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 – «Эксплуатационная практика»
для студентов направления подготовки /специальности
10.04.01 «Информационная безопасность»

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Содержание

1 Общие положения

Отчет по практике выполняется на персональном компьютере и должен содержать диск с выполненной работой и распечатку, содержащую части работы, записанные на диске:

Теоретическая часть:

Раскрытие теоретической темы работы, объем ориентировочно 10-15 страниц, (план, введение, основная часть, состоящая из нескольких разделов с подразделами, заключение с анализом и основными выводами, список использованной литературы (литература не старше 5 лет)).

Тема выбирается студентом индивидуально из примерной тематики теоретических заданий и согласуется с преподавателем, также студентом может быть предложена своя индивидуальная тема также согласуемая с преподавателем.

Практическая часть:

Результат решения практических заданий индивидуальное задание выдается руководителем практики

Отчет по практике выполняется на персональном компьютере на стандартных листах белой бумаги формата А4 (размером 210/297). Текст печатается на одной стороне листа с соблюдением размеров полей: слева – 30 мм; справа, сверху и снизу – 20 мм. Страницы нумеруются по центру вверху. Шрифт Times New Roman – 12 или 14 размера, межстрочный интервал – полуторный.

Диск с выполненной работой и распечаткой сдается преподавателю в установленные сроки. Отчет по практике проверяется преподавателем. После проверки и устранения замечаний, сделанных преподавателем в ходе просмотра диска и распечатки, работа подлежит устной защите для получения оценки.

Форма промежуточная аттестация - дифференцированный зачет.

2 Примерная тематика теоретических заданий

1. Правовая защита информации.
2. Морально-этические меры.
3. Организационные меры защиты.
4. Концептуальные основы защиты информации.
5. Концепции защиты информации.
6. Понятия национальной безопасности, национальных интересов Российской Федерации, угроз национальной безопасности, стратегических национальных приоритетов, доктрины информационной безопасности.
7. Законодательные и иные правовые акты в области технической защиты информации.
8. Нормативные правовые акты по технической защите информации.
9. Указы и распоряжения Президента РФ в области технической защиты информации. Постановления Правительства РФ.
10. руководящие документы ФСТЭК России, ФСБ России и других уполномоченных органов.
11. Органы по технической защите информации в РФ. ФСТЭК России.
12. Обеспечение защиты (некриптографическими методами) информации. Лицензирование деятельности в области ТЗИ.
13. Сертификация средств защиты информации.
14. Аттестация объекта информатизации по требованиям безопасности информации.

15. Классификация угроз и объектов защиты.
16. Угроза безопасности информации.
17. Угроза информационной безопасности АС.
18. Источник угрозы безопасности информации.
19. Критерии классификации угроз: по природе возникновения, по степени мотивации (случайные угрозы, преднамеренные угрозы), по положению относительно контролируемой зоны, по степени воздействия на АС, по виду нарушаемого свойства информации, по типу системы, на которую направлена угроза, по способу реализации.
20. Методы оценки опасности угроз.
21. Количественный и качественный риск.
22. Ожидаемый разовый ущерб.
23. Ежегодная частота возникновения рисков.
24. Общий годовой ущерб.
25. Объект информатизации.
26. Классификация объектов защиты.
27. Классификация информации.
28. Объекты информатизации, аттестуемые по требованиям безопасности информации.
29. Объект защиты информации.
30. Классификация объектов защиты.
31. Классификация автоматизированных систем (АС).
32. 9 классов защищённости АС от несанкционированного доступа (НСД).
33. Требования к защищенности для классов АС.
34. Классификация средств вычислительной техники (СВТ).
35. 7 классов защищённости СВТ от НСД.
36. Дискреционный принцип разграничения доступа.
37. Мандатный принцип разграничения доступа.
38. Угрозы несанкционированного доступа к информации.
39. Понятие несанкционированного доступа.
40. Модель потенциального нарушителя. Злоумышленник.
41. Основные классы атак в сетях на базе TCP/IP.
42. Классификация угроз по сети: характер угрозы, цель реализации угрозы, условие начала атаки, наличие обратной связи, расположение нарушителя относительно атакуемой информационной системы, уровень эталонной модели ISO/OSI, на котором реализуется угроза.

3 Варианты практических заданий

Общее задание - Разработка проекта технической системы комплексной безопасности для заданного объекта (по вариантам)

4. Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1. Рекомендуемая литература.

4.1.1. Основная литература:

1. 1. Ворона, В.А. Комплексные (интегрированные) системы обеспечения безопасности / В.А. Ворона, В.А. Тихонов - Н:Горячая линия-Телеком - 2016, 160 с

2. Васильков А.В. Безопасность и управление доступом в информационных системах: учеб.пос. / А.В. Васильков, И.А. Васильков. - М.: Форум, 2010. - 367 с.

3. МелехинВ.Ф., Вычислительные машины системы и сети. - М.:ИЦ «АКАДЕМИЯ», 2010. - 560с.

4. Мельников В.П. Информационная безопасность и защита информации: учеб.пос. / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, 2008. -

336 с.
5. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/ П. Б. Хорев М.: ФОРУМ, 2015. - 352 с.
6. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Учеб.пособ. - М.: ДМК Пресс, 2012. - 592 с.
7. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин - М.: ИНФРА-М, 2010. - 594 с.
8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. - М. ИД «ФОРУМ», 2011. - 416 с.

4.1.2 Законы Российской Федерации в области защиты информации (защиты государственной тайны)

1. ФЗ РФ «Об информации, информационных технологиях и о защите информации»
2. ФЗ РФ «О коммерческой тайне» (в редакции Федерального закона от 02.02.2006 № 19 - ФЗ).
3. ФЗ РФ «О персональных данных» от 27.07.2006 № 152ФЗ.
4. ФЗ РФ от 23 сентября 1992 г. N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».
5. Закон РФ от 19 февраля 1993 г. N 4524-1 «О федеральных органах правительственной связи и информации» (с изменениями от 24 декабря 1993 года, по состоянию на 1 апреля 1994 года).
6. Закон РФ от 10 июня 1993 года N 5151-1 «О сертификации продуктов и услуг».
7. Закон РФ от 10 июня 1993 года N 5154-1 «О стандартизации».
8. Закон РФ от 01 июля 1993 г. N 5306-1 «О внесении изменений и дополнений в Закон Российской Федерации «О федеральных органах государственной безопасности».
9. Закон РФ от 20 января 1995 года N 15-ФЗ «О связи».

4.1.3 ГОСТы в области защиты информации (защиты государственной тайны):

1. ГОСТ Р 34.10-94«Информационная технология криптографическая защита информации процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
2. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
3. ГОСТ Р 50862-96 «Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость».

4.1.4 Указы Президента РФ в области защиты информации (защиты государственной тайны)

1. Указ Президента РФ от 7 октября 1993г. N 1607 «О государственной политике в области охраны авторского права и смежных прав».
2. Указ Президента РФ от 31 декабря 1993г. N 2334 «О дополнительных гарантиях прав граждан на информацию»
3. Указ Президента РФ от 20 января 1994г. N 170 «Об основах государственной политики в сфере информатизации»
4. Указ Президента РФ от 3 апреля 1995 г. N 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»
5. Указ Президента РФ от 3 июля 1995 г. N 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации».
6. Указ Президента РФ от 30 ноября 1995г. N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».
7. Указ Президента РФ от 26 августа 1996г. N 1268 «О контроле за

экспортом из Российской Федерации товаров и технологий двойного назначения».

8. Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента РФ от 30 мая 1997 года N 226-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

4.1.5 Постановления Правительства РФ в области защиты информации (защиты государственной тайны)

1. Постановление Правительства РФ от 24 декабря 1994 г. N 1418 «О лицензировании отдельных видов деятельности» (с изменениями от 5 мая, 3 июня, 7 августа,12 октября 1995г.).

2. Постановление Правительства РФ от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и(или) оказанием услуг по защите государственной тайны».

3. Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации».

4. Постановление Правительства РФ от 04 сентября 1995г. N 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

5. Постановление Правительства РФ от 17 ноября 2007 г. № 781 об Утверждении «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

4.1.6 Нормативные документы в области защиты информации от несанкционированного доступа

1. Защита от несанкционированного доступа к информации. Термины и определения. ГОСТЕХКОМИССИЯ РОССИИ.

2. Постановление правительства РФ от 30 апреля 1997 г. N 513 «О внесении дополнения в Положение о лицензировании».

3. Положение «О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

4. Нормативные документы в области защиты информации от несанкционированного доступа.

4.2 Дополнительная литература

1. Тихонов, В.А. Технические системы охранной и пожарной сигнализации / В.А. Тихонов, В.А. Ворона - - Н:Горячая линия-Телеком - 2012, 376 с3.
2. Силаенков А.Н. Проектирование системы информационной безопасности: учеб. пособие - Омск: Изд-во ОмГТУ, 2009. - 128 с.
3. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. - М.: Вузовский учебник, 2006.- 525 с.
4. Козлачков П.С. Основные направления развития систем информационной безопасности. - М.: финансы и статистика, 2004.- 736 с.
5. Леваков Г.Н. Анатомия информационной безопасности. - М.: ТК Велби, издательство Проспект, 2004.- 256 с.
6. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. - М.: БХВ- Петербург, Арлит, 2002.- 456 с.
7. Сыч О.С. Комплексная антивирусная защита локальной сети. - М.: финансы и статистика, 2006.- 736 с.

4.3 Интернет-ресурсы

1 Университетская библиотека online. http://www.biblioclub.ru.

2. ЭБС «IPRbooks». http://www.iprbookshop.ru.

3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.

4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru

4.4 Материально-техническое обеспечение дисциплины (модуля)

Перечень материально-технического обеспечения включает в себя:

групповые и индивидуальные консультаций проводятся в аудитории оснащенный следующим оборудованием - мультимедиа-проектор Epson EB-445Wi с подвесным креплением, экран раскладной, акустическая система Sven 5+1, компьютер CeleronCore420/IG965/512/80;

текущий контроль и промежуточная аттестация проводятся в аудитории оснащенный следующим оборудованием – персональные компьютеры (13 шт.) в составе CeleronCore420/IG965/512/80 с выходом в сеть Internet, объединенные в локальную вычислительную сеть, доска магнитно-маркерная 1-элементная 120x240, короткофокусный мультимедиа-проектор Epson EB-436Wi с настенным креплением и набором кабелей;

для самостоятельной работы используется аудитория оснащенная следующим оборудованием - компьютеры (6 шт.) в составе CeleronCore420/IG965/512/80, книжные шкафы для учебной литературы и учебно-методических материалов.

Методические указания составлены с требованиями ФГОС ВО, с учетом рекомендаций Положения об учебно-методическом комплексе дисциплины СКФУ и ОП ВО по направлению подготовки 10.04.01 Информационная безопасность.