МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

УТВЕРЖДАЮ

Директор Пятигорского института
(филиал) СКФУ
Т.А. Шебзухова

Рабочая программа практики
УП.05.01 Учебная практика

Специальность 09.02.01 Компьютерные системы и комплексы

Форма обучения очная

Рабочая программа учебной практики разработана на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы.

Рабочая программа учебной практики разработана:

1 Хаджиев А.А., преподаватель колледжа Пятигорского института (филиал) СКФУ

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

СОГЛАСОВАНО:

Представитель работодателя

Зам. Генерального директора

ООО «Миллениум - плюс» Давыдов А.А.

должность представителя работодателя, наименование организации и город ее расположения — Фамилия, инициалы

1. Паспорт программы практики

1.1. Место учебной практики в структуре программы подготовки специалистов среднего звена (далее ППССЗ)

Учебная практика УП.05.01 принадлежит к циклу профессиональные модули, проводится в 7 семестре.

1.2. Цели и задачи учебной практики

Цель: закрепление и углубление знаний, полученных студентами в процессе теоретического обучения; приобретение необходимых умений, навыков и опыта практической работы по изучаемой специальности.

Задачи: формирование у студента общих и профессиональных компетенций; приобретение практического опыта, реализуемого в рамках ОП СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 09.02.01 Компьютерные системы и комплексы; проверка знаний, полученных при изучении ПМ 05 Веб технологии и защита информации.

Вид профессиональной деятельности: Веб технологии и защита информации.

В ходе прохождения практики обучающийся должен

иметь практический опыт:

- применения нормативно-технической документации;
- создания защищенных резервных копий данных;
- использования методов криптографии и алгоритмов шифрования при передачи конфиденциальной информации;
- установки и проверки устройств с помощью антивирусных программ и утилит;
- передачи конфиденциальной информации по защищенным каналам;
- установки и сопровождения антивирусных программ;
- восстановления компьютера после поражения вирусами;
- подключения устройств с соблюдением требований информационной безопасности.

уметь:

- выполнять требования нормативно-технической документации;
- применять знания о кибербезопасности в решении поставленных задач;
- защищать личную информацию;
- создавать надежные пароли;
- устранять нарушения кибербезопасности;
- выбирать и использовать антивирусную программу;
- восстанавливать пораженные "компьютерными вирусами" объекты;
- подключить организацию к Internet с соблюдением требований информационной безопасности;
- классифицировать автоматизированные системы согласно руководящих документов Гостехкомиссии Российской Федерации;

знать:

- регламенты, процедуры, технические условия и нормативы;
- определения кибербезопасности и кибератак;
- требования к криптографическим системам защиты информации;
- алгоритмы шифрования;
- методы криптоанализа;

- классификацию вирусов и антивирусных программ;
- программы для защиты информации;
- основные понятия и определения, используемые при изучении информационной безопасности;
- классификацию угроз информационной безопасности;
- классические и современные методы взлома интрасетей;
- классификацию и правила защиты от "компьютерных вирусов";
- способы организации информационной безопасности на предприятии;
- нормы и требования российского законодательства в области лицензирования и сертификации;

обладать общими и профессиональными компетенциями

1.3. Трудоемкость освоения программы учебной практики:

Трудоемкость освоения учебной практики УП.05.01 составляет 2 недели (72 час.).

2. Результаты практики

Результатом учебной практики является:

освоение общих компетенций (ОК)

Код	Наименование результата практики
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

профессиональных компетенций (ПК):

Код	Наименование результата практики
ПК 4.6	Выполнять требования нормативно-технической документации.

3. Структура и содержание программы практики

3.1. Структура практики

Коды формируемых компетенций	Наименование профессионального модуля	Объем времени, отведенный на практику (в неделях, часах)	Период проведения практики
ОК 01 ОК 02 ОК 04 ОК 09 ПК 4.6	ПМ.05 Веб технологии и защита информации	2 недели, 72 час.	*7 семестр*

3.2. Содержание практики

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование дисциплин, междисциплинарных курсов с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Веб технологии и защита информации	Вводный инструктаж по технике безопасности. Антивирусная защита ПК.	Тема 7. Классификация вирусов. Антивирусная защита персональных компьютеров.	МДК.05.01 Персональная кибербезопасность	6
	Законодательство в области защиты информации.	Тема 1. Основные понятия персональной кибербезопасности. Информационная безопасность и кибербезопасность. Тема 12. Законы и стандарты информационной безопасности.	МДК.05.01 Персональная кибербезопасность	6
	Защита данных от несанкционированного доступа.	Тема 4. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.	МДК.05.01 Персональная кибербезопасность	6
	Использование VPN.	Тема 9. Современные методы защищенной аутентификации.	МДК.05.01 Персональная кибербезопасность	6
	Использование облачных сервисов для хранения, передачи и совместного доступа к файлам.	Тема 8. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств защиты информации.	МДК.05.01 Персональная кибербезопасность	6
	Использование электронной подписи.	Тема 11. Электронная цифровая подпись. Виды электронной цифровой подписи.	МДК.05.01 Персональная кибербезопасность	6
	Исследование признаков присутствия вредоносного ПО. Исследование сетевой активности.	Тема 2. Сущность и понятие защиты информации.	МДК.05.02 Техническая защита информации	6
	Парольная защита Архива с файлами.	Тема 3. Основы защиты информации.	МДК.05.02 Техническая защита информации	6

	Передача Архива с файлами, защищенного паролем.	Тема 3. Основы защиты информации.	МДК.05.02 Техническая защита информации	6
	Проверка компьютера лечащими утилитами.	Тема 7. Классификация вирусов. Антивирусная защита персональных компьютеров.	МДК.05.01 Персональная кибербезопасность	6
	Хранение и защита информации.	Тема 4. Определение классов защищенности средств вычислительной техники от несанкционированного доступа.	МДК.05.02 Техническая защита информации	6
	Шифрование и расшифрование данных.	Тема 4. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.	МДК.05.01 Персональная кибербезопасность	6

4. Условия организации и проведения практики

4.1. Требования к документации, необходимой для проведения практики:

- программа учебной практики;
- договор об организации практики;
- направление на практику;
- индивидуальное задание;
- дневник практики;
- аттестационный лист;
- характеристика работы обучающегося;
- отчет по практике.

4.2. Требования к учебно-методическому обеспечению практики

Практика имеет целью комплексное освоение студентами ПМ.05 Веб технологии и защита информации, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и практического опыта.

Учебная практика проходит в компьютерных классах и лабораториях колледжа с установленным лицензионным программным обеспечением.

Для написания отчета студентам выдаются Методические указания по организации и проведению учебной практики и индивидуальные задания.

Индивидуальные задания по ПМ.05 Веб технологии и защита информации:

1. Алгоритмы шифрования с открытым ключом (асимметричные).
2. Алгоритмы шифрования с секретным ключом (симметричные).
3. Антивирусная защита персональных компьютеров.
4. Антивирусные программы, их назначение и виды.
5. Антишпионское ПО.
6. Аудит программного кода по требованиям безопасности.
7. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

8. Виды алгоритмов шифрования данных.
9. Виды защищаемой информации.
10. Виды компьютерных вирусов.
11. Виды угроз безопасности информации.
12. Виды электронной цифровой подписи.
13. Законодательство о персональных данных.
14. Защита авторских прав.
15. Защита данных пользователей портала государственных услуг.
16. Защита документов от изменения или искажения цифровой подписью.
17. Защита компьютера от вирусов встроенными средствами операционной системы.
18. Защита личности как носителя информации.
19. Защита от внутренних угроз.
20. Защита своих данных и денежных средств от киберпреступлений.
21. Идентификация по голосу. Скрытые возможности.
22. Идентификация, аутентификация и авторизация.
23. Инженерные конструкции и сооружения для защиты информации. Их классификация.
24. Как подписывать с помощью ЭЦП электронные документы различных форматов.
25. Каналы утечки информации. Технические каналы утечки
26. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
27. Квантовая криптография.
28. Классификация антивирусных программ.
29. Классификация вирусов.
30. Классификация датчиков охранной сигнализации.
31. Классификация источников и носителей информации.
32. Компьютерная преступность. Виды преступной деятельности.
33. Криптографическая защита информации.
34. Криптографические атаки.
35. Криптографические методы шифрования и дешифрования информации.
36. Мероприятия по управлению доступом к информации.
37. Методы борьбы с фишинговыми атаками.
38. Методы защиты информации от преднамеренного доступа.
39. Методы несанкционированного доступа к информации.
40. Методы обеспечения безопасности каналов передачи данных.
41. Методы обеспечения достоверности передачи информации.
42. Методы противодействия киберпреступникам.
43. Методы расшифрования секретных данных.
44. Методы шифрования данных.
45. Назначение, функции и типы систем видеозащиты.
46. Обеспечение безопасности Web-сервисов.
47. Обзор современных платформ архивации данных.
48. Обзор угроз и технологий защиты Wi-Fi-сетей.
49. Особенности процессов аутентификации в корпоративной среде.
50. Оценка безопасности автоматизированных систем.
51. Параметры системы защиты информации.
52. Передача секретной информации с помощью шифрования.
53. Подписание документов с помощью цифровой подписи.
54. Потенциальные каналы утечки информации.
55. Причины киберпреступлений.
56. Проблемы кибербезопасности.
57. Проверка пользователя при входе в систему государственных услуг.
58. Программные средства анализа локальных сетей на предмет уязвимостей.

59. Простые приемы, используемые для защиты компьютера от умышленных действий.
60. Процедура идентификации, как основа процесса обнаружения объекта.
61. Процесс передачи и получения зашифрованной информации.
62. Реализация криптографических методов.
63. Системный подход к защите информации.
64. Современные компьютерные вирусы.
65. Современные методы киберпреступлений.
66. Современные угрозы и защита электронной почты.
67. Способы защиты баз данных, имеющих парольный доступ.
68. Способы защиты информации методами криптографии.
69. Сравнение антивирусных программ по их характеристикам.
70. Средства идентификации личности.
71. Стандарт шифрования данных DES.
72. Требования к криптографическим системам защиты информации.
73. Угрозы сохранности данных в компьютере случайного характера.
74. Утечки информации: как избежать. Безопасность смартфонов.
75. Цифровые водяные знаки в изображениях.
76. Электронная цифровая подпись.
77. Этапы проектирования системы защиты информации.
78. Этапы разработки мер по предотвращению угроз утечки информации.

4.3. Требования к материально-техническому обеспечению

Реализация программы учебной практики УП.05.01 осуществляется в учебных лабораториях и мастерских СКФУ, предусмотренных ФГОС СПО.

Материально-техническое обеспечение соответствует профессиональной деятельности и дает возможность овладеть установленными компетенциями по всем осваиваемым видам деятельности, предусмотренным программой, с использованием современных технологий, материалов и оборудования.

Все помещения соответствуют требованиям техники безопасности и противопожарной безопасности при проведении учебной практики.

4.4. Перечень основной и дополнительной литературы, интернет-ресурсов, необходимых для проведения практики

Основные источники:

1. Ермакова, А. Ю. Методы и средства защиты компьютерной информации: учебное пособие / А. Ю. Ермакова. — Москва: РТУ МИРЭА, 2020. — 223 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844

2. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург: Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

3. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

Дополнительные источники:

1. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург: Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924

2. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В.

Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184

3. Фот, Ю. Д. Методы защиты информации: учебное пособие / Ю. Д. Фот. — Оренбург: ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/159977.

Интернет-источники:

1. https://nsportal.ru/npo-spo/informatsionnaya-bezopasnost/library/2014/04/08/metodicheskaya-razrabotka-prakticheskikh-0 - Практические работы по дисциплине Информационной безопасности
2. https://infopedia.su/24x858c.html - Информационные основы кибербезопасности

4.5. Требования к руководителям практики от образовательного учреждения

Руководителем практики является преподаватель, осуществляющий обучение студентов в рамках профессиональной подготовки.

Требования к уровню квалификации руководителя практики определяются ФГОС СПО по специальности 09.02.01 Компьютерные системы и комплексы.

5. Контроль и оценка результатов практики

По завершении практики в 7 семестре студент пишет отчет по практике и сдает дифференцированный зачет (защита отчета по практике).