

Методические рекомендации

по организации и проведению учебной практике «эксплуатационная практика»

для студентов направления подготовки /специальности

10.03.01 Информационная безопасность

шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Пятигорск, 2021 г.

Содержание

<u>Введение</u>	4
Цели учебной практики студентов	4
Задачи учебной практики	4
Место учебной практики в структуре ООП бакалавриата	4
Формы проведения учебной практики	5
Место и время проведения учебной практики	5
Компетенции обучающегося, формируемые в результате прохождения учебной практики	5
Структура и содержание учебной практики	7
Образовательные, научно-исследовательские и научно-производственные технологии, используемые на учебной практик	7
Учебно-методическое обеспечение самостоятельной работы студентов на учебной практике	7
Теоретические задания	8
Индивидуальные задания	8
Формы промежуточной аттестации (по итогам учебной практики)	9
Учебно-методическое и информационное обеспечение учебной практики	10
Материально-техническое обеспечение учебной практики	11

Введение

Методические указания по организации эксплуатационной практики разработаны в соответствии с требованиями ФГОС ВО с учетом рекомендаций ОП по направлению и профилю подготовки 10.03.01 «Информационная безопасность», «Положением о порядке проведения практики студентов» и учебным планом направления 10.03.01 «Информационная безопасность».

Методические указания по организации эксплуатационной практики предназначены для студентов всех форм обучения направления подготовки бакалавров 10.03.01 «Информационная безопасность» и содержат материалы по организации, проведению и контролю прохождения практики, примерному распределению времени в период практики; указывают обязанности студентов, ставят задачи практики, содержат индивидуальные и теоретические задания и требования к оформлению результатов производственной практики.

Эксплуатационная практика студентов является составной частью основной образовательной программы высшего профессионального образования подготовки высококвалифицированных специалистов, представляет собой вид занятий, непосредственно ориентированных на практическую подготовку обучающихся.

1. Цели практики

Целями эксплуатационной практики являются закрепление и углубление знаний, полученных студентами в процессе теоретического обучения, приобретение необходимых умений, навыков, компетенций и опыта практической работы по изучаемому направлению.

2. Задачи практики

Задачами Эксплуатационной практики являются:

- получения практических навыков самостоятельной и коллективной работы при решении поставленных задач;
- углубленное изучение и приобретение практических навыков в работе над защитой информации в условиях реального предприятия;
- приобретение и закрепление практических навыков работы с системами защиты персональных данных, защиты электронного документооборота, разработка документации политики безопасности предприятия
- разработка моделей угроз для предприятия.

3. Место практики в структуре образовательной программы

Эксплуатационная практика непосредственно ориентирована на профессионально-практическую подготовку обучающихся. Эксплуатационная практика базируется на освоении таких дисциплин как «Организационное и правовое обеспечение информационной безопасности», «Научно-исследовательская работа», «Управление проектами по защите информации и экономика защиты информации», «Разработка и эксплуатация защищенных автоматизированных информационных систем».

Эксплуатационная практика является одним из основных видов профильной подготовки студентов и представляет собой комплексные практические занятия, дополненные другими формами участия в работе предприятия, в ходе которых происходит ознакомление с приборами, программным обеспечением и другими технологиями в области защиты информации и дальнейшее формирование профессиональных знаний.

Для успешного прохождения учебной практики студент должен обладать «входными» знаниями, умениями и готовностями, приобретенными в результате освоения предшествующих частей ОП, а именно:

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;
- способы и средства документирования, классификацию типов носителей документной информации;
- структуру документов и нормативные требования к составлению и оформлению управленческих и научно – технических документов
- Место и роль информационной безопасности в системе национальной безопасности РФ;
- Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;
- Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- Принципы и методы организационной защиты информации;
- Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам;
- Принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

уметь:

- формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- пользоваться нормативными документами по защите информации;
- организовывать работу с управленческой (деловой) и научно-технической документацией;
- составлять документы на любом носителе;
- Формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств;
- Пользоваться нормативными документами по защите информации.

владеть:

- навыками работы с нормативными правовыми актами;
- способностью к разработке проектной и рабочей технической документации, оформлению законченных проектно-конструкторских работ в соответствии с нормами и стандартами;
- готовностью к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам;
- Методикой анализа результатов работы средств обнаружения вторжений;
- Навыками выявления и уничтожения компьютерных вирусов;
- Навыками разработки должностных инструкций в сфере защиты информации;
- Навыками разработки моделей угроз и моделей нарушителя.

4. Формы проведения практики

Эксплуатационная практика проводится в форме:

- консультативных занятий;
- работы на предприятии в должности практиканта или иной должности согласно договору предприятия с вузом;
- практической отработки перечня вопросов, рекомендуемых кафедрой и программой;
- работы на оборудовании предприятия.

5. Место и время проведения практики

Эксплуатационная практика проводится на четвертом курсе во 2 семестре продолжительностью две недели. Эксплуатационная практика проводится на рабочем месте на предприятии, оснащенном современным технологическим оборудованием и программным обеспечением в сфере защиты информации.

6. Компетенции обучающегося, формируемые при прохождении практики

6.1 Наименование компетенции

Индекс	Формулировка:
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

7. Структура и содержание учебной практики

Общая трудоемкость производственной эксплуатационной практики составляет 3 зачетных единиц - 81 часов.

№ п/п	Разделы (этапы) практики	Виды учебной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Лекции	Лаб. работы	Практ. занятия	Сам. работа	
1	Подготовительный этап (инструктаж по технике безопасности)				10	Устный отчет
2	Производственный этап: 1. Анализ деятельности предприятия, его структуры, бизнес-процессов; 2. Исследование средств защиты информации на предприятии и возможностей разработки и внедрения дополнительных систем защиты информации для конкретных предприятий – мест прохождения практики.				10 10	Письменн ый отчет Письменн ый отчет
	3. Проработка индивидуального теоретического задания по вариантам				20	Письменны й отчет
	Решение индивидуального практического задания по вариантам				20	Письменны й отчет
	5. Подготовка и оформление отчета				21	

3	Заключительный этап (защита отчета)					Защита отчета по практике
	Итого				81	

8. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на производственной практике

В процессе прохождения производственной практики используются интерактивные методы и технологии, которые формируют общекультурные компетенции у студентов за счет:

- консультаций с применением дистанционных и мультимедийных технологий;
- исследовательская работа на производстве под руководством сотрудника предприятия;
- самостоятельных работ с использованием ПК и современного оборудования и программного обеспечения на предприятии.

9. Учебно-методическое обеспечение самостоятельной работы студентов на производственной практике

За две недели до начала практики руководитель практики от университета проводит со студентами организационное собрание, на котором обеспечивает их программой и методическими указаниями по организации учебной практики, а также бланками предписаний на практику. Всем практикантам выдаются теоретические и индивидуальные задания.

9.1 Теоретические задания

Задание на производственную эксплуатационную практику включает проработку теоретического вопроса и написание по нему обзорного реферата, включаемого в отчет по практике (теоретическая часть).

Варианты заданий:

1. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных.
2. Основные положения ФЗ № 152 «О персональных данных».
3. Основные положения Постановления № 1119 «Об утверждении порядка требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Обеспечение контроля и надзора за выполнением требований по защите ПДн. Виды предусмотренных законодательством проверок.
5. Перечень нормативно-правовых актов, регламентирующих порядок наказаний за нарушение правил обработки персональных данных.
6. Типы информационных систем персональных данных
7. Порядок определения наличия недеklarированных возможностей в системной и прикладном ПО
8. Определения уровня защищенности ИСПДн
9. Методика определения актуальных угроз безопасности ИСПДн.
10. Модель угроз безопасности ИСПДн. Модель нарушителя.
11. Выполнение мер по защите информационных систем персональных данных в соответствии с приказом №21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. Перечень организационно-распорядительных документов, регламентирующих защиту ПДн и ИСПДн на объекте.
13. Перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации.
14. Создания компьютерной системы с учетом обеспечения информационной безопасности;
15. Человеческий фактор и модель нарушителя безопасности информации
16. Понятие и сущность политики безопасности и модели безопасности;
17. Виды и характеристики моделей безопасности компьютерных систем;
18. Применение и показатели защищенности межсетевых экранов
19. Применение «Общих критериев» при оценке защищенных систем 14
20. Построение парольных систем. Угрозы безопасности парольных систем
21. Разновидности способов аутентификации

9.1 Индивидуальные задания

Т.к. эксплуатационная практика является предшествующей для преддипломной практики и работе над ВКР, то на учебной практике студенту предоставляется возможность ознакомления с техническими характеристиками, особенностями работы технических средств защиты и специальным программным обеспечением.

Варианты заданий:

1. Разработка системы защиты персональных данных предприятия.
2. Разработка подсистемы программно-аппаратной защиты информации для КСЗИ ЛВС малого коммерческого предприятия».

3. Проект по совершенствованию системы защищенного электронного документооборота в организации при использовании «облачных» технологий.
4. Совершенствование методики управления инцидентами в проектных решениях, вырабатываемых на предприятии.
5. Совершенствование методики управления информационными рисками при реализации проектных решений на предприятии.
6. Разработка проекта системы ЗИ для распределенной вычислительной сети в учреждении здравоохранения.
7. Разработка усовершенствованной подсистемы СКУД типового предприятия.
8. Проектирование системы ИТЗИ кабинета руководителя среднего госпредприятия.
9. Анализ существующей системы ИТЗИ кабинета руководителя госпредприятия.
10. Организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации.
11. Оценка эффективности предлагаемой системы инженерно-технической защиты кабинета руководителя госпредприятия.
12. Разработка автоматизированной системы аудита защиты персональных данных высшего учебного учреждения.
13. Разработать перечень мероприятий по устранению выявленных недостатков подсистемы компьютерной безопасности предприятия.
14. Разработка подсистемы компьютерной безопасности для малого коммерческого предприятия.
15. Проект по совершенствованию системы программно-аппаратной защиты информации автоматизированного рабочего места сотрудника предприятия.
16. Разработка проекта подсистемы сетевого аудита информационной безопасности основных компонентов ЛВС крупного промышленного предприятия.
17. Разработка проекта подсистемы защиты персональных данных в информационной системе высшего учебного заведения.
18. Разработка модели нарушителя и модели угроз для малого коммерческого предприятия.
19. Разработка модели нарушителя и модели угроз для предприятия малого бизнеса.
20. Разработка модели нарушителя и модели угроз для госпредприятия.

10. Формы промежуточной аттестации (по итогам учебной практики)

Аттестация по итогам эксплуатационной практики производится в 8 семестре и заключается в защите составленного обучающимся отчета по практике.

В процессе практики текущий контроль за работой студентов, в том числе самостоятельной, осуществляется руководителям практики в рамках консультаций и проверки выполненного теоретического и индивидуального заданий в соответствии с методическими указаниями по организации учебной практики студентов.

По окончании практики студент-практикант составляет письменный отчет и сдает его руководителю практики от университета одновременно с бланками предписаний на практику, подписанными непосредственным руководителем практики. Бланки предписаний на практику - официальный документ, удостоверяющий прохождение студентом практики согласно утвержденному календарному плану (графику). Бланки предписаний на практику наравне с отчетом о прохождении практики является основным документом, по которому студент отчитывается о выполнении программы. Во время практики студент должен ежедневно кратко и аккуратно документировать в бланках все, что им проделано за день по выполнению программы и индивидуальных заданий. По окончании практики заполненные бланки предоставляются руководителю практики. Руководитель практики дает краткое заключение о качестве работы студента за каждый день (или определенный период).

Отчет о практике должен содержать сведения о конкретно выполненной студентом работе в период практики, а также краткое описание выполненной работы, выводы и предложения. В отчет должен быть включен специальный раздел об итогах выполнения студентами индивидуального и теоретического задания на практике.

Оформление, структура и содержание отчета по практике. Отчет - итоговый документ, на основании которого и после его защиты студент получает зачет по практике.

Оформление отчета по учебной практике следует производить согласно методическим указаниям «Методические указания по оформлению отчетов по практике, рефератов, курсовых и дипломных работ/проектов».

Объем отчета вместе с приложениями – 15-25 страниц формата А4. Он должен быть изложен грамотно, аккуратно оформлен, напечатан с помощью компьютера.

Структурно отчет содержит следующие элементы: титульный лист, введение, основная часть (перечень разделов), заключение, список использованных источников, приложения.

Во введении необходимо рассмотреть актуальность применения новых, перспективных средств защиты информации, определить цели и задачи эксплуатационной практики, а также структуру отчета.

Основная часть должна состоять из трех разделов:

1. Анализ деятельности предприятия, его обеспечения в сфере защиты информации.
2. Теоретическая часть (реферативное изложение теоретического задания);
3. Практическая часть (описание выполнения индивидуального задания).

При написании теоретической части необходимо пользоваться рекомендованной литературой.

В заключительной части отчета студенту рекомендуется, проанализировав положительный опыт, полученный в результате прохождения практики, сделать критические замечания. Замечания должны носить конструктивный характер.

Защита студентами отчетов по практике осуществляется в комиссии в течение 3-х дней после окончания практики или в установленные кафедрой и институтом сроки. По итогам аттестации (защиты отчета) выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно). Студенты, не выполнившие программу практик по уважительной причине, направляются на практику вторично, в свободное от учебы время.

Студенты, не выполнившие программу практик без уважительной причины или получившие отрицательную оценку, могут быть отчислены из университета как имеющие академическую задолженность в порядке, предусмотренном Уставом вуза.

11. Учебно-методическое и информационное обеспечение учебной практики

Перечень основной литературы:

1. Чернышев, А. Б. (Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске). Теория информационных процессов и систем : учеб. пособие / А.Б. Чернышев, В.Ф. Антонов, Г.Б. Суюнова ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 169 с..
2. Кочетков М.В. Системы охраны [Электронный ресурс]: учебное пособие/ Кочетков М.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2015.— 99 с.— Режим доступа: <http://www.iprbookshop.ru/29284>.— ЭБС «IPRbooks», по паролю.

Перечень дополнительной литературы

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. – М.: ИНФРА-М, 2012.
2. Федотов Е.А. Администрирование программных и информационных систем [Электронный ресурс]: учебное пособие/ Федотов Е.А.— Электрон. текстовые данные.— Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012.— 136 с.— Режим доступа: <http://www.iprbookshop.ru/27280>.— ЭБС «IPRbooks», по паролю.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по практике:

1. Методические указания по организации и проведению эксплуатационной практики для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. <http://elibrary.ru> - Научная электронная библиотека eLIBRARY.RU

2. <http://www.biblioclub.ru> - Университетская библиотека online

12. Материально-техническое обеспечение учебной практики

Определяется структурой места прохождения практики, если практика проходит на кафедре ВУЗа используется следующее материально-техническое обеспечение:

- переносной проектор Acer PO100 экран LUMA 1300, ноутбук (1 шт) Asus K50I T44002.2/3072/GT320M/250/5400/DVD-RW, наборы демонстрационного оборудования и учебно-наглядных пособий.
- специализированная учебная мебель и технические средства обучения, служащие для представления учебной информации: компьютеры с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду, книжные шкафы для учебной литературы и учебно-методических материалов