МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Декан факультета
факультет компьютерных наук

А.А. Крыловецкий

15.07.2022г.

ПРОГРАММА ПРАКТИКИ

Б2.О.02(П) Производственная практика, эксплуатационная

1. Код и наименование направления подготовки/специальности:
10.03.01 Информационная безопасность

2. Профиль подготовки/специализация: безопасность компьютерных систем

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации ФКН

6. Составители программы:
Емцева Анастасия Александровна, ассистент

7. Рекомендована:
Протокол НМС ФКН №5 от 25.04.2022 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2024-2025 **Семестр(ы)**: 6

9. Цель практики:

Целью производственной эксплуатационной практики является приобретение практических навыков и компетенций в сфере профессиональной деятельности по обеспечению информационной безопасности, а также приобщение бакалавров к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций.

Задачи практики:

- формирование у студентов умений и навыков: проведения технического обследования объекта информационной защиты; сбора экспериментального и экспертного материала и его теоретического обобщения; настройки, эксплуатации и поддержании в работоспособном состоянии компонентов систем обеспечения информационной безопасности;
- обучение студентов методикам работы с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности;

10. Место практики в структуре ООП:

Обязательная часть, блок Б2.

Для успешного прохождения практики студент должен обладать знаниями, умениями и навыками, сформированными в процессе освоения учебных дисциплин: Б1.О.16 Дискретная математика; Б1.О.28 Информатика; Б1.О.29 Алгоритмы и структуры данных; Б1.О.35 Введение в программирование; Б1.О.47 Web-технологии; Б1.О.14 Теория вероятностей и математическая статистика; Б1.О.30 Объектно-ориентированное программирование; Б1.О.31 Технологии и методы программирования; Б1.О.36 Языки и системы программирования; Б1.О.40 Организационное и правовое обеспечение информационной безопасности.

В результате прохождения практики, студент должен уметь решать следующие профессиональные задачи, соответствующие трудовым функциям профессиональных стандартов в информационной безопасности, соответствующих экспериментально-исследовательская деятельности:

- Знать правила эксплуатации и особенности применяемого в профильной организации оборудования, уметь работать с действующими стандартами, положениями и инструкциями по деятельности подразделения.
- Знания и умения по установке, настройке, эксплуатация и поддержании в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований, администрирование подсистем информационной безопасности объекта;
- Демонстрировать практический опыт проведения аттестации объектов информатизации по требованиям безопасности информации, аудит информационной безопасности автоматизированных систем, составление необходимых инструкций, проведение оценки соответствия выполненной работы техническому заданию и действующим нормативным документам.
- Разрабатывать технологическую и эксплуатационную документацию.
- Профессионально взаимодействовать с представителями организаций, представлять презентации результатов технических предложений, подготавливать и оформлять документацию.

11. Вид практики, способ и форма ее проведения

Вид практики: _____*производственная*_____*(учебная / производственная)*.
Способ проведения практики: ____*стационарная*_____ *(стационарная, выездная / выездная полевая).*
Реализуется полностью в форме практической подготовки (ПП).

12. Планируемые результаты обучения при прохождении практики (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-1.1	способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.1	знает архитектуру и принципы построения и защиты операционных систем	Знать: - принципы и основные направления обеспечения информационной безопасности; - методы управления информационной безопасностью.
		ОПК-1.1.2	знает программные интерфейсы настроек политик управления доступом в операционных системах	Знать: - основные угрозы информационной безопасности и модели нарушителя в информационных системах; - методы и средства контроля эффективности технической защиты информации.
		ОПК-1.1.3	умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации	Уметь: - выявлять уязвимости информационно-технологических ресурсов информационных систем; - применять основные инструменты защиты операционных систем.
		ОПК-1.1.4	владеет навыками настройки антивирусной защиты при обеспечении безопасности операционных систем	Владеть: - методами управления информационной безопасностью информационных систем.
		ОПК-1.1.5	знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации.
		ОПК-1.1.6	умеет использовать криптографические протоколы, применяемые в компьютерных сетях	Уметь: - применять инструменты для работы с криптографическими протоколами.
		ОПК-1.1.7	владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации	Владеть: - методами организации и управления деятельностью служб защиты информации на предприятии.
ОПК-1.2	способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-1.2.1	знает виды политик управления доступом и информационными потоками в компьютерных сетях	Знать: - принципы формирования политики информационной безопасности; - основные методы обобщения, восприятия и анализа информации.
		ОПК-1.2.2	умеет настраивать правила обработки	Уметь: - определять информационную инфраструктуру и информационные

			пакетов в компьютерных сетях	ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем.
		ОПК-1.2.3	владеет навыками управления средствами межсетевого экранирования в компьютерных сетях	Владеть: - навыками настройки основных средств сетевого взаимодействия
		ОПК-1.2.4	владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации	Владеть: - методами формирования требований по защите информации; - навыками анализа информационной инфраструктуры информационной системы и ее безопасности
		ОПК-1.2.5	знает принципы функционирования программных средств криптографической защиты информации	Знать: - основные средства и методы криптографической защиты информации.
ОПК-1.3	способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-1.3.1	знает принципы построения систем управления базами данных	Знать: - принципы организации информационных систем в соответствии с требованиями по защите информации.
		ОПК-1.3.2	умеет применять методы защиты информации в системах управления базами данных	Уметь: - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; - разрабатывать проекты нормативных документов и организационно-распорядительных документов, регламентирующих работу по защите информации.
		ОПК-1.3.3	владеть навыками обеспечения безопасности в базах данных	Владеть: - методами выявления угроз информационной безопасности информационных систем
		ОПК-1.3.4	знает правила математической логики при составлении запросов к реляционным моделям	Знать: основные конструкции и принципы формирования запросов к реляционным базам данных.
		ОПК-1.3.5	умеет оценивать сложность алгоритмов	Уметь: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - проявлять в своей профессиональной деятельности качества, наиболее востребованные в современном информационном обществе, способность ориентиро-

				ваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им. Пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.
ОПК-1.4	способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.1	знает требования стандартов по оценке уровня безопасности	Знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации; - основы организационного и правового обеспечения информационной безопасности; - основные понятия и методы в области управленческой деятельности;
		ОПК-1.4.2	умеет определять уровень безопасности и соответствие профилю защиты	Уметь: - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем.
		ОПК-1.4.3	знает источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению	Знает источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей. Умеет применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование). Владеет практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода.
		ОПК-1.4.4	умеет анализировать угрозы безопасности информации в компьютерных системах и сетях	Знает источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей. Умеет применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование). Владеет практическими навыками анализа исходного кода на предмет наличия уязвимостей, навы-

				ками использования специализированных утилит статического и динамического анализа кода.
		ОПК-1.4.5	знает принципы функционирования программных средств криптографической защиты информации	Знает принципы функционирования программных средств криптографической защиты информации. Владеет практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.

13. Объем практики в зачетных единицах / ак. час. — 6/216.

Форма промежуточной аттестации - *зачет с оценкой*.

14. Виды учебной работы

Вид учебной работы	Трудоемкость					
	Всего	По семестрам				
		№ 6		№ семестра		…
		ч.	ч., в форме ПП	ч.	ч., в форме ПП	
Всего часов	216	216	216			
в том числе:						
Лекционные занятия (контактная работа)						
Практические занятия (контактная работа)	3	3	3			
Самостоятельная работа	213	213	213			
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*						
Итого:	216	216	216			

15. Содержание практики (или НИР) [1]

№ п/п	Разделы (этапы) практики	Содержание раздела
1	Подготовительный	Инструктаж по технике безопасности, общее знакомство с местом практики (научно-исследовательскими лабораториями), составление и утверждение графика прохождения практики, изучение литературных источников по теме экспериментального исследования, реферирование научного материала и т.д.
2	Основной (экспериментальный, исследовательский и т.д.)	Освоение методов исследования, выполнение производственных заданий, проведение самостоятельных экспериментальных исследований, посещение отделов предприятий, знакомство с особенностями организационно-управленческой деятельности предприятия и т.д.
3	Заключительный (информационно-аналитический)	Обработка экспериментальных данных, составление и оформление отчета и т.д.

[1] *При реализации практики частично в форме практической подготовки необходимо отметить (*) содержание разделов, реализуемых в форме практической подготовки.*

16. Перечень учебной литературы, ресурсов сети «Интернет», необходимых для прохождения практики

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник

1	Казарин Олег Викторович. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / О.В. Казарин, А.С. Забабурин .— Москва : Юрайт, 2018 .— 311, [1] с. : ил., табл. — (Специалист) .— Библиогр. в конце гл. — ISBN 978-5-9916-9043-0.
2	Баранова Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330 .— ISBN 978-5-369-01761-6 .— ISBN 978-5-16-013849-7.
3	Мельников, Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова.— 2-е изд., перераб. и доп. — Москва : КноРус, 2018 .— 371 с. : ил., цв. ил., табл. — (Бакалавриат) .— Библиогр.: с. 369-371.
4	Ажмухамедов, И. М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева. — Санкт-Петербург : Интермедия, 2017. — 264 с. — ISBN 978-5-4383-0160-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103196 (дата обращения: 30.11.2020). — Режим доступа: для авториз. пользователей.
5	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
6	Криптографические методы защиты информации [Электронный ресурс] : учебно- методическое пособие : [для студ. фак. прикладной математики, информатики и механи- ки очной и очно-заоч. форм обучения, для направлений и специальностей: 01.03.02 - Прикладная математика и информатика, 02.03.02 - Фундаментальная информатика и информационные технологии, 01.04.02 - Прикладная математика и информатика, 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: Б.Н. Воронков, Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-241.pdf>.
7	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
8	Шифрование. Кодирование. Архивация [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 2-го к. днев. отд-ния фак. приклад. математики, информатики и механики ; для специальности 080500.62 -Бизнес-информатика] / Воронеж. гос. ун-т ; сост. Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— Windows 2000; Adobe Acrobat Reader .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m13-218.pdf>.

б) дополнительная литература:

№ п/п	Источник
1	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры: [для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям] / под ред. Т.А. Поляковой, А.А. Стрельцова .— Москва : Юрайт, 2018 .— 324, [1] с. : ил. — (Бакалавр и магистр. Академический курс) .— Библиогр.: с. 324-[325].
2	Ищейнов Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
3	Хорев Павел Борисович. Методы и средства защиты информации в компьютерных системах: учебное пособие для студ. вузов, обуч. по направлению 230100 (654600) "Информатика и вычислительная техника" / П.Б. Хорев .— М. : ACADEMIA, 2005 .— 254, [1] с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 251-252 .— ISBN 5-7695-1839-1.

4	Малюк Анатолий Александрович. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для студ. вузов, обуч. по специальности 075400 - "Комплексная защита объектов информации" / А.А. Малюк .— М. : Горячая линия-Телеком , 2004 .— 280 с. : ил/ .— (Учебное пособие) .— Библиогр.: с. 276-278 .— ISBN 5-93517-197-X.
5	Галицкий, Александр Владимирович. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин .— М. : ДМК Пресс, 2004 .— 613 с. : ил .— (Администрирование и защита) .— Библиогр.: с.599-608 .— Предм. указ.: с.603-613 .— ISBN 5-94074-244-0.
6	Варлатая Светлана Климентьевна. Защита и обработка конфиденциальных документов : учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова ; Дальневост. федер. ун-т .— Москва : Проспект, 2015 .— 178, [1] с. : ил., табл. — Библиогр.: с. 177 .— ISBN 978-5-392-19176-5
7	Андрианов В. И. "Шпионские штучки 2", или Как сберечь свои секреты / Под общ. ред. Колесниченко О. В. и др. — СПб. : Полигон, 1997 .— 271 с. — ISBN 5-89173-015-4 : 12.33.
8	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурсы Интернет
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/).
3	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019 «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019 ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020. «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № 43/8 от 10.02.2020.
4	Меры защиты информации в государственных информационных системах. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/675)
5	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (https://fstec.ru/component/attachments/download/289)
6	Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., Методический документ. (http://fstec.ru/component/attachments/download/812).
7	Методика моделирования угроз безопасности информации. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/2727).
8	Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/).
9	Организационные основы защиты информации на предприятии (http://content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html).
10	Правовое обеспечение системы защиты информации на предприятии (http://old.ci.ru/inform11_97/aiti1.htm)
11	Участие в планировании и организации работ по обеспечению защиты объекта (https://studref.com/651196/prochie/uchastie_v_planirovanii_i_organizatsii_rabot_po_obespecheniyu_zaschity_obekta)

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

17. Информационные технологии, используемые при проведении практики, включая программное обеспечение и информационно-справочные системы (при необходимости)

Практика проводится на профильных предприятиях (организациях, учреждениях, фирмах), с которыми заключены договора на прохождение практики, а также в аудиториях, компьютерных и специализированных лабораториях факультета компьютерных наук ВГУ. Предприятия предоставляют студентам материально-техническую базу для прохождения практики.

При проведении в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения

Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение практики:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Практика проводится на профильных предприятиях (организациях, учреждениях, фирмах), с которыми заключены договора на прохождение практики, а также в аудиториях, компьютерных и специализированных лабораториях факультета компьютерных наук ВГУ. Предприятия предоставляют студентам материально-техническую базу для прохождения практики.

N п/п	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19" (30 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316П
2	Лаборатория информационной безопасности компьютерных систем: персональные компьюте-ры на базе i3-8100-3,9ГГц, мониторы ЖК 24" (13 шт.), мультимедийный проектор, экран. Лабораторное оборудование программно-аппаратных средств обеспечения информацион-ной безопасности: персональные компьютеры на базе Intel i3-8100 3.60ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управля-емый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лаборатор-ная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС".	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 303П
3	В соответствии с договором № 427 от 20.05.2019 о практической подготовке обучающихся	107023, г. Москва, ул. Измайловский Вал, д. 30, ООО «Философия.ИТ» (Лига цифровой экономики)
4	В соответствии с договором № 564 от 11.05.2021 о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 53, оф. 501, ООО «Ангелы ИТ
5	В соответствии с договором № 273 от 24.02.2021 о практической подготовке обучающихся	125009, г. Москва, ул. Воздвиженка, д. 10, Акционерное общество «Банк ДОМ.РФ»
6	В соответствии с договором № 22/01-2 от 20.01.2022 о практической подготовке обучающихся	394018, г. Воронеж, ул. Свободы, д. 69, оф. 45, ООО «ЭЛ-ЭКС»
7	В соответствии с договором №22/02-10 от 21.02.2022 о практической подготовке обучающихся	394006, г. Воронеж, ул. Карла Маркса, д. 46 Управление Федеральной налоговой службы по Воронежской области
8	В соответствии с договором № 1431 от 19.07.2019 г. о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 70 Департамент финансов Воронежской области

9	В соответствии с договором № 22/05-20 от 05.05.2022 о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 1Д, пом. 1, ООО «СёрфСтудио»
10	В соответствии с договором № 22/03-100 от 30.03.2022 о практической подготовке обучающихся	443090, Самарская область, г. Самара, улица Гастелло, дом 43А, помещение Н15, ООО «Хоулмонт Самара»
11	В соответствии с договором № 22/01-1 от 20.01.2022 о практической подготовке обучающихся	394026, г. Воронеж, ул. Текстильщиков, д. 5Б, пом. 177, ООО «ФИТТИН»
12	В соответствии с договором № 35-22-01/09600/355 от 31.03.2022 - № 22/04-44 зарег. 12.04.2022 о практической подготовке обучающихся	196084, г. Санкт-Петербург, ул. Киевская, д. 5, к. 4 ООО «Газпромнефть-Цифровые решения»
13	В соответствии с договором № 22/05-21 от 05.05.2022 г. о практической подготовке обучающихся	394000, г. Воронеж, ул. Пятницкого, 55 ООО ТК «Контакт»
14	В соответствии с договором № 22/05-36 от 12.05.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 6а, помещение V ООО «Техномаркет
15	В соответствии с договором № ДОГ-3500-22-000000176 – 22/06-28 от 27.05.2022 г. зарег. 06.06.2022 г. о практической подготовке обучающихся	162602, Вологодская обл., г. Череповец, ул. Ленина, д. 123А ОАО «Северсталь — Инфоком»

19. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Раздел (этап) Подготовительный	ОПК-1.1.1 ОПК-1.1.2 ОПК-1.1.5 ОПК-1.2.1 ОПК-1.2.5 ОПК-1.3.1 ОПК-1.3.4 ОПК-1.4.1	Знает: - архитектуру и принципы построения и защиты операционных систем; - программные интерфейсы настроек политик управления доступом в операционных системах; - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - виды политик управления доступом и информационными потоками в компьютерных сетях; - принципы функционирования программных средств криптографической защиты информации; - принципы построения систем управления базами данных; - правила математической логики при составлении запросов к реляционным моделям; - требования стандартов по оценке уровня безопасности.	Дневник практики, Отчет по практике.
2.	Раздел (этап) экспериментальный, исследовательский	ОПК-1.1.3 ОПК-1.1.4 ОПК-1.1.6 ОПК-1.1.7 ОПК-1.2.2 ОПК-1.2.3 ОПК-1.2.4 ОПК-1.3.2 ОПК-1.3.3 ОПК-1.3.5	- умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации; - владеет навыками настройки антивирусной защиты при обеспечении безопасности операционных систем;	Дневник практики, Отчет по практике.

		ОПК-1.4.2	- умеет использовать криптографические протоколы, применяемые в компьютерных сетях; - владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации; - умеет настраивать правила обработки пакетов в компьютерных сетях; - владеет навыками управления средствами межсетевого экранирования в компьютерных сетях; - владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации; - умеет применять методы защиты информации в системах управления базами данных; - владеет навыками обеспечения безопасности в базах данных; - умеет оценивать сложность алгоритмов; - умеет определять уровень безопасности и соответствие профилю защиты.	
3.	Заключительный (информационно-аналитический)	ОПК-1.1.1 ОПК-1.1.3 ОПК-1.1.5 ОПК-1.2.1 ОПК-1.2.5 ОПК-1.3.1 ОПК-1.3.2 ОПК-1.3.3 ОПК-1.3.4 ОПК-1.3.5 ОПК-1.4.1 ОПК-1.4.2	- знает архитектуру и принципы построения и защиты операционных систем; - умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации; - знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - знает виды политик управления доступом и информационными потоками в компьютерных сетях; - знает принципы функционирования программных средств криптографической защиты информации; - знает принципы построения систем управления базами данных; - умеет применять методы защиты информации в системах управления базами данных; владеть навыками обеспечения безопасности в базах данных; - знает правила математической логики при составлении запросов к реляционным моделям; - умеет оценивать сложность алгоритмов; - знает требования стандартов по оценке уровня безопасности; - умеет определять уровень безопасности и соответствие профилю защиты.	Дневник практики, Отчет по практике.
Промежуточная аттестация форма контроля – зачет с оценкой				

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания и критерии их оценивания

20.1 Текущий контроль успеваемости Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Оценка знаний, умений и навыков, характеризующих этапы формирования компетенций, при прохождении практики проводится в ходе промежуточной аттестаций. Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

20.2 Промежуточная аттестация Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

СТРУКТУРА ОТЧЕТА ПО ПРАКТИКЕ

1. Отчет по практике должен включать титульный лист, содержание, введение, описание теоретических и практических аспектов выполненной работы, заключение, необязательный список использованных источников, приложения.
2. На титульном листе должна быть представлена тема практики, группа и фамилия студента, данные о предприятии, на базе которого выполнялась практика, фамилия руководителя.
3. Во введении студенты должны дать краткое описание задачи, решаемой в рамках практики.
4. В основной части отчета студенты приводят подробное описание проделанной теоретической и (или) практической работы, включая описание и обоснование выбранных решений, описание программ и т.д.
5. В заключении дается краткая характеристика проделанной работы, и приводятся ее основные результаты.
6. В приложениях приводятся непосредственные результаты разработки: тексты программ, графики, диаграммы, и т.д.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА

1. Отчет оформляется в печатном виде, на листах формата А4.
2. Основной текст отчета выполняется шрифтом 13-14 пунктов, с интервалом 1,3-1,5 между строками. Текст разбивается на абзацы, каждый из которых включает отступ и выравнивание по ширине.
3. Текст в приложениях может быть выполнен более мелким шрифтом.
4. Отчет разбивается на главы, пункты и подпункты, включающие десятичную нумерацию.
5. Рисунки и таблицы в отчете должны иметь отдельную нумерацию и названия.
6. Весь отчет должен быть оформлен в едином стиле: везде в отчете для заголовков одного уровня, основного текста и подписей должен использоваться одинаковый шрифт.
7. Страницы отчета нумеруются, начиная с титульного листа. Номера страниц проставляются в правом верхнем углу для всего отчета кроме титульного листа.
8. Содержание отчета должно включать перечень всех глав, пунктов и подпунктов, с указанием номера страницы для каждого элемента содержания.
9. Ссылки на литературу и другие использованные источники оформляются в основном тексте, а сами источники перечисляются в списке использованных источников.

Описание технологии проведения

Промежуточная аттестация по практике включает подготовку и защиту отчета/проекта и/или выполнение практического задания.

Отчет содержит следующие составляющие: обработанный и систематизированный материал по тематике практики; экспериментальную часть, включающую основные методы проведения исследования и статистической обработки, обсуждение

полученных результатов; заключение, выводы и список литературных источников. Отчет обязательно подписывается (заверяется) руководителем практики. Результаты прохождения практики докладываются обучающимся в виде устного сообщения с демонстрацией презентации на заседании кафедры (заключительной конференции).

По результатам доклада с учетом характеристики руководителя и качества представленных отчетных материалов обучающемуся выставляется соответствующая оценка. Дифференцированный зачет по итогам практики выставляется обучающимся руководителем практики на основании доклада и отчетных материалов, представленных обучающимся.

При оценивании используются количественные шкалы оценок.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Программа практики выполнена в полном объеме и в соответствии с утвержденным графиком. Подготовленные отчетные материалы отражают адекватное формулирование цели и задач исследования, выбранный метод обеспечил решение поставленных в ходе практики задач	Повышенный уровень	Отлично
Программа практики выполнена в соответствии с утвержденным графиком. Подготовленные отчетные материалы и представленный доклад не соответствует одному (двум) из перечисленных критериев. Недостаточно продемонстрировано, или содержатся отдельные пробелы.	Базовый уровень	Хорошо
Обучающийся частично выполнил план работы практики (не менее 50%). В представленных отчетных материалах выявлено несоответствие выбранного метода цели и задачам исследования. При прохождении практики не были выполнены все поставленные перед практикантом задачи (можно привести перечень задач практики), отчетные материалы имеют ряд недочетов по объему, необходимым элементам и качеству представленного материала.	Пороговый уровень	Удовлетворительно
Обучающийся не выполнил план работы практики. В представленных отчетных материалах отсутствуют необходимые элементы: нет отзыва научного руководителя, не сформулированы цель и задачи работы, не приведены или ошибочны предложенные методы и т.д.	–	Неудовлетворительно