

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Пятигорский институт (филиал) СКФУ

Методические рекомендации

по организации и проведению производственной практики
Технологическая (проектно-технологическая) практика
Для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Пятигорск, 2021 г.

Оглавление

Введение.....	3
1. Цели практики.....	3
2. Задачи практики.....	3
3. Место практики в структуре образовательной программы.....	3
4. Формы проведения практики.....	4
5. Место и время проведения практики.....	5
6. Компетенции обучающегося, формируемые при прохождении практики.....	5
7. Структура и содержание учебной практики.....	5
8. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на производственной технологической практике.....	6
9. Учебно-методическое обеспечение самостоятельной работы студентов на технологической практике.....	6
9.1 Теоретические задания.....	6
9.2 Индивидуальные задания.....	7
10. Формы промежуточной аттестации (по итогам учебной исследовательской практики).....	8
11. Учебно-методическое и информационное обеспечение учебной практики.....	9
12. Материально-техническое обеспечение учебной практики.....	9

Введение

Методические указания по организации технологической 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 производственной 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 технологической практики.

Производственная 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

Целью производственной технологической 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 технологической практики является:

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

3. Место практики в структуре образовательной программы

Технологическая практика непосредственно ориентирована на профессионально-практическую подготовку обучающихся. Технологическая практика базируется на освоении таких дисциплин как «Методы и средства криптографической защиты информации», «Техническая защита информации», «Защита информации от утечки по техническим каналам».

Технологическая практика является одним из основных видов профильной подготовки студентов и представляет собой комплексные практические занятия, дополненные другими видами учебного процесса, в ходе которых происходит ознакомление с устройствами и программным обеспечением в области защиты информации и дальнейшее формирование профессиональных знаний.

Для успешного прохождения учебной технологической 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;

- технологии обнаружения компьютерных атак и их возможности;
- средства реализации атак.
- механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
- атаки на сетевые службы.
- атаки с использованием промежуточных узлов и территорий.
- основные уязвимости и типовые атаки на современные компьютерные системы;
- возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;
- методы защиты компьютерных сетей;
- классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты информации современными программно-аппаратными средствами..

уметь:

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

владеть:

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

4. Формы проведения практики

Технологическая практика проводится в форме:

- консультативных занятий;
- практической отработки перечня вопросов, рекомендуемых кафедрой и программой;
- работы на компьютерах и оборудовании, предоставляемом предприятием.

5. Место и время проведения практики

Производственная технологическая практика проводится на первом курсе в 6 семестре продолжительностью две недели. Производственная технологическая практика проводится на предприятиях профиля данной специальности, оснащенных современным технологическим оборудованием и компьютерной техникой.

6. Компетенции обучающегося, формируемые при прохождении практики

6.1 Наименование компетенции

Индекс	Формулировка:
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

7. Структура и содержание учебной практики

Общая трудоемкость учебной 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 сетевого оборудования, операционных систем специального программного обеспечения, используемого на предприятии, должностных инструкций и документации в сфере защиты информации.				10	Письменный отчет
					10	Письменный отчет
	3. Проработка индивидуального теоретического задания по вариантам				20	Письменный отчет
	Решение индивидуального практического задания по вариантам				20	Письменный 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 технологической практике.

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

- консультаций с применением мультимедийных технологий;
- самостоятельных работ с использованием ПК и современного оборудования на предприятии.

9. Учебно-методическое обеспечение самостоятельной работы студентов на технологической 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 производственной практики, а также бланками предписаний на практику. Всем практикантам выдаются теоретические и индивидуальные задания.

9.1 Теоретические задания

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

Варианты заданий:

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.

5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows 7.
6. Защита рабочих станций с использованием персональных сетевых фильтров.
7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
11. Преимущества технологии терминального доступа. Обеспечение безопасности.
12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
14. Система единого входа в сеть на основе протокола Kerberos.
15. Создание единого пространства безопасности на базе Active Directory.
16. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
17. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки.
18. Применение инструментальных средств аудита безопасности компьютерных систем.
19. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности.
20. Методика проведения инструментальных проверок.
21. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

9.2 Индивидуальные задания

Т.к. производственная технологическая практика является предшествующей для таких дисциплин как «Управление проектами по защите информации и экономика защиты информации», «Комплексная система защиты информации на предприятии», «Разработка и эксплуатация защищенных автоматизированных информационных систем, то на технологической практике студенту предоставляется возможность ознакомления с техническими характеристиками, особенностями работы технических и программных средств защиты информации на конкретном предприятии.

Варианты заданий:

1. Внедрение системы криптографической защиты КриптоПро на предприятии
2. Внедрение системы криптографической защиты Secret Disk Enterprise на предприятии
3. Внедрение системы криптографической защиты CipherTrust Data Security Platform на предприятии
4. Внедрение системы криптографической защиты КриптоАРМ на предприятии
5. Внедрение системы криптографической защиты Fin-TrusT на предприятии
6. Внедрение системы криптографической защиты ViPNet L2-10G на предприятии
7. Внедрение системы криптографической защиты Dcrypt XG на предприятии
8. Внедрение системы криптографической защиты «Палиндром» на предприятии
9. Внедрение системы криптографической защиты ViPNet Coordinator KB 4 на предприятии
10. Внедрение системы криптографической защиты С-Терра Юнит на предприятии
11. Внедрение системы криптографической защиты КриптоПро Архив на предприятии
12. Внедрение межсетевого экрана МЭ «Блокпост-Экран 2000/XP» на предприятии
13. Внедрение межсетевого экрана TrustAccess на предприятии
14. Внедрение межсетевого экрана TrustAccess-S на предприятии
15. Внедрение межсетевого экрана StoneGate Firewall на предприятии
16. Внедрение программного комплекса Сервер безопасности CSP VPN Server на предприятии
17. Внедрение программного комплекса Шлюз безопасности CSP VPN Gate на предприятии
18. Внедрение программного комплекса Клиент безопасности CSP VPN Client на предприятии

19. Внедрение межсетевого экрана Idecso ICS 3 на предприятии

20. Внедрение программного комплекса Трафик Инспектор 3.0 на предприятии

10. Формы промежуточной аттестации (по итогам учебной исследовательской практики)

Аттестация по итогам производственной технологической практики производится в 6 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 от предприятия, а также руководителем от вуза в рамках консультаций и проверки выполненного теоретического и индивидуального заданий в соответствии с методическими указаниями по организации производственной 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 производственной 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 учебной практики, а также структуру отчета.

Основная часть должна состоять из трех разделов:

Анализ деятельности предприятия и средств защиты информации, которые используются в ходе его работы.

Теоретическая часть (реферативное изложение теоретического задания);

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. Леонова О.В. Основы научных исследований [Электронный ресурс]: учебное пособие/ Леонова О.В.— Электрон. текстовые данные.— М.: Московская государственная академия водного транспорта, 2015.— 70 с.— Режим доступа: <http://www.iprbookshop.ru/46493>.— ЭБС «IPRbooks», по паролю.
2. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон.текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
3. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
4. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
5. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

Перечень дополнительной литературы:

1. Лонцева И.А. Основы научных исследований [Электронный ресурс]: учебное пособие/ Лонцева И.А., Лазарев В.И.— Электрон. текстовые данные.— Благовещенск: Дальневосточный государственный аграрный университет, 2015.— 185 с.— Режим доступа: <http://www.iprbookshop.ru/55906>.— ЭБС «IPRbooks», по паролю.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. : [учебник] / В.Г. Олифер, Н.А. Олифер. - 4-е изд. - СПб. : Питер, 2011. - 944 с.
3. Таненбаум, Э. Компьютерные сети : [учеб. пособие] / Э. Таненбаум ; пер. с англ. В. Шрага. - 4-е изд. - СПб. : Питер, 2007. - 992 с. .
4. Сети и телекоммуникации : учеб.пособие / Б.В. Соболев, А.А. Манин, М.С. Герасименко. - Ростов н/Д : Феникс, 2015. - 191 с. .
5. Галицкий, А. В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. - М. : ДМК Пресс, 2004. - 616 с.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по практике:

1. Методические указания по организации и проведению учебной практики – «Технологическая практика» для студентов направления 10.03.01 «Информационная безопасность».
2. Инструкции по технике безопасности и охране труда при работе на предприятии, где проходит практика.
3. Методические рекомендации для оформления рефератов, отчетов по практике, курсовых работ/проектов, выпускных квалификационных работ Пятигорск: 2015 г. – 20 с.

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

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