДО»	392008, г. Тамбов, ул. Советская, д. 182
4.	ООО «Максоком»	392000, г. Тамбов, ул. Державинская, д. 16, корпус А
5.	ООО «ПМК Бухгалтер»	392000, г. Тамбов, ул. Студенецкая набережная, д. 20
6.	ООО «Портал-68»	392000, г. Тамбов, ул. Коммунальная, д. 21а
7.	ООО «Русагро-Тамбов» филиал «Жердевский»	393671, Тамбовская обл., г. Жердевка, ул. Интернациональная, 1А
8.	ПАО «Пигмент»	392000, г. Тамбов, ул. Монтажников, д. 1
9.	ТОГБУ «Региональный информационно-технический центр»	392000, г. Тамбов, ул. Советская, д. 118
10.	ТОГБУЗ «ГКБ им. Арх. Луки г. Тамбова»	392000, г. Тамбов, ул. Гоголя, д. 6
11.	ТОГУП «Водгазхоз»	392000, г. Тамбов, ул. Студенецкая, д. 3

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Зач01	Зачет с оценкой	4 семестр

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику, включающее рабочий график (план) проведения практики, индивидуальное задание, планируемые результаты практики;
- отзыв руководителя практики от профильной организации о работе обучающегося в период прохождения практики;
- дневник практики;
- аннотированный отчет.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по практике и индикаторами достижения компетенций.

ИД5-(ПК-4) Владеет способностью участвовать в разработке и проектировании программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированной системы

Результаты обучения	Контрольные мероприятия
Владеет способностью участвовать в разработке проектных решений программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированной системы	Зач01
Владеет способностью участвовать в разработке эксплуатационной документации на программно-аппаратные и технические (в том числе криптографические) средства защиты информации автоматизированной системы	Зач01
Владеет способностью участвовать в разработке программно-аппаратных и технических (в том числе криптографических) средств защиты информации автоматизированных систем	Зач01
Владеет способностью тестировать программно-аппаратные и технические (в том числе криптографических) средства защиты информации автоматизированных систем	Зач01

Вопросы к защите отчета по практике Зач01

1. Хеш-функция. Свойства криптографических хеш-функций.
2. Выбор криптографической хеш-функции. Безопасные и небезопасные хеш-функции.
3. Реализация криптографического хеширования в Python.
4. Функции для вычисления контрольной суммы в Python.
5. Аутентификация данных. Генерация ключей. Хеширование с ключом.
6. Функции HMAC в Python. Аутентификация данных между сторонами.
7. Атаки по времени.
8. Симметричное шифрование. Блочные шифры. Потоковые шифры. Режимы шифрования.
9. Проблема распределения ключей. Асимметричное шифрование.
10. Асимметричное шифрование. Шифрование с открытым ключом RSA.
11. Асимметричное шифрование. Обеспечение неотказуемости.
12. Цифровые подписи. Цифровые подписи RSA. Проверка цифровой подписи RSA. Реализация цифровой подписи в Python.
13. Безопасность транспортного уровня. Протоколы SSL, TLS.
14. Атака «человек посередине» на протоколы SSL, TLS.
15. Рукопожатие TLS. Согласование набора шифров. Обмен ключами. Аутентификация сервера.
16. Использование протокола HTTPS в Django с сервером Gunicorn. Самоподписанные сертификаты открытого ключа.
17. Использование TLS для пакетов запросов, соединения с базами данных, отправки электронной почты.
18. Сеансы HTTP. HTTP cookies.
19. Сохранение состояния сеанса. Сериализатор сессий на Python. Простые сеансы на основе кеша в Django.

20. Сеансы на основе кеша с возможностью записи в Django. Механизм сеанса на основе базы данных в Django.
21. Механизм сессий на основе файлов в Django. Механизм сеансов на основе куки-файлов.
22. Хранение паролей в веб-приложениях. «Соленое» хеширование. Функции извлечения ключей.
23. Авторизация на уровне приложения. Управление разрешениями.
24. Стандарт OAuth 2. Типы разрешений. Процесс авторизации.
25. Реализация OAuth в Django. Задачи сервера авторизации. Задачи сервера ресурсов.
26. Атаки межсайтового скриптинга. Постоянные XSS. Отраженные XSS. XSS на основе DOM.
27. Валидация пользовательских данных. Валидация форм в Django.
28. Экранирование вывода. Встроенные в Django утилиты рендеринга.
29. Заголовки HTTP-ответов. Заголовок X-XSS-Protection.
30. Политика безопасности контента. Составление политики безопасности контента в Django.
31. Развертывание политики с помощью django-csp. Индивидуализированные политики. Сообщение о нарушениях CSP.
32. Подделка межсайтовых запросов. Управление идентификатором сеанса.
33. Соглашения по управлению состояниями. Проверка методов HTTP.
34. Проверка заголовка реферера. Заголовок ответа Referrer-Policy.
35. Межсайтовая подделка запроса. Токены CSRF. POST-запросы. Небезопасные методы запроса.
36. Cross-origin resource sharing (CORS). Простые CORS-запросы.
37. Проверка CORS с помощью django-cors-headers. Настройка политики Access-Control-Allow-Origin.
38. Предварительная проверка запросов CORS. Противодействие CORS и CSRF.

8.2. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме зачета с оценкой используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике, полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике, в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Оценка «неудовлетворительно» выставляется обучающемуся, если он не представил на защиту отчет по практике, в целом соответствующий установленным требованиям, либо при ответах на вопросы не дал удовлетворительных ответов.

Результат обучения по практике считается достигнутым при получении обучающимся оценки «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.