МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

Рассмотрена и утверждена на заседании ученого совета факультета от ___.___.20____ протокол №

УТВЕРЖДАЮ
Декан факультета ФИТКБ
_____/Бредихин А.В./
28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Научно-исследовательская работа»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы _____ А.С. Пахомова
Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко
Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

1.1. Цели практики способствовать формированию и развитию у студентов знаний о сущности и специфике научно-исследовательской деятельности как неотъемлемой части профессиональной компетентности будущего специалиста в области информационной безопасности телекоммуникационных систем.

1.2. Задачи прохождения практики

– дать навыки выполнения научно-исследовательской работы и развить умения: – создание благоприятных условий для формирования высокопрофессиональной и творчески активной личности будущего специалиста;

– обеспечение интеграции учебных занятий и научно-исследовательской работы студентов; – повышение массовости и эффективности участия студентов в научно-исследовательских работах студента (НИРС) путем привлечения их к исследованиям по наиболее значимым направлениям в юриспруденции; – вести библиографическую работу с привлечением современных информационных технологий;

– формулировать и разрешать задачи, возникающие в ходе выполнения научно-исследовательской работы; – выбирать необходимые методы исследования (модифицировать существующие, разрабатывать новые методы), исходя из задач конкретного исследования; – применять современные информационные технологии при проведении научных исследований;

– обрабатывать полученные результаты, анализировать и представлять их в виде законченных научно-исследовательских разработок (отчета по научно-исследовательской работе, тезисов докладов, научной статьи);

– обрабатывать полученные результаты, анализировать и представлять их в виде законченных научно-исследовательских разработок (отчета по научно-исследовательской работе, тезисов докладов, научной статьи); – оформлять результаты проделанной работы в соответствии с требованиями нормативных документов регуляторов в сфере информационной безопасности.

2. ХАРАКТЕРИСТИКА ПРАКТИКИ

Вид практики – Производственная практика

Тип практика – Научно-исследовательская работа

Форма проведения практики – дискретно

Способ проведения практики – стационарная, выездная.

Стационарная практика проводится в профильных организациях, расположенной на территории г. Воронежа.

Выездная практика проводится в местах проведения практик, расположенных вне г. Воронежа.

Способ проведения практики определяется индивидуально для каждого студента и указывается в приказе на практику.

Место проведения практики – перечень объектов для прохождения практики устанавливается на основе типовых двусторонних договоров между предприятиями (организациями) и ВУЗом или ВУЗ.

3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Практика «Научно-исследовательская работа» относится к части, формируемой участниками образовательных отношений блока Б2.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс прохождения практики «Научно-исследовательская работа» направлен на формирование следующих компетенций:

ПК-9.2 - Способен разрабатывать средства защиты СССЭ (за исключением сетей связи специального назначения) от НД и компьютерных атак

ПК-9.5 - Способен управлять рисками систем защиты сетей электросвязи от НД, проведении НИОКР в сфере разработки средств и систем защиты СССЭ от НД, создания ЗТКС

ПК-9.6 - Способен использовать методы искусственного интеллекта в последующей профессиональной деятельности в качестве научных сотрудников, преподавателей образовательных организаций высшего образования, инженеров, технологов

ПК-9.7 - Способен выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности в области моделирования и анализа сложных естественных и искусственных систем

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ПК-9.2	**Знать**: архитектуру современных систем и средств защиты информации, принципы построения межсетевых экранов, СОВ, обнаружения вторжений и криптографической защиты каналов. **Уметь**: проектировать и реализовывать защитные механизмы, способные отражать целенаправленные компьютерные атаки и блокировать несанкционированный доступ. **Владеть**: навыками проектирования и реализации адаптивных систем защиты информации, обладающих высокой устойчивостью к целевым атакам, способностью к динамическому реконфигурированию политик безопасности и сохранению функциональности в условиях интенсивного враждебного воздействия..

ПК-9.5	**Знать**: жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ. **Уметь**: выстраивать баланс между уровнем защиты и производительностью сети, прогнозировать эволюцию угроз и заранее закладывать контрмеры в новые разработки. **Владеть**: методологией управления рисками на всех этапах жизненного цикла систем защиты СССЭ и ЗТКС, включая прогнозирование эволюции векторов угроз, интеграцию контрмер на стадии НИОКР и обеспечение требуемого уровня остаточного риска при заданных эксплуатационных характеристиках.
ПК-9.6	**Знать**: современные подходы машинного обучения, нейронные сети, системы обнаружения аномалий и генеративные модели applied к безопасности. **Уметь**: обучать модели распознавать новые виды атак, автоматизировать реагирование и усиливать традиционные средства защиты интеллектом. **Владеть**: практическими методами применения технологий машинного обучения и искусственного интеллекта для обнаружения аномалий, классификации атак неизвестных классов, автоматизации реагирования и интеллектуального усиления традиционных средств защиты информации.
ПК-9.7	**Знать**: математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях. **Уметь**: видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели. **Владеть**: методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.

5. ОБЪЕМ ПРАКТИКИ

Общий объем практики составляет составляет 3 з.е., ее продолжительность – 2 недели.

Форма промежуточной аттестации: зачет с оценкой.

6. СОДЕРЖАНИЕ ПРАКТИКИ

6.1 Содержание разделов практики и распределение трудоемкости

по этапам

№ п/п	Наименование этапа	Содержание этапа	Трудоемкость, час
1	Подготовительный этап	Проведение собрания по организации практики. Знакомство с целями, задачами, требованиями к практике и формой отчетности. Распределение заданий. Инструктаж по охране труда и пожарной безопасности.	*2*
2	Знакомство с ведущей организацией	Изучение организационной структуры организации. Изучение нормативно-технической документации.	*10*
3	Практическая работа	Выполнение индивидуальных заданий. Сбор практического материала.	*84*
4	Подготовка отчета	Обработка материалов практики, подбор и структурирование материала для раскрытия соответствующих тем для отчета. Оформление отчета. Предоставление отчета руководителю.	*10*
5	Защита отчета		*2*
		Итого	*108*

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

7.1 Подготовка отчета о прохождении практики

Аттестация по итогам практики проводится в виде зачета с оценкой на основе экспертной оценки деятельности обучающегося и защиты отчета. По завершении практики студенты в последний день практики представляют навыпускающую кафедру: дневник практики, включающий в себя отзывы руководителей практики от предприятия и ВУЗа о работе студента в период практики с оценкой уровня и оперативности выполнения им задания по практике, отношения к выполнению программы практики и т.п.; отчет по практике, включающий текстовые, табличные и графические материалы, отражающие решение предусмотренных заданием на практику задач. В отчете приводится анализ поставленных задач; выбор необходимых методов и инструментальных средств для решения поставленных задач; результаты решения задач практики; общие выводы по практике. Типовая структура отчета:

1. Титульный лист
2. Содержание
3. Введение (цель практики, задачи практики)
4. Практические результаты прохождения практики
5. Заключение
6. Список использованных источников и литературы
7. Приложения (при наличии)

7.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 11 семестре для очной формы обучения по четырехбалльной системе: «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Экспертная оценка результатов**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**

ПК-9.2	Знать: архитектуру современных систем и средств защиты информации, принципы построения межсетевых экранов, СОВ, обнаружения вторжений и криптографической защиты каналов. Уметь: проектировать и реализовывать защитные механизмы, способные отражать целенаправленные компьютерные атаки и блокировать несанкционированный доступ. Владеть: навыками проектирования и реализации адаптивных систем защиты информации, обладающих высокой устойчивостью к целевым атакам, способностью к динамическому реконфигурированию политик безопасности и сохранению функциональности в условиях интенсивного враждебного воздействия.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимально возможного количества баллов	61%-80% от максимально возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможного количества баллов
ПК-9.5	Знать: жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ. Уметь: выстраивать баланс между уровнем защиты и производительностью сети, прогнозировать эволюцию угроз и заранее закладывать контрмеры в новые разработки. Владеть: методологией управления рисками на всех этапах жизненного цикла систем защиты СССЭ и ЗТКС, включая прогнозирование эволюции векторов угроз, интеграцию контрмер на стадии НИОКР и обеспечение требуемого уровня остаточного риска при заданных эксплуатационных характеристиках.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимально возможного количества баллов	61%-80% от максимально возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможного количества баллов

ПК-9.6	Знать: современные подходы машинного обучения, нейронные сети, системы обнаружения аномалий и генеративные модели безопасности. Уметь: обучать модели распознавать новые виды атак, автоматизировать реагирование и усиливать традиционные средства защиты интеллектом. практическими методами применения технологий машинного обучения и искусственного интеллекта для обнаружения аномалий, классификации атак неизвестных классов, автоматизации реагирования и интеллектуального усиления традиционных средств защиты информации.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимально возможного количества баллов	61%-80% от максимально возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможного количества баллов
ПК-9.7	Знать: математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях. Уметь: видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели. Владеть: методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимально возможного количества баллов	61%-80% от максимально возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможного количества баллов

	поведения защищаемых систем в условиях дестабилизирующих воздействий.					

Экспертная оценка результатов освоения компетенций производится руководителем практики (или согласованная оценка руководителя практики от ВУЗа и руководителя практики от организации).

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

8.1 Перечень учебной литературы, необходимой для освоения практики

Основная литература

1. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб. пособие. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

2. Теория сетевых войн [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (894 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00

3. Методические указания к выполнению научно- исследовательской работы «Риск-анализ атакуемых информационных технологий и систем» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Г. Остапенко, Р. К. Бабаджанов, Н. Н. Корнеева. - Электрон. текстовые, граф. дан. (572 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00

Дополнительная литература

1. Горовая, В. И. Научно-исследовательская работа : учебное пособие для вузов / В. И. Горовая. — Москва : Издательство Юрайт, 2022. — 103 с. — (Высшее образование). — ISBN 978-5-534-14688-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496767.

2. Землянский, А. А. Управление информационными ресурсами в научно-исследовательской работе : учебное пособие / А. А. Землянский, И. Е. Быстренина. — 2-е изд. — Москва : Дашков и К, 2021. — 110 с. — ISBN 978-5-394-04149-5. — Текст : электронный // Цифровой образовательный ре-

сурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/107830.html.

3. Амелина, К. Е. Научно-исследовательская работа : учебно-методическое пособие / К. Е. Амелина, О. М. Стороженко. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2020. — 40 с. — ISBN 978-5-7038-5488-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115351.html

4. Кузнецова, М. М. Научно-исследовательская работа (практика по получению профессиональных навыков и опыта научно-исследовательской работы) : учебное пособие / М. М. Кузнецова. — Санкт-Петербург : Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2020. — 93 с. — ISBN 978-5-7937-1916-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118401.html

8.2 Перечень ресурсов сети "Интернет", необходимых для проведения практики

Anti-Malware (информационно-аналитический сайт по ИБ, основная тема - антивирусы и их исследования; есть форум); **AuditNet** (все об аудите ИТ и ИБ); **CCCure** (обучение по ИБ, сертификация, тестирование, аналитика, лучшие практики, документы); **CERT** (информация об уязвимостях, аналитика, исследования, лучшие практики, проведение расследований); **Datum** (сайт Ассоциации защиты прав операторов и субъектов персональных данных); **Information Security Forum** (лучшие практики, исследования, отчеты, методологии); **ISO27000.ru** (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО); **NIST** - Национальный институт стандартов и технологий США (лучшие практики, публикации на тему ИБ, материалы исследований); **SANS** (лучшие практики, статьи, исследования, информация об угрозах и уязвимостях); **Secunia** (информация об уязвимостях); **Security Focus** (информация об угрозах и уязвимостях, новости, средства обеспечения и анализа безопасности); **Security Lab** (новости, информация об угрозах и уязвимостях, статьи, средства обеспечения и анализа безопасности); **SecurityManagement.ru** (форум по ИБ); **SecurityPolicy.RU** (открытая библиотека документов по ИБ); **the Center for Internet Security** (средства анализа безопасности, лучшие практики, чек-листы); **wikIsec** - Энциклопедия информационной безопасности (публикации, статьи); **Windows IT Pro/RE** (раздел по безопасности русского издания журнала); **WinSecurity.ru** (статьи, документация, новости по безопасности Windows); **Журнал Информационная безопасность** (публикации, статьи, обзоры, форум); **Раздел форума по ИБ на сайте Bankir.ru** (форум по ИБ); **Центр безопасности Microsoft TechNet** (рекомендации, обновления, средства обеспечения и анализа безопасности).

Онлайн-сервисы по ИБ

2ip.ru (информация по IP); **Anubis** (поведенческий анализатор); **Change IP Country** (анонимайзер); **DomainTools** (информация по IP, интернет-утилиты); **Exploit Search** (поиск эксплойтов); **F-Secure Health Check** (проверка безопасности компьютера); **ha.ckers** (xss); **HackerTarget.com** (сканер уязвимостей); **hackvector** (xss); **Kaspersky Online Scanner** (антивирусный сканер); **LogBud** (большой набор интернет-утилит); **Nmap Online** (сетевой сканер); **Norton Safe Web** (проверка безопасности сайтов); **Online MD5 Crack** (восстановление паролей по хэшу MD5); **OpenDNS** (фильтрация нежелательных сайтов, защита от фишинга и вредоносных программ) (обзор); **ophrack** (восстановление паролей); **PDF X-RAY** (антивирусная проверка PDF-файлов); **plain-text.info** (восстановление паролей);**Qualys SSL Server Test** (анализ настроек SSL на веб-серверах); **Ring of Saturn Internetworking** (большой набор интернет-утилит); **Secunia Online Software Inspector** (проверка установки обновлений программного обеспечения); **SSL Analyzer** (проверка безопасности веб-сайта); **Sucuri SiteCheck** (проверка веб-сайта на наличие вредоносного кода); **SurfPatrol** (проверка безопасности браузера); **URL Analysis** (проверка безопасности ссылок); **Virus Total** (антивирусная проверка); **Wepawet** (антивирусная провека сайтов); **WhatIsMyIPAddress.com** (информация по IP); **РосНИИРОС** (whois).

8.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по практике, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Научная библиотека ВГТУ https://cchgeu.ru/university/library/

Электронный каталог научной библиотеки ВГТУ https://cchgeu.ru/university/library/elektronnyy-katalog/

Зональная научная библиотека ВГТУ https://lib.vsu.ru/

Профессиональные базы данных и информационные справочные системы

https://cchgeu.ru/university/library/prof-bd/index.php

Стандарты по информации, библиографии, библиотечному и издательскому делу (СИБИД)

https://cchgeu.ru/university/library/sibid/

ЭБС IPRBooks https://www.iprbookshop.ru/

ЭБС Лань https://e.lanbook.com/

ЭБС Университетская библиотека https://biblioclub.ru/

Методические и иные документы кафедры СИБ

https://cchgeu.ru/education/cafedras/kafsib/?docs

https://cchgeu.ru/education/programms/bksiss-3pp/?docs2021#md

https://cchgeu.ru/education/programms/ubtss-3pp/?docs2021#md

https://cchgeu.ru/education/programms/abis-3pp/?docs2021#md

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Практика обучающихся организуется как на базах практик, так и в в ВГТУ на базе кафедры систем информационной безопасности. Материально-техническая база определяется в зависимости от места прохождения практики и содержания практической подготовки обучающегося. В состав материально-технического обеспечения, необходимого для успешного прохождения практики на базе кафедры систем информационной безопасности входит следующее оборудование:

1. Система виброакустической и акустической защиты помещений «Соната АВ» в комплекте – 47190 – 1 шт
2. Системный телефон 2519-30 – 1 шт
3. Устройство защиты объектов информации «Соната-Р2»
4. Устройство защиты телефонных линий «МП-1Ц - 4212»
5. Устройство комбинированной защиты объектов «Соната РК-1» -19812
6. Частотомер Ч3-34А – 5 шт
7. Частотомер электронный счётный Ч3-33
8. Радиостанция 63 З21с-1 –
9. Измеритель модуляции СКЗ-43 – 2 шт.
10. Вольтметр В7-37 – 2 шт.
11. Вольтметр В7-26 – 5 шт.
12. Вольтметр В3-38Б – 4 шт.
13. Генератор Г3-112 – 4 шт.
14. Генератор Г4-102 – 6 шт.
15. Генератор Г3-112 – 4 шт.
16. Генератор Г3-116 – 2 шт.
17. Радиостанция ИП 1.100.074 «Лен-В» 1з21С-4 - 10 шт.
18. Индикатор поля камуфлированный «Редут» - 1 шт.
19. Осцилограф GOS-620FG – 2 шт.
20. Осцилограф С1-55 – 2 шт.
21. Паяльная станция LUKEY-852D+ - 2 шт.
22. Радиоприёмник З-399А - 3
23. Радиостанция 63 Р21с-1
24. Индикатор поля – 1 шт
25. Имитатор ИМФ-2

Практика реализуется в следующих помещениях кафедры с перечнем техники (оборудования), используемой для организации практики в форме практической подготовки: 402/5 - метрологии, электроники и схемотехники; 403/5 - спецоборудования; 404/5 - операционных систем и систем баз данных; 405/5 - сетей и систем передачи информации; 201/5 - методов и языков программирования; 402/3 - устройств приема сигналов; 410/3 - устройств передачи сигналов.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4