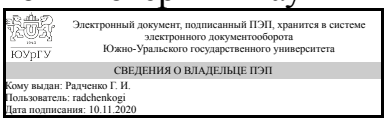
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Директор института
Высшая школа электроники и компьютерных наук



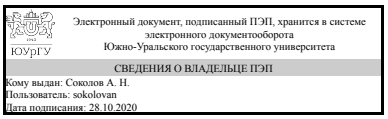
Г. И. Радченко

РАБОЧАЯ ПРОГРАММА
практики
к ОП ВО от 26.06.2019 №084-2481

Практика Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности
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

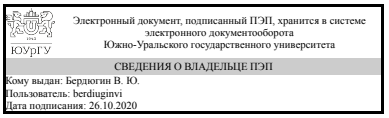
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
доцент



В. Ю. Бердюгин

Челябинск

1. Общая характеристика

Вид практики

Производственная

Способ проведения

Стационарная или выездная

Тип практики

практика по получению профессиональных умений и опыта профессиональной деятельности

Форма проведения

Дискретно по видам практик

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;
- формирование 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 деятельности 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.

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)
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-5 способностью проводить анализ рисков информационной безопасности	Знать:место анализа рисков в общей системе обеспечения информационной

автоматизированной системы	безопасности.
	Уметь:определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.
	Владеть:методами выявления угроз информационной безопасности информационных систем.
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	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-28 способностью управлять информационной безопасностью автоматизированной системы	Знать:основные методы управления информационной безопасностью.
	Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
	Владеть:методами управления информационной безопасностью автоматизированных систем.

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.1.37 Комплексное обеспечение защиты информации объекта информатизации Б.1.24.02 Правовое обеспечение информационной безопасности Б.1.28 Безопасность операционных систем	В.1.08 Основы аттестации объектов информатизации критически важных объектов В.1.09 Обеспечение информационной безопасности на критически важных объектах Б.1.43 Аудит информационной безопасности

Б.1.30.01 Разработка защищенных автоматизированных систем Б.1.24.01 Организационное обеспечение информационной безопасности Б.1.25 Техническая защита информации Производственная практика, эксплуатационная практика (6 семестр)	Б.1.30.02 Эксплуатация защищенных автоматизированных систем Производственная практика, преддипломная практика (10 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.1.24.01 Организационное обеспечение информационной безопасности	Знать: источники и классификацию угроз информационной безопасности; основы организационного обеспечения информационной безопасности. Уметь: разрабатывать технические задания на создание подсистем информационной

	безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов. Владеть: методами формирования требований по защите информации.
Б.1.37 Комплексное обеспечение защиты информации объекта информатизации	Знать: принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; выявлять уязвимости информационно-технологических ресурсов информационных систем. Владеть: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами выявления угроз информационной безопасности информационных систем.
Б.1.25 Техническая защита информации	Знать: технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации. Уметь: анализировать и оценивать угрозы информационной безопасности объекта. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам.
Б.1.30.01 Разработка защищенных автоматизированных систем	Знать: методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Уметь: исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. Владеть: методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.
Производственная практика, эксплуатационная практика (6 семестр)	Наличие у студента профессионально значимых качеств, устойчивого интереса к профессиональной деятельности.

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 организацией и ее информационной системой: 1. Познакомиться и записать историю развития предприятия. 2. Составить паспорт предприятия с точки зрения обеспечения информационной безопасности. 3. Познакомиться с информационной системой (ИС) предприятия: • описать аппаратные средства ИС; • описать программные средства ИС; • выделить и описать элементы ИС, требующие защиты информации и элементы, предназначенные для защиты	40

	информации.	
2.3	Изучение используемого современного программного обеспечения.	16
2.4	Анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности: - автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите; - информационных технологий, формирующих информационную инфраструктуру предприятия (организации) в условиях существования угроз в информационной сфере и задействующих информационно-технологические ресурсы, подлежащие защите; - технологий обеспечения информационной безопасности автоматизированных систем; - систем управления информационной безопасностью автоматизированных систем. Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования: 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 описания выбранного объекта проектирования и проведения исследований на предмет его защищенности: • дать общее описание предприятия и выбранного объекта проектирования 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 угрозы (воздействия и утечки) и источники угроз (внутренние, внешние, случайные) защищаемой информации; • сформулировать цели защиты по категориям каналов утечки информации (ПЭМИН, речевая, видовая информация, НСД).	64
2.5	Участие в практической работе по обеспечению защиты информации: 1. Приобрести практические навыки по настройке и установке различных видов программных и аппаратных средств защиты информации с учетом политики информационной безопасности предприятия. 2. Собрать материалы для подготовки выпускной квалификационной работы.	32
3	Обработка и систематизация полученных результатов, материалов.	24

	Оформление и защита отчета о производственной практике.	

7. Формы отчетности по практике

По окончанию 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 – дифференцированный зачет.

8.1. Паспорт фонда оценочных средств

Наименование разделов практики	Код контролируемой компетенции (или ее части)	Вид контроля
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-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Проверка дневника прохождения практики
Все разделы	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Проверка дневника прохождения практики
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Проверка дневника прохождения практики
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Проверка отчета по практике
Все разделы	ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Проверка отчета по практике
Все разделы	ПК-5 способностью проводить анализ	Проверка отчета по

	рисков информационной безопасности автоматизированной системы	практике
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Проверка отчета по практике
Все разделы	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Проверка отчета по практике
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-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Дифференцированный зачет
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Дифференцированный зачет
Все разделы	ПК-28 способностью управлять информационной безопасностью 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 (всего три проверки). При оценивании используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания. При условии корректного и полного заполнения 1 раздела дневника обучающему начисляется 1 балл. При условии корректного и полного заполнения 1 и 2 разделов дневника	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 % Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %

	- 3 балла. При условии корректного и полного заполнения 1, 2 и 3 разделов дневника - 6 баллов. Максимальное количество баллов - 6. Весовой коэффициент - 1	
Проверка отчета по практике	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания. 3 балла – отчет содержит логичное, последовательное изложение материала с соответствующими выводами и обоснованными положениями; 2 балла – отчет содержит в целом грамотно изложенную теоретическую главу, однако с не вполне обоснованными выводами; 1 балл – документ базируется на практическом материале, но имеет поверхностный анализ, просматривается непоследовательность изложения материала, представлены необоснованные выводы. Максимальное количество баллов - 3. Весовой коэффициент - 2.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %
Дифференцированный зачет	К зачету допускаются студенты, представившие заверенные по месту проведения практики Дневник прохождения практики (включающий индивидуальное задание и характеристику работы практиканта организацией) и Отчет о прохождении практики. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Зачет проводится в устной	Отлично: величина рейтинга обучающегося 85…100 %. Хорошо: величина рейтинга обучающегося 75…84 %. Удовлетворительно: величина рейтинга обучающегося 60…74 %. Неудовлетворительно: величина рейтинга обучающегося 0…59 %.

	форме в виде защиты представленного Отчета о прохождении практики, в ходе которого студент отвечает на поставленные вопросы об особенностях прохождения практики. Показатели оценивания. Своевременность представления документов: 3 балла - документы представлены в установленные сроки; 2 - балла документы представлены в течение недели после установленного срока; 1 балл - срок задержки представления документов более одной недели. Характеристика работы практиканта организацией: 3 балла - замечаний по прохождению студентом практики не имеется; 2 балла - по прохождению практики имеются замечания непринципиального характера; 1 балл - в характеристике имеются замечания принципиального характер в отношении личных и деловых качеств студента. Защита отчета: 3 балла - при защите студент показывает глубокое знание вопросов, изученных в соответствии с заданием на практику, свободно оперирует данными, уверенно отвечает на вопросы об особенностях прохождения практики; 2 балла – при защите студент в целом показывает знание проблематики практики, однако не вполне уверенно отвечает на дополнительные вопросы; 1 балл – при защите студент проявляет неуверенность, показывает слабое знание объекта прохождения практики. Максимальное количество баллов – 9.	

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. Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия

б) дополнительная литература:

1. Микрюков, В. Ю. Безопасность жизнедеятельности [Текст] учебник для вузов В. Ю. Микрюков. - М.: КноРус, 2016

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 студентов бакалавриата. [Электронный ресурс] / Э.М. Киселева, Г.А. Костецкая, Р.И. Попова. — Электрон. дан. — СПб. : РГПУ им. А. И. Герцена, 2014. — 56 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
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. ООО "ГарантУралСервис"-Гарант(бессрочно)

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