



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**  
**Эксплуатационная 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	3 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	3	108	0	0	0	86,25	4	17,75	Зачет с оценкой
из них на практ. подготовку			0	0	0	27	0	0	

Программу составил(и):

канд. техн. наук, Заведующий кафедрой, Трубиенко О.В. \_\_\_\_\_

Рабочая программа практики

**Эксплуатационная 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

«Эксплуатационная 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:	3 з.е. (108 акад. час.).

## 3. ТИП, ВИД И СПОСОБ ПРОВЕДЕНИЯ ПРАКТИКИ

Вид практики:	Производственная практика
Тип практики:	Эксплуатационная 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

«Эксплуатационная 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

## ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

## В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ ОБУЧАЮЩИЙСЯ ДОЛЖЕН

### 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
<b>1. Подготовительный этап</b>			
1.1	<b>Инструктаж по технике безопасности и охране труда (КрПА).</b> Проведение инструктажа. Знакомство с информационно-методической базой практики	8	1
1.2	<b>Распределение студентов по организациям. Определение индивидуального задания на практику. (КрПА).</b> Собеседование, утверждение индивидуального задания по практике.	8	2
1.3	<b>Заполнение бланков для прохождения эксплуатационной практики. (КрПА).</b> Проверка корректности заполнения бланков для прохождения эксплуатационной практики	8	1
1.4	<b>Инструктаж по ТБ на месте прохождения эксплуатационной практики (КрПА).</b> Проведение инструктажа в организации.	8	2
<b>2. Аналитический этап</b>			
2.1	<b>Выполнение заданий направленных на получение навыков практической подготовки (Ср).</b> Ознакомление со структурой организации, основными учредительными документами. Ознакомиться с внутренней организационно-распорядительной документацией - изучить положения, должностные инструкции, методическое обеспечение и др.	8	10
2.2	<b>Выполнение заданий направленных на получение навыков практической подготовки (Ср).</b> Ознакомление с используемыми информационными технологиями, парком компьютеров. Изучение архитектуры компьютерной сети, основных характеристик сетевого оборудования, функциональных особенностей программного обеспечения предприятия.	8	40
2.3	<b>Выполнение заданий направленных на получение навыков практической подготовки (Ср).</b> Самостоятельная работа по выполнению индивидуального задания.	8	200
2.4	<b>Собеседование по промежуточным результатам. (КрПА).</b> Индивидуальная беседа со студентам по промежуточным результатам практической подготовки.	8	2

<b>3. Практический этап</b>			
<b>3.1</b>	<b>Выполнение заданий направленных на получение навыков практической подготовки (Ср).</b> Поиск и сбор информацию об используемых предметно-ориентированных информационных системах, пакетах прикладных программ и специализированных информационных технологиях, используемых в организации. Обработка полученной информации.	8	60
<b>3.2</b>	<b>Выполнение заданий направленных на получение навыков практической подготовки (Ср).</b> Самостоятельная работа по выполнению индивидуального задания. Консультация с преподавателем и руководителем практики от предприятия по выполнению задания.	8	202,25
<b>3.3</b>	<b>Собеседование по промежуточным результатам. (КрПА).</b> Индивидуальная беседа со студентам по промежуточным результатам практической подготовки.	8	1,75
<b>4. Промежуточная аттестация (зачёт с оценкой)</b>			
<b>4.1</b>	<b>Подготовка к сдаче промежуточной аттестации (ЗачётСОц).</b>	8	17,75
<b>4.2</b>	<b>Контактная работа с преподавателем в период промежуточной аттестации (КрПА).</b>	8	0,25

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

### 7.1. Перечень компетенций

Перечень компетенций, на освоение которых направлена «Эксплуатационная 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

ОПК-1.1-З1 Знать

Вопрос: Какие виды тайн вы знаете?

Правильный ответ: Государственная, коммерческая, профессиональную, служебную

ОПК-1.1-У1 Уметь

Вопрос: Классификация защищаемой информации по степени секретности (конфиденциальности)(выбрать наиболее полный ответ):

- 1)Секретная, совершенно секретная, особая секретность
- 2)Секретная, совершенно секретная, особой важности
- 3)Секретная, совершенно секретная
- 4)Секрет, совершенный секрет, особый секрет

Правильный ответ: 2

ОПК-1.1-В1 Владеть

Вопрос: Что такое конфиденциальность информации

- 1)действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
- 2)зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель
- 3)Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- 4)действия, направленные на получение информации неопределенным кругом лиц или

передачу информации неопределенному кругу лиц;

Правильный ответ: 3

ОПК-10.1-31 Знать

Вопрос: Какие требования должна удовлетворять политика безопасности?

Правильный ответ: лаконичность и доступность обычному сотруднику

ОПК-10.1-У1 Уметь

Вопрос: Что такое политика информационной безопасности?

1)Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

2): Координированные действия по направлению и контролю над деятельностью организации в связи с рисками.

3)Процесс разработки и/или отбора и внедрения мер управления рисками информационной безопасности организации.

4)Процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимости уровня риска.

Правильный ответ: 1

ОПК-10.1-В1 Владеть

Вопрос: Политики должны содержать:

1)предмет, основные цели и задачи политики безопасности

2)условия применения политики безопасности и возможные ограничения

3)описание позиции руководства организации в отношении выполнения политики

безопасности и организации режима информационной безопасности организации в целом

4)права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации

5)порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности

Правильный ответ: 1,2,3,4,5

ОПК-10.2-31 Знать

Вопрос: Дать определение информационной безопасности

Правильный ответ: Это комплекс мер и средств, направленных на защиту конфиденциальности, целостности и доступности информации.

ОПК-10.2-У1 Уметь

Вопрос: Что такое SOC

1)структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и реагирования на киберинциденты.

2)система управления событиями безопасности

3)систематизированное описание техник (приёмов) и тактик, которые используют злоумышленники при атаках на организации

Правильный ответ: 1

ОПК-10.2-В1 Владеть

Вопрос: Что такое объект информатизации

1)Средство системы обработки информации, которое может быть выделено процессу обработки данных на определенный интервал времени.

2)Все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении

3)Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их

обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

4) Совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС.

Правильный ответ: 3

ОПК-10.3-31 Знать

Вопрос: Что такое угроза информационной безопасности организации?

Правильный ответ: Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации

ОПК-10.3-У1 Уметь

Вопрос: Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
- 2) соблюдение конфиденциальности информации ограниченного доступа
- 3) реализацию права на доступ к информации

Правильный ответ: 1,2,3

ОПК-10.3-В1 Владеть

Вопрос: Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- 1) своевременное обнаружение фактов несанкционированного доступа к информации
- 2) постоянный контроль за обеспечением уровня защищенности информации
- 3) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней
- 4) тесты для проверки устойчивости безопасности информации

Правильный ответ: 1,2,3

### 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.
Компьютерный класс	Компьютерная техника с возможностью подключения к сети «Интернет», мультимедийное оборудование, специализированная мебель.
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-



	образовательную среду организации.
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. Баланов А.Н. Комплексная информационная безопасность: полный справочник специалиста [Электронный ресурс]: Практическое пособие. - Вологда: Инфра-Инженерия, 2024. - 156 с. – Режим доступа: <https://znanium.ru/catalog/document?id=451735>
2. Баранова Е.К., Бабаш А.В., Ларин Д.А. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]: Учебное пособие. - Москва: Издательский Центр РИО, 2024. - 236 с. – Режим доступа: <https://znanium.ru/catalog/document?id=443250>
3. Баланов А. Н. Комплексная информационная безопасность [Электронный ресурс]: учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 400 с. – Режим доступа: <https://e.lanbook.com/book/414947>
4. Суворова Г. М. Информационная безопасность [Электронный ресурс]: учебное пособие для вузов. - Москва: Юрайт, 2024. - 277 с – Режим доступа: <https://urait.ru/bcode/544029>
5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2024. - 416 с. – Режим доступа: <https://znanium.ru/catalog/document?id=442922>
6. Медведев В. А. Информационная безопасность. Введение в специальность: учебник для вузов. - М.: КНОРУС, 2021. - 143 с.
7. 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. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие. - Москва: Издательский Центр РИО, 2024. - 336 с. – Режим доступа: <https://znanium.ru/catalog/document?id=442107>
9. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]: Монография. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 180 с. – Режим доступа: <https://znanium.com/catalog/document?id=431346>

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

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