



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

УТВЕРЖДАЮ

И.о. директора ИКБ

_____ Бакаев А.А.

«__» _____ 2025 г.

Рабочая программа практики

Производственная практика

Преддипломная практика

Читающее подразделение

**кафедра КБ-2 «Информационно-аналитические системы
кибербезопасности»**

Направление

10.03.01 Информационная безопасность

Направленность

**Организация и технологии защиты информации (в сфере
связи, информационных и коммуникационных
технологий)**

Квалификация

бакалавр

Форма обучения

очная

Общая трудоемкость

6 з.е.

Распределение часов дисциплины и форм промежуточной аттестации по семестрам

Семестр	Зачётные единицы	Распределение часов							Формы промежуточной аттестации
		Всего	Лекции	Лабораторные	Практические	Самостоятельная работа	Контактная работа в период практики и (или) аттестации	Контроль	
8	6	216	0	0	0	194,25	4	17,75	Зачет с оценкой
из них на практ. подготовку			0	0	0	97	0	0	

Программу составил(и):

канд. техн. наук, Заведующий кафедрой, Трубиенко О.В. _____

Рабочая программа практики

Преддипломная практика

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:

направление: 10.03.01 Информационная безопасность

направленность: «Организация и технологии защиты информации (в сфере связи, информационных и коммуникационных технологий)»

Рабочая программа одобрена на заседании кафедры

кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Протокол от 20.02.2025 № 7

Зав. кафедрой Трубиенко О.В. _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Протокол от _____ 2026 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Протокол от _____ 2027 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Протокол от _____ 2028 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Протокол от _____ 2029 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

1. ЦЕЛИ ОСВОЕНИЯ ПРАКТИКИ

«Преддипломная практика» имеет своей целью сформировать, закрепить и развить практические навыки и компетенции, предусмотренные данной рабочей программой в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность с учетом специфики направленности подготовки – «Организация и технологии защиты информации (в сфере связи, информационных и коммуникационных технологий)».

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Направление:	10.03.01 Информационная безопасность
Направленность:	Организация и технологии защиты информации (в сфере связи, информационных и коммуникационных технологий)
Блок:	Практика
Часть:	Часть, формируемая участниками образовательных отношений
Общая трудоемкость:	6 з.е. (216 акад. час.).

3. ТИП, ВИД И СПОСОБ ПРОВЕДЕНИЯ ПРАКТИКИ

Вид практики:	Производственная практика
Тип практики:	Преддипломная практика

Способ (способы) проведения практики определяются в соответствии с федеральным государственным образовательным стандартом. В случае, если стандарт не регламентирует способ проведения практики, то она проводится стационарно.

4. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ ПРАКТИКИ

«Преддипломная практика» направления подготовки 10.03.01 Информационная безопасность проводится на базе структурных подразделений РТУ МИРЭА или в организации, осуществляющей деятельность по профилю соответствующей образовательной программы (далее - профильная организация), в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора, заключаемого между образовательной организацией и профильной организацией.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ

В результате освоения практики обучающийся должен овладеть компетенциями:

ПК-1 - Способен проводить настройку, эксплуатацию и обслуживание средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

ПК-2 - Способен организовывать комплекс мер для защиты в информационно-аналитической системе информации ограниченного доступа

ПК-3 - Способен проводить анализ уязвимостей, осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем

ПК-4 - Способен разрабатывать и уточнять модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

ПК-1 : Способен проводить настройку, эксплуатацию и обслуживание средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

ПК-1.1 : Осуществляет настройку и обслуживание средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

Знать:

- этапы жизненного цикла информационно-аналитических систем

Уметь:

- осуществлять настройку и обслуживание средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

Владеть:

- навыками настройки и обслуживания средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

ПК-1.2 : Эксплуатирует средства защиты информации информационно-аналитических систем

Знать:

- средства защиты информации информационно-аналитических систем

Уметь:

- эксплуатировать средства защиты информации информационно-аналитических систем

Владеть:

- навыками эксплуатации средств защиты информации информационно-аналитических систем

ПК-2 : Способен организовывать комплекс мер для защиты в информационно-аналитической системе информации ограниченного доступа

ПК-2.1 : Составляет комплекс правил, процедур, практических приёмов, принципов и методов, средств обеспечения информационной безопасности автоматизированной системы

Знать:

- правила, процедуры, практические приёмы, принципы и методы, средства обеспечения информационной безопасности автоматизированной системы

Уметь:

- составлять комплекс правил, процедур, практических приёмов, принципов и методов, средств обеспечения информационной безопасности автоматизированной системы

Владеть:

- навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения информационной безопасности автоматизированной системы

ПК-2.2 : Подготавливает документы, определяющие правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации

Знать:

- правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации

Уметь:

- подготавливать документы, определяющие правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации

Владеть:

- навыками подготовки документов, определяющих правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации

ПК-3 : Способен проводить анализ уязвимостей, осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем**ПК-3.1 : Разрабатывает предложения по совершенствованию системы управления защитой информации автоматизированной системы****Знать:**

- способы совершенствования системы управления защитой информации автоматизированной системы

Уметь:

- разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы

Владеть:

- навыками разработки предложений по совершенствованию системы управления защитой информации автоматизированной системы

ПК-3.2 : Проводит анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных средств и информационных систем**Знать:**

- доступные информационные источники, известные уязвимости

Уметь:

- проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных средств и информационных систем

Владеть:

- навыками проведения анализа доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных средств и информационных систем

ПК-4 : Способен разрабатывать и уточнять модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем**ПК-4.1 : Классифицирует и оценивает угрозы безопасности информации автоматизированной системы****Знать:**

- классификацию угроз безопасности информации автоматизированной системы

Уметь:

- классифицировать и оценивать угрозы безопасности информации автоматизированной системы

Владеть:

- навыками классификации и оценки угроз безопасности информации автоматизированной системы

ПК-4.2 : Разрабатывает и уточняет модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем**Знать:**

- модели угроз и нарушителя

Уметь:

- разрабатывать и уточнять модели угроз и нарушителя для обеспечения безопасности

информации автоматизированных систем

Владеть:

- навыками разработки и уточнения модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем

В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ ОБУЧАЮЩИЙСЯ ДОЛЖЕН

Знать:

- этапы жизненного цикла информационно-аналитических систем
- классификацию угроз безопасности информации автоматизированной системы
- модели угроз и нарушителя
- средства защиты информации информационно-аналитических систем
- способы совершенствования системы управления защитой информации автоматизированной системы
- правила, процедуры, практические приёмы, принципы и методы, средства обеспечения информационной безопасности автоматизированной системы
- доступные информационные источники, известные уязвимости
- правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации

Уметь:

- разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы
- разрабатывать и уточнять модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем
- классифицировать и оценивать угрозы безопасности информации автоматизированной системы
- составлять комплекс правил, процедур, практических приёмов, принципов и методов, средств обеспечения информационной безопасности автоматизированной системы
- эксплуатировать средства защиты информации информационно-аналитических систем
- осуществлять настройку и обслуживание средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем
- подготавливать документы, определяющие правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации
- проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных средств и информационных систем

Владеть:

- навыками классификации и оценки угроз безопасности информации автоматизированной системы
- навыками подготовки документов, определяющих правила и процедуры для обеспечения защиты информации в информационных и информационно-аналитических системах в ходе их эксплуатации
- навыками разработки предложений по совершенствованию системы управления защитой информации автоматизированной системы
- навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения информационной безопасности автоматизированной системы
- навыками эксплуатации средств защиты информации информационно-аналитических систем
- навыками настройки и обслуживания средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем

- навыками проведения анализа доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных средств и информационных систем
- навыками разработки и уточнения модели угроз и нарушителя для обеспечения безопасности информации автоматизированных систем

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

При проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений и лидерских качеств.

Код занятия	Наименование разделов и тем /вид занятия/	Сем.	Часов
1. Раздел 1			
1.1	Выполнение заданий направленных на получение навыков практической подготовки (Ср). Отчет	8	194,25 (из них 97 на практ. подг.)
1.2	Контактная работа в период практики (КрПА). Контактная работа в период практики	8	3,75
2. Промежуточная аттестация (зачёт с оценкой)			
2.1	Подготовка к сдаче промежуточной аттестации (ЗачётСОц).	8	17,75
2.2	Контактная работа с преподавателем в период промежуточной аттестации (КрПА).	8	0,25

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

7.1. Перечень компетенций

Перечень компетенций, на освоение которых направлена «Преддипломная практика», с указанием результатов их формирования в процессе освоения образовательной программы, представлен в п.3 настоящей рабочей программы

7.2. Типовые контрольные вопросы и задания

1. Анализ автоматизированной системы защиты конфиденциальной информации на основе программного обеспечения с открытым исходным кодом;
2. Анализ системы защиты информации телекоммуникационной сети предприятия на основе контроля электромагнитных излучений технических средств;
3. Разработка утилиты управления информационной безопасностью ПЭВМ;
4. Разработка программного комплекса оценки соответствия системы защиты информации многофункционального объекта информатизации требованиям безопасности информации;
5. Разработка автоматизированной системы защищенного электронного документооборота;
6. Разработка системы защиты информации локальной вычислительной сети предприятия;
7. Разработка способа защищенной передачи данных по радиоканалам;
8. Разработка пространственно распределенной системы контроля радиосигналов на предприятии;
9. Разработка алгоритма электронной подписи для систем защищенного документооборота;

10. Анализ систем доверенной аутентификации с использованием сканирования отпечатка пальцев в системе защищенного документооборота;

11. Разработка программы контроля и предотвращения несанкционированного подключения USB-устройств к ПЭВМ

7.3. Фонд оценочных материалов

Полный перечень оценочных материалов представлен в приложении 1.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Наименование помещения	Перечень основного оборудования
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мультимедийное оборудование, специализированная мебель, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.
Компьютерный класс	Компьютерная техника с возможностью подключения к сети «Интернет», мультимедийное оборудование, специализированная мебель.
Базы практики	Оборудование и технические средства обучения, позволяющем выполнять определенные виды работ, предусмотренные заданием на практику.

8.2. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. P7-Офис.
2. Google Chrome. Свободное программное обеспечение
3. Wireshark. Свободное программное обеспечение (лицензия GNU GPL2)
4. Debian Linux. Свободное программное обеспечение (лицензия GNU GPL)
5. Microsoft Visual Studio Community. Свободное программное обеспечение (Лицензия Microsoft EULA)

8.3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

8.3.1. Основная литература

1. Нестеров С. А. Информационная безопасность: учебник и практикум для академического бакалавриата. - М.: Юрайт, 2017. - 321 с.
2. Медведев В. А. Информационная безопасность. Введение в специальность: учебник для вузов. - М.: КНОРУС, 2021. - 143 с.
3. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс].. - Санкт-Петербург: Лань, 2020. - 124 с. — Режим доступа: <https://e.lanbook.com/book/133924>

8.3.2. Дополнительная литература

1. Запечников С.В. Информационная безопасность открытых систем:.. - Москва: Горячая линия - Телеком, 2008. - 558 с.

2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей.: - М.: ФОРУМ: ИНФРА-М, 2010. - 416 с.
3. Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Доп. УМО вузов в кач. учеб. пособия для вузов. - СПб.: Питер, 2008. - 272 с.

8.4. РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Научная электронная библиотека <http://www.elibrary.ru>
2. Wolfram: вычисления и знания, рука к руке <http://www.wolfram.com>
3. Информационно-правовой портал ГАРАНТ <http://www.garant.ru>

8.5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ПРАКТИКИ

На первом организационном собрании необходимо ознакомить студентов с содержанием рабочей программы практики, с порядком и графиком прохождения практики.

В начале прохождения практики, на организационно-подготовительном этапе студентам необходимо:

- оформить задание на практику;
- пройти инструктаж по технике безопасности и противопожарной технике;
- ознакомиться с содержанием рабочей программы практики, правилами и обязанностями практиканта на предприятии, структурой подразделений (рабочих мест) практики, режимом работы предприятия;
- ознакомиться со структурой заключительного отчета по практике.

За период прохождения производственной практики студент самостоятельно изучает документацию, связанную с будущей профессиональной деятельностью, учебную, справочную, нормативную и научно-техническую литературу по соответствующим разделам данной программы. Литература подбирается в библиотеке университета (включая доступ к ЭБС), публичных научно-технических библиотеках. Закрепление результатов практики осуществляется путем самостоятельной работы студентов с рекомендуемой литературой.

В ходе прохождения практики студент должен решить все поставленные перед ним задачи и написать отчет о своей деятельности в рамках практики, а также выполненные работы (трудовые действия, трудовые функции), связанные с будущей профессиональной деятельностью обучающегося.. В отчете должны быть описаны все основные этапы прохождения практики в соответствии с заданием. Окончательно оформленный и подписанный студентом отчет сдается руководителю практики не позже, чем за 3 дня до защиты. В указанное руководителем практики время студент обязан явиться на кафедру для защиты отчета.

8.6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБУЧЕНИЮ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Освоение практики обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных

материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиа материалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.