

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ

Проректор по учебной и научной
работе

 Лейфа А.В. Лейфа

1 июля 2024 г.

ПРОГРАММА ПРАКТИКИ

**«ПРОИЗВОДСТВЕННАЯ ПРАКТИКА ПО МОДУЛЮ "ЗАЩИТА ИНФОРМАЦИИ В
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С
ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАМ...»**

Направление подготовки 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Направленность (профиль) образовательной программы –

Квалификация выпускника – Техник по защите информации

Год набора – 2024

Форма обучения – Очная

Составитель Д.В. Фомин, старший преподаватель,

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

Программа практики составлена на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1551

Программа практики обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО

Учебно-методическое управление

Чалкина Н.А. Чалкина

1 июля 2024 г.

СОГЛАСОВАНО

Научная библиотека

Петрович О.В. Петрович

1 июля 2024 г.

СОГЛАСОВАНО

Выпускающая кафедра

Казакова Т.А. Казакова

1 июля 2024 г.

СОГЛАСОВАНО

Центр цифровой трансформации и
технического обеспечения

Тодосейчук А.А. Тодосейчук

1 июля 2024 г.

1. ТИП ПРАКТИКИ И СПОСОБ ПРОВЕДЕНИЯ

1.1. Тип (форма проведения) практики

Вид практики: производственная.

Тип практики: технологическая.

Форма проведения практики: дискретно.

1.2. Способы проведения практики

Способы проведения практики: выездная и стационарная.

2. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Целью проведения технологической (далее производственной) практики является приобретение обучающимися профессиональных навыков, практического опыта, закрепление, систематизация и расширение теоретических знаний по дисциплинам учебного плана; подготовка информационной и опытной базы для написания выпускной квалификационной работы. Целями производственной практики являются: подготовка к решению производственных задач предприятия, сбор материала для выполнения выпускной квалификационной работы; закрепление и углубление теоретических знаний, полученных при изучении дисциплин учебного плана; приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение современного состояния и направлений развития компьютерной техники и информационных технологий; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем информационной безопасности; изучение комплексного применения методов и средств обеспечения информационной безопасности; изучение источников информации и системы оценок эффективности ее использования; закрепление и углубление практических навыков в области информационной безопасности; повышение уровня освоения компетенций в профессиональной деятельности. Задачи производственной (технологической) практики: изучить особенности практической работы по направлению информационная безопасность; овладеть навыками делового общения, принятия организационно- управленческих решений, сбора и анализа- информации, расчета экономических показателей системы информационной безопасности, анализа и интерпретации деятельности профильных хозяйствующих субъектов; развить навыки аналитической и научно- исследовательской деятельности, подготовки аналитических отчетов и информационных обзоров; овладеть методами и приобрести опыт решения профессиональных задач. В период производственной (технологической) практики обучающийся: Знакомится: с историей, традициями и организационной структурой подразделения предприятия; с формами организации производственного процесса и его технологическим обеспечением; с составом и особенностями эксплуатации программных и технических средств обработки и защиты информации; с актуальными для подразделения проблемами обеспечения информационной безопасности. Изучает: порядка организации труда на рабочих местах; требований конфиденциального делопроизводства; основных обязанностей должностных лиц подразделения; основных характеристик и возможностей, используемых в подразделении технических, программных средств защиты информации. Приобретает практические навыки: проверки, настройки и использования технических и программных средств защиты информации; выполнения основных функциональных обязанностей в соответствии с должностью; работы с документацией, анализа и обобщения материалов; реализации и апробации предложений и проектных решений.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной	Код и наименование индикатора достижения профессиональной компетенции
-------------------------------------	---

<p>компетенции</p> <p>ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно – телекоммуникационных систем и сетей</p>	<p>Практический опыт: установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;</p> <p>Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно- аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно- аппаратных (в том числе криптографических) средств защиты информации</p> <p>Знания: способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС</p>
<p>ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях</p>	<p>Практический опыт: поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС</p> <p>Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно- аппаратных (в том числе криптографических) средств защиты информации</p> <p>Знания: возможных угроз безопасности информации в</p>

	<p>ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядка тестирования функций программных и программно- аппаратных (в том числе криптографических) средств защиты информации; организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации</p>
<p>ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.</p>	<p>Практический опыт: защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно- аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями</p> <p>Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно- аппаратных (в том числе криптографических) средств защиты информации</p> <p>Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации</p>

4. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОП

Производственная практика по специальности 10.02.04 Обеспечение безопасности телекоммуникационных систем направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках профессионального модуля: ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств

защиты, для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение безопасности телекоммуникационных систем. Производственная практика проходит в 8 семестре в объеме 108 ак. часов

5. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Базами производственной практики являются предприятия и организации, с которыми заключен договор о практической подготовке обучающихся. Основными условиями прохождения производственной практики в данных предприятиях и организациях являются наличие квалифицированного персонала, оснащенность современным оборудованием.

Время проведения производственной практики – 8-й семестр.

6. ОБЪЕМ ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТЬ В НЕДЕЛЯХ

Объем практики в зачетных единицах составляет 3 з.ед, 108 академических часов. Длительность практики – 4 недели.

7. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Разделы (этапы) практики	Содержание раздела (этапа) практики	Трудоемкость (в академических часах)
1	Организационно-подготовительный	Подготовительный этап: - участие в установочном собрании по практике; - подготовка документов, подтверждающие факт направления на практику; - выбор темы исследования, получение задания от руководителя практики; - инструктаж по технике безопасности.	8
2	Аналитический	Ознакомление: с организацией информационного обеспечения подразделения; с процессом проектирования и эксплуатации информационных средств; с методами планирования и проведения мероприятий по созданию (разработке) проекта (подсистемы) информационной среды предприятия для решения конкретной задачи. Изучение: структурные и функциональные схемы предприятия, организацию деятельности подразделения; порядок и методы ведения делопроизводства; требования к техническим, программным средствам, используемым на предприятии. Приобретение практических навыков: выполнения функциональных обязанностей; ведения документации; проектирования информационных систем; практической апробации предлагаемых проектных решений. Сбор материалов для написания выпускной квалификационной работы. Выполнение индивидуального задания.	126

3	Отчетный	Выработка на основе проведенного исследования выводов и предложений; подготовка отчетной документации по итогам практики; оформление отчета по производственной практике в соответствии с требованиями; сдача отчета о практике на кафедру; Защита отчета.	10
Итого 108.0 часов			

8. ОБРАЗОВАТЕЛЬНЫЕ, НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ И НАУЧНО-ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ НА ПРАКТИКЕ

Основными образовательными технологиями, используемыми на технологической практике, являются: - проведение обзорных лекций; - изучение современных методов анализа информации и интерпретации результатов; - выполнение письменных аналитических и расчетных заданий в рамках практики с использованием рекомендуемых информационных источников (учебники, статьи в периодической печати, сайты в сети Интернет); - консультации преподавателя по актуальным вопросам, возникающим у студентов в ходе ее выполнения; методологии выполнения домашних заданий, подготовке отчета по практике и доклада по нему, выполнению аналитических заданий; - ознакомительные беседы с сотрудниками производственных подразделений базы производственной практики; - самостоятельная работа обучающихся вне аудитории, в которую включается выполнение разделов практики в соответствие с индивидуальным заданием и рекомендованными источниками литературы. Основными образовательными научно производственными технологиями, используемыми на производственной (технологической) практике, являются: - проведение обзорных лекций; - обсуждение материалов практики с руководителем; - ознакомительные беседы с сотрудниками производственных подразделений базы производственной практики; - проведение защиты отчета о практике. Основными возможными научно- исследовательскими технологиями, используемыми на производственной практике, являются: - сбор научной литературы по тематике задания на производственной практике; - сбор и компоновка научно-технической документации с целью углубленного исследования предметной области - участие студента в решении научно-производственных задач организации, учреждения или предприятия (выполнение достаточно широкого спектра работ, связанных с отработкой профессиональных знаний, умений и навыков): - участие в формировании пакета научно-исследовательской документации как на базе практики, так и в учебных подразделениях Университета.

9. ФОРМА ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Результаты работы, выполненной в процессе прохождения производственной практики, представляются в виде отчета. Содержание отчета определяется, прежде всего, индивидуальным заданием на производственную практику. 1. Общие сведения о предприятии, учреждении, организации, на котором проходила производственная практика. 2. Структурная схема предприятия (или его подразделения), дать описание организации управления его деятельностью. 3. Описать состав и основные характеристики средств вычислительной техники, используемые в подразделении. 4. Сделать обзор технических средств защиты информации и организационных мер обеспечения информационной безопасности. 5. Рассказать о результатах домашней работы, использованные литературные материалы, содержание лекций, экскурсий, консультаций. 6. Привести анализ собранной информации, необходимой для выполнения практической работы. 7. Дать анализ информационных потоков, возможные угрозы, способы защиты от них. 8. Изложить методику решения конкретной задачи, и полученные результаты решения этой задачи.

10. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ

АТТЕСТАЦИИ ПО ПРАКТИКЕ

ВОПРОСЫ

1. Содержание и задачи процесса управления информационной безопасностью на предприятии.
2. Содержание и задачи процесса управления информационной безопасностью предприятия в целом.
3. Системный подход к проектированию, внедрению и поддержанию системы обеспечения информационной безопасности на предприятии.
4. Стандартизация в сфере управления информационной безопасностью предприятия (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408).
5. Ресурсы предприятия, подлежащие защите с точки зрения информационной безопасности.
6. Перечень нормативно- методических и организационно- распорядительных документов по защите информации на предприятии.
7. Концепция безопасности предприятия и информационная безопасность.
8. Назначение и содержание политики информационной безопасности предприятия в целом, его структурных подразделений, частных политик безопасности. Средства их реализации.
9. Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.
10. Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.
11. Организация контроля эффективности выполнения персоналом, ответственным за информационную безопасность, своих функциональных обязанностей.
12. Программные средства поддержки процессов управления информационной безопасностью.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРАКТИКЕ

11.1. Литература

Основная литература

1. Романюк, В. А. Основы радиоэлектроники: учебник для среднего профессионального образования / В. А. Романюк. — Москва: Издательство Юрайт, 2024. — 288 с. — (Профессиональное образование). — ISBN 978-5-534-10394-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542110>
2. Мэйволд, Э. Безопасность сетей: учебное пособие для СПО / Э. Мэйволд. — Саратов: Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102183.html>
3. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543873>

Дополнительная литература

1. Максимов, Н. В. Компьютерные сети: учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2022. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1714105>

2. Миленина, С. А. Электротехника, электроника и схемотехника : учебник и практикум для среднего профессионального образования / С. А. Миленина, Н. К. Миленин ; под редакцией Н. К. Миленина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 406 с. — (Профессиональное образование). — ISBN 978-5-534-04676-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536766>

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340>

4. Ситников, А. В. Электротехнические основы источников питания : учебник / А. В. Ситников, И. А. Ситников. — Москва : КУРС : ИНФРА-М, 2022. — 240 с. — (Среднее профессиональное образование). - ISBN 978-5-906818-76-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1725082>

5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537691>

6. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 464 с. — (Профессиональное образование). — ISBN 978-5-534-17310-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542157>

7. Хачатрян, Г. А. Организация и технология работы с конфиденциальными документами : учебник для СПО / Г. А. Хачатрян, И. В. Кузнецова. — 2-е изд. — Саратов : Профобразование, 2024. — 238 с. — ISBN 978-5-4488-1026-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/137716.html>

8. Шишмарёв, В. Ю. Электрорадиоизмерения. Практикум : практическое пособие для среднего профессионального образования / В. Ю. Шишмарёв. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 234 с. — (Профессиональное образование). — ISBN 978-5-534-08588-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539909>

11.2. Программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	VirtualBox	Бесплатное распространение по лицензии GNU GPL https://www.virtualbox.org/wiki/GPL
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	7-Zip	Бесплатное распространение по лицензии GNU LGPL http://www.7-zip.org/license.txt .
4	Fedora Workstation 27	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.htm .
5	Ubuntu Desktop	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.html .
6	Debian	Бесплатное распространение по лицензии GNU GPL https://www.debian.org/legal/licenses/
7	http://www.amursu.ru	Официальный сайт ФГОУ ВО «Амурский

		государственный университет»
8	http://www.iprbookshop.ru	Научно- образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу.
9	http://e.lanbook.com	Электронно- библиотечная система Издательство «Лань» – тематические пакеты: математика, физика, инженерно- технические науки. Ресурс, включающий в себя как электронные версии книг издательства «Лань» и других ведущих издательств учебной литературы, так и электронные версии периодических изданий по естественным, техническим и гуманитарным наукам.
10	ЭБС ЮРАЙТ https://urait.ru/	Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.

11.3. Профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	https://scholar.google.ru/	GoogleScholar — поисковая система по полным текстам научных публикаций всех форматов и дисциплин.
2	https://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - российский информационно- аналитический портал в области науки, технологии, медицины и образования
3	http://neicon.ru	Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно- информационного консорциума (НЭИКОН)
4	https://uisrussia.msu.ru/	Университетская информационная система РОССИЯ (УИС РОССИЯ).
5	https://fstec.ru/	Федеральная служба по техническому и экспортному контролю. Официальный сайт
6	https://g-sopka.ru/	ГосСОПКА — это государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, нарушение или прекращение работы которых может крайне негативно повлиять на экономику страны или безопасность граждан. Корпоративный центр ГосСОПКА автоматизирует выявление инцидентов, реагирование на них и взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ).
7	https://www.elibrary.ru/	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.

12. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

При выполнении различных видов работ на практике используются следующие информационные технологии: системы мультимедиа; самостоятельная работа с учебной, учебно- методической и научной литературой, с источниками Интернет, с использованием справочно- правовых систем и электронных библиотечных информационно-справочных систем.

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Материально- техническая база предприятия, на котором проводится практика соответствует действующим санитарным и противопожарным правилам и нормам. Во время прохождения практики обучающийся использует современную компьютерную технику, программные и технические средства, предоставляемые на предприятии (организации). Практика проводится в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам. Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам и к электронной информационно- образовательной среде университета. Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.