

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Директор института
Высшая школа электроники и
компьютерных наук

20.07.2017 Г. И. Радченко

РАБОЧАЯ ПРОГРАММА
практики
к ОП ВО от 28.06.2017 №007-03-0527

Практика Производственная практика
для специальности 10.05.03 Информационная безопасность автоматизированных систем

Уровень специалист **Тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов

форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.
(ученая степень, ученое звание)

07.07.2017
(подпись)

А. Н. Соколов

Разработчик программы,
к.техн.н., доц., заведующий
кафедрой
(ученая степень, ученое звание,
должность)

07.07.2017
(подпись)

А. Н. Соколов

1. Общая характеристика

Вид практики

Производственная

Способ проведения

Стационарная или выездная

Тип практики

эксплуатационная

Форма проведения

Дискретная

Цель практики

- закрепление и конкретизация результатов теоретического обучения;
- приобретение студентами умений и навыков самостоятельной практической работы в области информационной безопасности и защиты информации;
- получение студентами практических навыков выполнения мероприятий по организационной, правовой и технической защите информации, овладение методами работы с программами, обеспечивающими информационную безопасность;
- развитие у студентов навыков проведения анализа деятельности предприятий и организаций по усовершенствованию их работы с позиции защиты информации;
- всестороннее описание объекта информатизации и проведение исследований на предмет его защищенности с целью применения полученных знаний при подготовке курсовых работ по последующим дисциплинам "Техническая защита информации" и "Программно-аппаратные средства обеспечения информационной безопасности", а также с целью формирования будущей темы выпускной квалификационной работы.

Задачи практики

- изучение функциональной и организационной структуры предприятия;
- ознакомление с комплексом мероприятий по охране труда и технике безопасности;
- ознакомление с должностными инструкциями обслуживающего персонала;
- изучение и анализ принципов организации информационных систем в соответствии с требованиями информационной защищенности;
- освоение методов организации и управления деятельностью служб защиты информации на предприятии;
- освоение технологии проектирования, построения и эксплуатации комплексных систем защиты информации на предприятии;
- освоение современных научных методов исследований уязвимостей и защищенности информационных процессов;
- освоение методик проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- разработка предложений по совершенствованию организации информационных

систем, действующих на предприятии, в соответствии с требованиями информационной защищенности;

- формирование и развитие у студентов профессионально значимых качеств, устойчивого интереса к профессиональной деятельности.

Краткое содержание практики

Ознакомление с профессиональной деятельностью и структурой предприятия. Изучение нормативно-технической документации, должностных инструкций технического персонала, инструкций по охране труда и технике безопасности. Знакомство с правовыми положениями в области информационной безопасности и защиты информации. Изучение современного специализированного программного обеспечения и средств защиты информации объектов информатизации и автоматизированных систем. Изучение и анализ принципов организации информационных систем в соответствии с требованиями информационной защищенности. Участие в решении повседневных практических задач отдела (службы), на который возложены обязанностями по защите информации на предприятии.

2. Компетенции обучающегося, формируемые в результате прохождения практики

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения при прохождении практики (ЗУНы)
ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знать:закономерности, связи и отношения в многомерном творческом пространстве взаимоотношений между коллегами по работе; механизмы и результаты воздействия макро- и микросоциумов на человека, под влиянием которых проходит рабочий процесс.
	Уметь:проводить кооперацию с коллегами по работе с учетом закономерностей и механизмов микро- и микросоциумов.
	Владеть:навыками проявления профессионализма при многомерных взаимоотношениях в коллективе для достижения наилучших результатов трудовой деятельности.
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии.
	Уметь:анализировать правовые акты и осуществлять правовую оценку информации.

	Владеть:навыками применения нормативных правовых актов в профессиональной деятельности.
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Знать:интерфейсы и основные правила настройки существующих программных средств системного, прикладного и специального назначения (по защите информации).
	Уметь:выполнять последовательность работ, связанных с установкой, настройкой и обслуживанием существующих программных средств.
	Владеть:навыками применения программных средств системного, прикладного и специального назначения (по защите информации); навыками освоения новых информационных технологий.
ПК-3 способностью проводить анализ защищенности автоматизированных систем	Знать:место информационной безопасности автоматизированных систем в системе национальной безопасности РФ; риски информационной безопасности и проблемы построения комплексной системы защиты информации на предприятии; важность проведения анализа информационной безопасности объектов информатизации и автоматизированных систем.
	Уметь:выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности.
	Владеть:навыками проведения анализа защищенности объектов информатизации и автоматизированных систем.
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знать:нормативные правовые акты и нормативные методические документы в области политики информационной безопасности предприятия; важность организации всеохватывающей политики информационной безопасности предприятия.
	Уметь:формировать перечень требований по реализации политики информационной безопасности на предприятии.
	Владеть:навыками применения знаний нормативных правовых актов и нормативных методических документов в области информационной безопасности

	для формирования политики информационной безопасности предприятия.
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы.
	Уметь: применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы.
	Владеть: применением инструментов администрирования подсистем информационной безопасности автоматизированной системы.

3. Место практики в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ	Перечень последующих дисциплин, видов работ
Б.1.27 Безопасность сетей электронных вычислительных машин Б.1.28 Безопасность операционных систем Б.1.22 Организация ЭВМ и вычислительных систем Б.1.17 Основы информационной безопасности Б.1.24.02 Правовое обеспечение информационной безопасности	Б.1.24.01 Организационное обеспечение информационной безопасности Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности Б.1.25 Техническая защита информации Производственная практика (8 семестр)

Требования к «входным» знаниям, умениям, навыкам студента, необходимым для прохождения данной практики и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.24.02 Правовое обеспечение информационной безопасности	Знать: правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и

	стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области информационной безопасности. Уметь: применять действующую законодательную базу в области обеспечения информационной безопасности. Владеть: навыками работы с нормативными правовыми актами.
Б.1.28 Безопасность операционных систем	Знать: принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; методы администрирования операционных систем семейств UNIX и Windows. Уметь: формулировать и настраивать политику безопасности операционных систем семейств UNIX и Windows. Владеть: навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.
Б.1.27 Безопасность сетей электронных вычислительных машин	Знать: методы проектирования и администрирования компьютерных сетей. Уметь: проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети. Владеть: навыками эксплуатации и администрирования локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности.
Б.1.17 Основы информационной безопасности	Знать: основные термины по проблематике информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России. Уметь: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. Владеть: профессиональной терминологией в области информационной безопасности.
Б.1.22 Организация ЭВМ и вычислительных систем	Знать: архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем. Уметь: проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем. Владеть: методиками оценки показателей качества и эффективности ЭВМ и

4. Время проведения практики

Время проведения практики (номер уч. недели в соответствии с графиком) с 44 по 47

5. Структура практики

Общая трудоемкость практики составляет зачетных единиц 6, часов 216, недель 4.

№ раздела (этапа)	Наименование разделов (этапов) практики	Кол-во часов	Форма текущего контроля
1	Вводный раздел практики (формирование плана прохождения практики, знакомство с деятельностью и структурой организации (предприятия), изучение нормативно-технической документации и инструкций по технике безопасности).	24	Проверка дневника практики
2	Основной раздел (знакомство со специализированным оборудованием и программным обеспечением, изучение технологических процессов, участие в решении практических задач технического, эксплуатационного или проектного отделов).	168	Проверка дневника практики
3	Подготовка и защита отчета по практике (обработка и систематизация полученных результатов, оформление и защита отчета).	24	Проверка отчета по практике

6. Содержание практики

№ раздела (этапа)	Наименование или краткое содержание вида работ на практике	Кол-во часов
1.1	В начале практики руководитель от предприятия совместно со студентом составляют краткий план прохождения практики с учетом рекомендаций данной программы, профилем и технической оснащенностью предприятия. План прохождения практики согласовывается с руководителем практики от вуза.	4
1.2	Общее знакомство с деятельностью и структурой предприятия.	4
1.3	Вводный инструктаж, ознакомление с режимами работы и условиями труда на предприятии: 1. Изучение вопросов охраны труда на предприятии в целом. 2. Изучение условий труда в подразделении. 3. Выяснение потенциально опасных мест в рабочем помещении. 4. Знакомство с мероприятиями по технике безопасности и индивидуальными защитными средствами.	8
1.4	Изучение должностных инструкций технического персонала.	8
2.1	Знакомство с оборудованием подразделения.	16

2.2	Знакомство с информационной системой предприятия: 1. Познакомиться и записать историю развития предприятия. 2. Составить паспорт предприятия с точки зрения обеспечения информационной безопасности. 3. Познакомиться с информационной системой (ИС) предприятия с целью применения полученных знаний при подготовке курсовой работы по последующей дисциплине "Программно-аппаратные средства обеспечения информационной безопасности": • описать аппаратные средства ИС; • описать программные средства ИС; • выделить и описать элементы ИС, требующие защиты информации и элементы, предназначенные для защиты информации.	40
2.3	Изучение используемого современного программного обеспечения.	32
2.4	Знакомство с системами защиты информации: 1. Познакомиться с предоставленными документами по обеспечению защиты информации. 2. Дать описание основных средств и методов обеспечения защиты информации на предприятии (в учреждении, организации). 3. Составить заключение о степени достаточности мер по обеспечению информационной безопасности предприятия. 4. Собрать информационные материалы для всестороннего описание выбранного объекта информатизации (защищаемого помещения) и проведения исследований на предмет его защищенности с целью применения полученных знаний при подготовке курсовых работ по последующей дисциплине "Техническая защита информации": • дать общее описание предприятия и выбранного объекта информатизации (защищаемого помещения) с точки зрения назначения и выполняемых функций; • нарисовать схему контролируемой зоны предприятия и размещения объекта информатизации (защищаемого помещения); • нарисовать схему организационно-штатной структуры предприятия; • составить перечень сведений, подлежащих защите; • сформулировать цели защиты по категориям каналов утечки информации (ПЭМИН, речевая, видовая информация); • нарисовать схему защищаемого помещения; • описать параметры защищаемого помещения (стены, пол, потолок, окна, двери, предметы мебели, технические средства, инженерные и технические коммуникации); • сформулировать угрозы (воздействия и утечки) и источники угроз (внутренние, внешние, случайные) защищаемой информации.	48
2.5	Участие в практической работе по обеспечению защиты информации: Приобрести практические навыки по настройке и установке	32

	различных видов программных и аппаратных средств защиты информации с учетом политики информационной безопасности предприятия.	
3	Обработка и систематизация полученных результатов, материалов. Оформление и защита отчета о производственной практике.	24

7. Формы отчетности по практике

По окончании практики, студент предоставляет на кафедру пакет документов, который включает в себя:

- дневник прохождения практики, включая индивидуальное задание и характеристику работы практиканта организацией;
- отчет о прохождении практики.

Формы документов утверждены распоряжением заведующего кафедрой от 31.08.2016 №308-03-04.

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Форма итогового контроля – оценка.

8.1. Паспорт фонда оценочных средств

Наименование разделов практики	Код контролируемой компетенции (или ее части)	Вид контроля
Все разделы	ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Проверка дневника прохождения практики
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Проверка дневника прохождения практики
Все разделы	ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Проверка дневника прохождения практики
Все разделы	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Проверка дневника прохождения практики
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Проверка дневника прохождения практики
Все разделы	ПК-3 способностью проводить анализ защищенности автоматизированных	Проверка дневника прохождения практики

	систем	
Все разделы	ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Дифференцированный зачет
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Дифференцированный зачет
Все разделы	ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Дифференцированный зачет
Все разделы	ПК-3 способностью проводить анализ защищенности автоматизированных систем	Дифференцированный зачет
Все разделы	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Дифференцированный зачет
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Дифференцированный зачет

8.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Проверка дневника прохождения практики	В процессе прохождения практики проверяется корректность и полнота заполнения соответствующих разделов дневника.	Зачтено: Дневник прохождения практики корректно заполнен и отражает все разделы практики, приведенные в данной программе. Не зачтено: Дневник прохождения практики заполнен не корректно и/или не отражает какие-либо разделы практики, приведенные в данной программе.
Дифференцированный зачет	К зачету допускаются студенты, представившие заверенные по месту проведения практики Дневник прохождения практики	Отлично: выставляется за полностью раскрытые вопросы на высоком качественном уровне. Хорошо: выставляется в том

	(включающий индивидуальное задание и характеристику работы практиканта организацией) и Отчет о прохождении практики. Зачет проводится в устной форме в виде защиты представленного Отчета о прохождении практики, в ходе которого студент отвечает на поставленные вопросы об особенностях прохождения практики.	случае, если вопросы раскрыты хорошо с достаточной степенью полноты и содержательности. Удовлетворительно: выставляется в том случае, если вопросы раскрыты удовлетворительно, но имеются замечания по полноте и содержанию ответа. Неудовлетворительно: выставляется, если содержание ответов не совпадает с поставленными вопросами или ответ отсутствует.
--	--	--

8.3. Примерный перечень индивидуальных заданий

1. Автоматизированная система в защищенном исполнении организации (или предприятия любой формы собственности).
2. Анализ уязвимостей и организация защиты информации в локальной сети организации (или предприятия любой формы собственности).
3. Анализ уязвимостей и эффективности средств и способов защиты информации в автоматизированной системе предприятия или организации (любой формы собственности).
4. Инструментальный мониторинг защищенности автоматизированной системы предприятия (любой формы собственности).
5. Информационная система персональных данных организации (или предприятия любой формы собственности).
6. Комплексная защита информации в локальной сети организации (или предприятия любой формы собственности).
7. Подготовка к аттестации информационной системы персональных данных в организации (или предприятии любой формы собственности).
8. Сбор и анализ исходных данных для проектирования системы защиты информации организации (или предприятия любой формы собственности).
9. Система контроля и управления доступом на предприятии (любой формы собственности).
10. Система управления информационной безопасностью автоматизированной системы организации (или предприятия любой формы собственности).

9. Учебно-методическое и информационное обеспечение практики

Печатная учебно-методическая документация

а) основная литература:

1. Северин, В. А. Правовая защита информации в коммерческих организациях [Текст] учеб. пособие для вузов по специальности "Юриспруденция" В. А. Северин; под ред. Б. И. Пугинского. - М.: Академия, 2009. - 219, [1] с.
2. Защита информации [Текст] учеб. пособие по направлению 210700 "Инфокоммуникац. технологии и системы связи" А. П. Жук и др. - 2-е изд. - М.: РИОР : ИНФРА-М, 2015. - 391, [1] с.
3. Баранова, Е. К. Информационная безопасность и защита информации [Текст] учеб. пособие по направлению "Приклад. информатика" Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М.: РИОР : ИНФРА-М, 2016. - 320, [1] с. ил.

б) дополнительная литература:

1. ГОСТ Р 50922-2006 : Защита информации. Основные термины и определения : утв. и введ. в действие 27.12.06 : взамен ГОСТ Р 50922-96 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2008. - 7 с.
2. ГОСТ Р 51275-2006 : Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения : утв. и введ. в действие от 27.12.06 : взамен ГОСТ Р 51275-99 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2007. - 7 с.
3. ГОСТ Р 53112-2008 : Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний : утв. и введ. в действие от 18.12.08 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2009. - 21 с.
4. ГОСТ Р 53114-2008 : Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения : утв. и введ. в действие от 18.12.08 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2009. - 15 с.

из них методические указания для самостоятельной работы студента:

1. Форма дневника прохождения практики
2. Форма отчета о прохождении практики

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Киселева, Э.М. Методические рекомендации по организации и проведению производственной практики	Электронно-библиотечная система	Интернет / Авторизованный

		студентов бакалавриата. [Электронный ресурс] / Э.М. Киселева, Г.А. Костецкая, Р.И. Попова. — Электрон. дан. — СПб. : РГПУ им. А. И. Герцена, 2014. — 56 с.	Издательства Лань	
2	Основная литература	Шаньгин, В.Ф. Защита компьютерной информации. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2010. — 544 с.	Электронно-библиотечная система Издательства Лань	Интернет / Авторизованный

10. Информационные технологии, используемые при проведении практики

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. Microsoft-Windows(бессрочно)

Перечень используемых информационных справочных систем:

1. -Стандартинформ(бессрочно)
2. -Консультант Плюс(31.07.2017)
3. -Гарант(31.12.2017)

11. Материально-техническое обеспечение практики

Место прохождения практики	Адрес места прохождения	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, обеспечивающие прохождение практики
ФГУП "Приборостроительный завод", г.Трехгорный	456080, г. Трехгорный, ул. Заречная, 13	Стенды для отладки и испытаний микроэлектронного оборудования, серверы, ЛВС
ООО "Стратегия безопасности"	454052, г.Челябинск, ул. Пети Калмыкова, д.11-А	Программно-аппаратные комплексы по защите информации и оценке защищенности объектов информатизации.
АО "Челябинский радиозавод "Полет"	454080, Челябинск, ул. Тернопольская, 6	Стенды для отладки и испытаний микроэлектронного оборудования, серверы, ЛВС, средства доступа к глобальной сети