



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 20 22 г.

Рабочая программа производственной практики, эксплуатационной

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, эксплуатационной является углубление и закрепление знаний и умений, полученных студентом при теоретическом обучении; расширение технического кругозора студента; приобретение студентом навыков работы по специальности; подготовка студента к самостоятельной специальной деятельности.

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

- ознакомление со структурой подразделения, в котором проходит практика, его функциями и связями с другими подразделениями предприятия;
- изучение организации проектных работ;
- приобретение практических навыков на рабочем месте специалиста по защите информации; ознакомление с видами документации, стандартами, нормами и т.п.;
- закрепление знаний и выработка умений по проектированию средств защиты информации, составлению и использованию программного обеспечения и т.п.;
- выработка умений и навыков при работе на автоматизированном рабочем месте;
- выработка навыков творческого подхода к решению теоретических и практических задач по специальности.

2. Вид, тип и основные базы проведения практики

Вид практики – производственная.

Тип практики – эксплуатационная.

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;
- Информационная безопасность организации;
- Защита информации от утечки по техническим каналам;
- Безопасность компьютерных систем и сетей.

Для прохождения практики обучающийся должен:

Знать:

- основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы;
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения;
- современные угрозы сетевой безопасности в корпоративных вычислительных сетях;
- способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации;
- принципы организации информационных систем в соответствии с требованиями по защите



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

информации;

- особенности комплексного подхода к обеспечению информационной безопасности организации;
- методы и стандарты оценки защищенности;
- национальные и международные стандарты в области информационной безопасности;

Уметь:

- использовать СКЗИ для решения задач профессиональной деятельности;
- проводить анализ и оценку защищенности компьютерных сетей;
- администрировать средства защиты информации в компьютерных системах и сетях;
- анализировать и оценивать угрозы информационной безопасности объекта информатизации;
- проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации;
- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- определять политику контроля доступа работников к информации ограниченного доступа;
- формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации;
- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;
- проводить оценку угроз информационной безопасности;
- проводить оценку защищенности компьютерных систем согласно национальным и международным стандартам

Иметь практический опыт/Иметь навыки:

- методами синтеза и анализа криптографических систем и протоколов, закономерностями построения сложных криптосистем;
- навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем документооборота в электронной коммерции;
- выбора средств обеспечения информационной безопасности информационной системы современного предприятия;
- организации защиты информации в локальной сети
- навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами;
- навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами;
- навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий;
- работы с методикой определения структурного построения и состава системы защиты информации и разработкой организационно-нормативных документов, регламентирующих деятельность системы.
- использования нормативные правовые документы в своей профессиональной деятельности;
- обоснования проектных решений по организации и управлению службой защиты информации;
- сбора исходных данных и проведения их анализа для проектирования службы защиты информации;



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

- разработки предложения по совершенствованию системы управления службой защиты информации;
- использования методов изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности службы защиты информации.

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

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов

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

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

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

В результате прохождения практики обучающийся должен:

Знать:

- методы системного анализа;
- методы и средства самостоятельного решения задач в сфере профессиональной деятельности;
- основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности;
- принципы построения и работы, технические возможности и назначение, основные параметры и характеристику типовых электрических цепей, методы их анализа;
- основные принципы и основные этапы математического и имитационного моделирования, подходы к формализации явлений и процессов инфокоммуникационных систем, типовые модели объектов, явлений и процессов инфокоммуникационных систем;



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

- основные уязвимости элементов инфокоммуникационной инфраструктуры и принципы обеспечения ее информационной безопасности;

Уметь:

- применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников;
- определять приоритеты профессиональной деятельности и способы ее совершенствования;
- использовать основные методы правовой оценки различных подходов к решению задач в сфере профессиональной деятельности;
- рассчитывать основные параметры типовых электрических цепей в стационарных и переходных режимах и процессов в них, спектральные и корреляционные характеристики типовых детерминированных сигналов, параметры типовых трасс распространения радиоволн, характеристики типовых антенн, линий питания и отдельных устройств СВЧ;
- проводить измерения в спектральной и временной областях;
- оценивать технические возможности инфокоммуникационных систем и сетей и анализировать угрозы инфокоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности;

Иметь практический опыт/Иметь навыки:

- навыки использования методов поиска, обработки, критического анализа и синтеза информации, методики системного подхода для решения поставленных задач;
- навыки генерирования различных вариантов решения поставленных задач;
- навыки планирования самостоятельной деятельности в решении профессиональных задач;
- навыки разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельности по защите информации;
- навыки использования базовых способов кодирования и декодирования типовых помехоустойчивых кодов и кодов источников информации при решении профессиональных задач;
- навыки разработки моделей и проведения математического и имитационного моделирования типовых объектов, явлений и процессов инфокоммуникационных систем;
- навыки оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов инфокоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности.

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.



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

№ 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. Общее задание Задание №2. Индивидуальное задание	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 8 семестре. Текущий контроль осуществляется в форме руководства выполнения задания по производственной практике.

В ходе выполнения практики каждым обучающимся обязательно заполняется Дневник по 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
1	Качество подобранного материала для проведения анализа (максимум 15 баллов)	
	Наличие источников информации в соответствии с заданием (максимум 5 баллов)	
	Наличие актуальных первичных данных, материалов (максимум 10 баллов)	



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

2	Качественная оценка проведенного анализа собранных материалов (максимум 40 баллов)	
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)	
3	Выполнение общих требований к проведению практики (максимум 25 баллов)	
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)	
4	Защита отчета по практике (максимум 20 баллов)	
	Количество баллов за учебную практику (максимум 100 баллов)	

Обобщенные критерии проверки сформированности компетенции, шкала
оценивания компетенций

100-балльная система оценки	Традиционная (четыребалльная) 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	Компетенции не освоены. Обучающийся не владеет необходимыми знаниями, умениями, навыками или частично показывает знания, умения и



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

		освоены	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 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 ;



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

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 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

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.



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

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,
Зарубин И.А., начальник ЦПС в сфере ИБ и ПД ТСР.

Программа рассмотрена и утверждена на заседании Центра подготовки специалистов в сфере
информационной безопасности и противодействия техническим средствам разведки

« ____ » _____ 20__ г., протокол № ____

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № ____ от « ____ » _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Е.В. Мельникова
(подпись)

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № ____ от « ____ » _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Е.В. Мельникова
(подпись)

Программа обновлена

протокол заседания ЦПС в сфере ИБ и ПД ТСР № ____ от « ____ » _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Е.В. Мельникова
(подпись)