



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-1 «Защита информации»**  
Направление **10.03.01 Информационная безопасность**  
Направленность **Безопасность автоматизированных систем (в сфере связи, информационных и коммуникационных технологий)**  
Квалификация **бакалавр**  
Форма обучения **очная**  
Общая трудоемкость **15 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	15	540	0	0	0	512,25	10	17,75	Зачет с оценкой

Программу составил(и):

*старший преподаватель, Карамышева Е.О.* \_\_\_\_\_

*старший преподаватель, Головченко Д.А.* \_\_\_\_\_

*преподаватель, Яковлева В.Д.* \_\_\_\_\_

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: «Безопасность автоматизированных систем (в сфере связи, информационных и коммуникационных технологий)»

Рабочая программа одобрена на заседании кафедры

**кафедра КБ-1 «Защита информации»**

Протокол от 23.01.2025 № 6

Зав. кафедрой Артемова С.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-1 «Защита информации»**

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-1 «Защита информации»**

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-1 «Защита информации»**

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-1 «Защита информации»**

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 – «Безопасность автоматизированных систем (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:	Безопасность автоматизированных систем (в сфере связи, информационных и коммуникационных технологий)
Блок:	Практика
Часть:	Обязательная часть
Общая трудоемкость:	15 з.е. (540 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:

**ОПК-1** - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

**ОПК-10** - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

## **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ**

**ОПК-1 : Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;**

**ОПК-1.1 : Понимает принципы работы современных информационных технологий**

**Знать:**

- знает роль информации и информационных технологий в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении

**Уметь:**

- умеет выполнять сравнительный анализ программных и программно-аппаратных средств защиты информации автоматизированных информационных систем в защищенном исполнении

**Владеть:**

- владеет инструментальными средствами моделирования систем защиты информации автоматизированных информационных систем в защищенном исполнении

**ОПК-10 : Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;**

**ОПК-10.1 : Принимает участие в формировании политики информационной безопасности в качестве технического специалиста**

**Знать:**

- основные принципы обеспечения информационной безопасности и защиты информации

**Уметь:**

- осуществлять обоснованный выбор средств и систем управления информационной безопасности

**Владеть:**

- навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты

**ОПК-10.2 : Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности и управляет процессом их реализации на объекте защиты**

**Знать:**

- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

**Уметь:**

- проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем

**Владеть:**

- основными приемами эффективного обеспечения информационной безопасности автоматизированной системы

## **В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ ОБУЧАЮЩИЙСЯ ДОЛЖЕН**

**Знать:**

- знает роль информации и информационных технологий в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении
- основные принципы обеспечения информационной безопасности и защиты информации

- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

**Уметь:**

- умеет выполнять сравнительный анализ программных и программно-аппаратных средств защиты информации автоматизированных информационных систем в защищенном исполнении

- осуществлять обоснованный выбор средств и систем управления информационной безопасности

- проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем

**Владеть:**

- владеет инструментальными средствами моделирования систем защиты информации автоматизированных информационных систем в защищенном исполнении

- навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты

- основными приемами эффективного обеспечения информационной безопасности автоматизированной системы

## 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. Организационно-подготовительный раздел</b>			
<b>1.1</b>	<b>Инструктаж по требованиям техники безопасности и охране труда. Доведения порядка выполнения учебной практики. Организационное собрание. (КрПА).</b> Инструктирование обучаемых. Выдача заданий, знакомство с целью и основными этапами практики	8	9,75
<b>2. Получение навыков практической деятельности, сбор материалов и формирование</b>			
<b>2.1</b>	<b>Анализ информации и формирование отчёта по практической подготовке (Ср).</b> Этап сбора практических документальных материалов, этап практической деятельности и выполнение индивидуальных заданий	8	256,25
<b>2.2</b>	<b>Анализ информации и формирование отчёта по практической подготовке (Ср).</b> Этап сбора обработки и анализа выявленной информации. Подведение итогов. Выводы. Составление отчета.	8	256
<b>3. Промежуточная аттестация (зачёт с оценкой)</b>			
<b>3.1</b>	<b>Подготовка к сдаче промежуточной аттестации (ЗачётСОц).</b>	8	17,75
<b>3.2</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

1. Роль информации и информационных технологий в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении
2. Значение информации, информационных технологий в области обеспечения информационной безопасности автоматизированных систем в защищенном исполнении
3. Методы исследования предметной области в целях обоснования целесообразности создания автоматизированной системы в защищенном исполнении
4. Требования к автоматизированной системе в защищенном исполнении, процессу её создания и эксплуатации
5. Характеристика инструментальных средств моделирования предметной области функционирования автоматизированных информационных систем в защищенном исполнении
6. Выявление и анализ уязвимостей системы защиты информации автоматизированных систем в защищенном исполнении
6. Классификация уязвимостей автоматизированных информационных систем
7. Модель угроз информационной безопасности автоматизированных информационных систем
8. Модель нарушителя информационной безопасности автоматизированных информационных систем
9. Источники угроз информационной безопасности автоматизированных систем в защищенном исполнении
10. Классификация угроз информационной безопасности автоматизированных систем в защищенном исполнении
11. Методы анализа текущего состояния информационной безопасности в организации с целью разработки требований к создаваемой автоматизированной системе в защищенном исполнении
12. Задачи оценки экономической эффективности создания автоматизированных информационных систем в защищенном исполнении
13. Способы оценки экономической эффективности создания автоматизированных информационных систем в защищенном исполнении
14. Способы подготовки исходных данных для технико-экономического обоснования проектных решений по разработке автоматизированных систем в защищенном исполнении
15. Стандарты моделирования автоматизированных информационных систем с учетом требований по защите информации
16. Этапы разработки, внедрения и эксплуатации автоматизированных систем в защищенном исполнении
17. Организация и проведение диагностики и тестирования систем защиты информации автоматизированных систем в защищенном исполнении
18. Стандарты моделирования, применяемые в ходе выявления уязвимостей системы защиты информации автоматизированных систем в защищенном исполнении
19. Основные компоненты эксплуатационного процесса автоматизированных информационных систем в защищенном исполнении
20. Техническое обслуживание компонентов автоматизированных информационных систем в защищенном исполнении
21. Организация технического обслуживания компонентов автоматизированных информационных систем в защищенном исполнении
22. Виды технического обслуживания объектов автоматизированных систем в защищенном исполнении
23. Группы мероприятий, выполняемых в рамках технического обслуживания автоматизированных информационных систем в защищенном исполнении
24. Мероприятия, к выполнению которых привлекается эксплуатационный персонал в процессе эксплуатации автоматизированных информационных систем в защищенном исполнении
25. Стандарты моделирования, используемые для создания модели системы защиты автоматизированной информационной системы в защищенном исполнении
26. Возможные перспективы своей профессиональной карьеры в области защиты информации

## 27. Основные методики самоконтроля, саморазвития и самообразования

### 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
Лаборатория технической защиты информации, лаборатория неразрушающего контроля, проведения специальных обследований и специальных проверок	Компьютерная техника с возможностью подключения к сети Интернет
Лаборатория программно-аппаратных средств защиты информации	Аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе средства криптографической защиты информации (средства анализа защищенности компьютерных сетей, аппаратно-программные средства управления доступом к данным, стенды для изучения проводных и беспроводных компьютерных сетей, включающие абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.
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.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности	Аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе криптографические средства защиты информации, средствами сканирования защищенности компьютерных сетей, стенды для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, системы обнаружения атак, аппаратно-программными средствами управления доступом к данным,



	шифрования, средства контроля и управления доступом в помещения, охранная и пожарная сигнализация, средства климатического
Лаборатория программно-аппаратных средств защиты информации	Аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе средства криптографической защиты информации (средства анализа защищенности компьютерных сетей, аппаратно-программные средства управления доступом к данным, стенды для изучения проводных и беспроводных компьютерных сетей, включающие абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак
Лаборатория автоматизированных систем в защищенном исполнении	Аппаратно-программные средства управления доступом к данным, средства криптографической защиты информации, средства дублирования и восстановления данных, средства мониторинга состояния автоматизированных систем, средства контроля и управления доступом в помещения
Лаборатория защищенных автоматизированных систем	Аппаратно-программные средства управления доступом к данным, шифрования, средства дублирования и восстановления данных, средства мониторинга состояния автоматизированных систем, источники бесперебойного и аварийного питания, средства контроля и управления доступом в помещения, охранная и пожарная сигнализация, средства климатического контроля
Базы практики	Оборудование и технические средства обучения, позволяющем выполнять определенные виды работ, предусмотренные заданием на практику.

## 8.2. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Р7-Офис.
2. СКЗИ "Контитент-АП". Лицензионный договор № КБ/27621/1/108 от 07.10.2021
3. СЗИ vGate R2 Enterprise Plus. Лицензионный договор № КБ/27621/1/108 от 07.10.2021
4. Secret Net Studio 8. Лицензионный договор № КБ/27621/1/108 от 07.10.2021
5. СЗИ Secret Net LSP. Лицензионный договор № КБ/27621/1/108 от 07.10.2021

## 8.3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

### 8.3.1. Основная литература

1. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]: Учебник для вузов. - Москва: Юрайт, 2021. - 309 с – Режим доступа: <https://urait.ru/bcode/469866>
2. Нестеров С. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 324 с. – Режим доступа: <https://e.lanbook.com/book/114688>
3. Внуков А. А. Защита информации [Электронный ресурс]: Учебное пособие для вузов. - Москва: Юрайт, 2021. - 161 с – Режим доступа: <https://urait.ru/bcode/470131>

4. Внуков А. А. Основы информационной безопасности: защита информации [Электронный ресурс]: Учебное пособие Для СПО. - Москва: Юрайт, 2021. - 161 с – Режим доступа: <https://urait.ru/bcode/475890>

### **8.3.2. Дополнительная литература**

1. Петренко В. И., Мандрица И. В. Защита персональных данных в информационных системах. Практикум [Электронный ресурс]: учебное пособие для вузов. - Санкт-Петербург: Лань, 2020. - 108 с. – Режим доступа: <https://e.lanbook.com/book/149364>
2. Бирюков А. А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2013. - 473 с.

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

1. Информационно-правовой портал ГАРАНТ [http:// www.garant.ru](http://www.garant.ru)
2. Консультант Плюс [http:// www.consultant.ru](http://www.consultant.ru)
3. База данных Web of Science  
<http://www.webofknowledge.com>
4. Сайт Федеральной службы по техническому и экспортному контролю России  
<http://www.fstec.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.