



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

Министерство науки и высшего образования Российской Федерации

**ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

Центр подготовки специалистов в сфере информационной безопасности и противодействия  
техническим средствам разведки

ОДОБРЕНО:

Руководитель ОП

 Е.В. Мельникова  
(подпись)

« 01 » 09 2022 г.

**Рабочая программа производственной практики, технологической**

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

---

### **1. Цели практики**

Образовательная деятельность при проведении практики осуществляется в форме практической подготовки.

Целью производственной практики, технологической является закрепление и углубление знаний, полученных студентами в процессе теоретического обучения, приобретение необходимых умений, навыков, компетенций и опыта практической работы по изучаемому направлению.

Производственная практика направлена на получение профессиональных умений и опыта профессиональной деятельности:

- получения практических навыков самостоятельной и коллективной работы при решении поставленных задач;
- углубленное изучение и приобретение практических навыков в работе с системами криптографической защиты в рамках конкретного предприятия;
- изучение технологий внедрения, настройки и применения межсетевых экранов, трафик-инспекторов и других технологий защиты информации в компьютерных сетях организаций;
- изучение возможностей VPN-технологий для защиты информации на предприятии;
- приобретение и закрепление практических навыков работы с программно-аппаратными средствами защиты информации на предприятиях.

### **2. Вид, тип и основные базы проведения практики**

Вид практики – производственная.

Тип практики – технологическая.

База проведения практики: предприятия и организации г. Иваново и Ивановской области.

### **3. Место практики в структуре ОП**

Учебная, ознакомительная практика включена в обязательную часть в структуре ОП.

Дисциплины, на освоении которых базируется практика:

- Методы и средства криптографической защиты информации;
- Защита информации от утечки по техническим каналам;
- Программно-аппаратные средства защиты информации.

Для прохождения практики обучающийся должен:

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- технологии обнаружения компьютерных атак и их возможности;
- средства реализации атак.
- механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
- атаки на сетевые службы.
- атаки с использованием промежуточных узлов и территорий.
- основные уязвимости и типовые атаки на современные компьютерные системы;
- возможности и особенности использования специализированных программно- аппаратных средств при проведении аудита информационной безопасности;
- методы защиты компьютерных сетей;
- классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

---

– основные принципы администрирования защищенных компьютерных систем;  
– особенности реализации методов защиты информации современными программно-аппаратными средствами.

Уметь:

– выполнять функции администратора безопасности защищенных компьютерных систем;  
– выполнять настройку защитных механизмов сетевых программно-аппаратных средств;  
– настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;  
– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;  
– организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;  
– применять средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети.  
– Реализовывать цели и принципы зондирования узлов сети.  
– Использовать коммерческие и свободно распространяемые средства аудита безопасности компьютерных сетей.  
– Использовать особенности средств активного аудита.  
– применять средства анализа защищенности серверов приложений.

Иметь практический опыт/Иметь навыки:

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации;  
– средствами администрирования систем обнаружения компьютерных атак;  
– средствами и системами аудита информационной безопасности; методикой проведения аудита информационной безопасности;  
– средствами администрирования систем организации виртуальных частных сетей.  
– Навыками определения структуры информационно-телекоммуникационных сетей.  
– Навыками применения программных средств анализа топологии вычислительной сети, определения маршрутов прохождения сетевых пакетов, обнаружения объектов сети, построения схемы сети.  
– Навыками выявления телекоммуникационного оборудования, выявления и построения схемы информационных потоков защищаемой информации в компьютерной сети.

#### **4. Планируемые результаты обучения при прохождении практики**

##### **4.1. Компетенции, формированию которых способствует практика**

При прохождении практики формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) универсальные (УК):

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

б) общепрофессиональные (ОПК):

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



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

---

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

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-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах

ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях

ОПК-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

**4.2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с индикаторами достижения формируемых компетенций**

В результате прохождения практики обучающийся должен:

Знать:

- основные приемы, методы и способы выявления, наблюдения, измерения и контроля параметров исследуемых процессов;
- приемы, методы и способы обработки, представления и интерпретации результатов проведенных практических исследований;

Уметь:

- проводить расчеты по проекту сетей, сооружений и средств связи в соответствии с техническим заданием и с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ;
- проводить технико-экономическое обоснование проектных расчетов с использованием современных подходов и методов;
- использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи;
- составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию сооружений, сетей и оборудования связи, по программам испытаний;
- организовывать и осуществлять проверку технического состояния и оценку остатка ресурса сооружений, оборудования и средств связи;
- применять методы обслуживания, поиска неисправностей и ремонта оборудования средств связи;
- составлять заявку на оборудование, запасные части, измерительную технику;



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

- готовить техническую документацию на ремонт и восстановительные работы оборудования, средств, систем и сетей связи;
- организовывать и осуществлять систему мероприятий по охране труда и техники безопасности в процессе эксплуатации, технического обслуживания и ремонта телекоммуникационного оборудования;

Иметь практический опыт/Иметь навыки:

- навыками инструментальных измерений параметров телекоммуникационного оборудования;
- навыками поиска неисправностей узлов и блоков средств связи;
- навыками устранения неисправностей узлов и блоков средств связи;
- навыками организации работ определенного коллектива для проведения измерений параметров, поиска и устранения неисправностей узлов и блоков средств связи.

### 5. Объем и содержание практики

Объем практики составляет 9 зачетных единицы (324 академических часа).

Образовательная деятельность в форме практической подготовки организуется при проведении практики в полном объеме путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Продолжительность практики – 6 недель.

№ п/п	Разделы (этапы) практики	Содержание практики по разделам (этапам)	Формы текущего контроля успеваемости, форма промежуточной аттестации
1	Организационно-подготовительный этап	Организационное собрание: подготовка документов, подтверждающих факт направления на практику, получение индивидуального задания; Инструктаж по технике безопасности.	Тест по технике безопасности Ведение записи в дневнике практики
2	Основной этап	Сбор, обработка и анализ полученной информации. Выполнение заданий, в т.ч. индивидуальных, в соответствии с рабочим планом-графиком Задание №1. Внедрение криптографической системы Задание №2. Внедрение межсетевого экрана	Собеседование по выполнению заданий, в т.ч. индивидуальных Отчет Ведение записи в дневнике практики Презентация части проекта
3	Заключительный этап	Составление и оформление отчетности по практике	Зачет с оценкой

### 6. Характеристика форм отчетности и оценочных средств для текущего контроля успеваемости и промежуточной аттестации по практике

Текущий и итоговый контроль осуществляется руководителем производственной практики, в соответствии с календарным планом в 6 семестре. Текущий контроль осуществляется в форме руководства выполнения задания по производственной практике.

В ходе выполнения практики каждым обучающимся обязательно заполняется Дневник по



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

практике.

Формой отчетности по практике является Отчет.

Формой промежуточной аттестации производственной практики является зачет с оценкой, который проводится как защита отчета по практике по получению профессиональных умений и опыта профессиональной деятельности.

Неудовлетворительные результаты промежуточной аттестации по практике или непрохождение промежуточной аттестации по практике при отсутствии уважительных причин признаются академической задолженностью.

## 6.2 Оценка результатов прохождения практики

### Шкала оценки результатов прохождения практики

№ п.п.	Наименование показателя	Максимум баллов
<b>1</b>	<b>Качество подобранного материала для проведения анализа (максимум 15 баллов)</b>	
	Наличие источников информации в соответствии с заданием (максимум 5 баллов)	
	Наличие актуальных первичных данных, материалов (максимум 10 баллов)	
<b>2</b>	<b>Качественная оценка проведенного анализа собранных материалов (максимум 40 баллов)</b>	
2.1	Выполнение требований к содержательной части отчета, соответствие заданию (максимум 10 баллов)	
2.2	Оценка степени самостоятельности проведенного анализа (максимум 10 баллов)	
2.3	Оценка качества проведенного анализа собранных материалов, данных (максимум 20 баллов)	
<b>3</b>	<b>Выполнение общих требований к проведению практики (максимум 25 баллов)</b>	
3.1	Своевременное выполнение отдельных этапов прохождения практики и предоставление документов (максимум 10 баллов)	
3.2	Выполнение требований руководителя по выполнению заданий (максимум 10 баллов)	
3.3	Выполнение требований к оформлению отчета по практике (максимум 5 баллов)	
<b>4</b>	<b>Защита отчета по практике (максимум 20 баллов)</b>	
	<b>Количество баллов за учебную практику (максимум 100 баллов)</b>	



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

Обобщенные критерии проверки сформированности компетенции, шкала  
оценивания компетенций

100-балльная система оценки	Традиционная (четырёхбалльная) система оценки	Критерий оценивания	Содержание критерия оценивания
85 - 100	отлично / зачтено	Продвинутый уровень освоения компетенций	Компетенции освоены. Обучающийся показывает глубокие знания, демонстрирует умения и навыки решения сложных задач. Способен самостоятельно решать проблему / задачу на основе изученных методов, приемов и технологий.
70 - 84	хорошо / зачтено	Повышенный уровень освоения компетенций	Компетенции освоены. Обучающийся показывает полноту знаний, демонстрирует умения и навыки решения типовых задач в полном объеме.
50 - 69	удовлетворительно / зачтено	Базовый уровень освоения компетенций	Компетенции освоены. Обучающийся показывает общие знания, умения и навыки, входящие в состав компетенций, имеет представление об их применении, но применяет их с ошибками.
0 - 49	неудовлетворительно / незачтено	Заявленные компетенции не освоены	Компетенции не освоены. Обучающийся не владеет необходимыми знаниями, умениями, навыками или частично показывает знания, умения и навыки, входящие в состав компетенций.

## 7. Учебно-методическое и информационное обеспечение практики

Основная литература:

1. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.
2. Гулятьева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гулятьева. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574729> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.
3. Гриценко, Ю. Б. Вычислительные системы, сети и телекоммуникации : учебное пособие / Ю. Б. Гриценко ; Томский Государственный университет систем управления и



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

радиоэлектроники (ТУСУР), Факультет дистанционного обучения. – Томск : ТУСУР, 2015. – 134 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=480639> (дата обращения: 04.12.2022). – Библиогр.: с. 123-124. – Текст : электронный.

4. Рыбальченко, М. В. Архитектура информационных систем : учебное пособие / М. В. Рыбальченко ; Южный федеральный университет. – Таганрог : Южный федеральный университет, 2015. – Часть 1. – 92 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=462011> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9275-1765-7. – Текст : электронный.

**Дополнительная литература:**

1. Галатенко, В. А. Основы информационной безопасности: Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233063> (дата обращения: 04.12.2022). – ISBN 5-9556-0052-3. – Текст : электронный.
2. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=362895> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – Текст : электронный.
3. Архитектуры и топологии многопроцессорных вычислительных систем: курс лекций : учебное пособие / А. В. Богданов, В. В. Корхов, В. В. Мареев, Е. Н. Станкова. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2004. – 176 с. : ил., табл., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=232995> (дата обращения: 04.12.2022). – ISBN 5-9556-0018-3. – Текст : электронный.
4. Высокопроизводительные вычислительные системы и квантовая обработка информации : учебное пособие : [16+] / В. Ф. Гузик, С. М. Гушанский, Е. В. Ляпунцова, В. С. Потапов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2021. – 202 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=683922> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9275-3787-7. – Текст : электронный.

**Нормативные документы:**

1. Федеральный закон от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации" <http://www.consultant.ru/>
2. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне" <http://www.consultant.ru/>
3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция). <http://www.consultant.ru/>
4. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция). <http://www.consultant.ru/>
5. Трудовой кодекс Российской Федерации; <http://www.consultant.ru/>
6. Постановление Правительства РФ от 14.02.2008 N 71 (ред. от 02.11.2013) "Об утверждении - Типового положения об образовательном учреждении высшего





Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

---

профессионального образования (высшем учебном заведении)". <http://www.garant.ru/>

7. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации <https://fstec.ru/>

8. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации <https://fstec.ru/>

9. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации <https://fstec.ru/>

10. Положение от 27 октября 1995 г. N 199 О сертификации средств защиты информации по требованиям безопасности информации <https://fstec.ru/>

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» <https://uni.ivanovo.ac.ru>

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» [www.biblioclub.ru](http://www.biblioclub.ru)

Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru>

Электронный каталог НБ ИвГУ <http://lib.ivanovo.ac.ru/index.php/ek>

СПС «Консультант Плюс» <http://www.consultant.ru>

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

## **8. Материально-техническое обеспечение практики**

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.



Основная профессиональная образовательная программа  
10.03.01 Информационная безопасность  
(Безопасность компьютерных систем  
(по отрасли или в сфере профессиональной деятельности))

---

**Автор(ы) программы практики:** Агупова Н.С., специалист ЦПС в сфере ИБ и ПД ТСР

Программа рассмотрена и утверждена на заседании ЦПС в сфере ИБ и ПД ТСР

«\_\_\_» \_\_\_\_\_ 20\_\_ г., протокол № \_\_\_\_\_

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_ / Мельникова Е.В.  
(подпись)

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_ / Мельникова Е.В.  
(подпись)

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_ / Мельникова Е.В.  
(подпись)