

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Шебзухова Татьяна Александровна

Должность: Директор Института сервиса, туризма и дизайна (филиал) Северо-Кавказского
федерального университета

Дата подписания: 21.09.2023 12:48:41

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1c8ef96f

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего
профессионального образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ» Институт сервиса, туризма и дизайна (филиал) СКФУ в г.
Пятигорске**



**Методические указания
по выполнению практических работ
по дисциплине
«Персональная кибербезопасность»**

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

2. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

4. Учебно-методическое и информационное обеспечение дисциплины

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Персональная кибербезопасность» – подготовка студента к решению нестандартных ситуаций касательной дестабилизации информационной системы или нарушения целостности данных, а также их потери.

3. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Тема самостоятельного изучения № 1. Первичные навыки обеспечения кибербезопасности на рабочем месте

Вид деятельности студентов: самостоятельное изучение литературы

Итоговый продукт самостоятельной работы: конспект
Средства и технологии оценки: отчет
План конспекта:

Определите участки операционной системы, в которой некорректно установлены права доступа, т.е., пользователь может вносить корректировки в те участки в которых он не должен имеет права доступа

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1

Тема самостоятельного изучения № 2. Анализ разрушительности кибератак.

Вид деятельности студентов: самостоятельное изучение литературы
Итоговый продукт самостоятельной работы: конспект
Средства и технологии оценки: отчет

План конспекта:

Используя инструменты поисковых служб, самостоятельно найдите киберугрозы для персонального компьютера работающего как рабочая станция в организации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1

Тема самостоятельного изучения № 3 Приоритизация классов киберугроз.

Вид деятельности студентов: самостоятельное изучение литературы

Итоговый продукт самостоятельной работы: конспект **Средства и технологии оценки:** отчет **План конспекта:**

Провести анализ своего ПК и результат представить в отчете с подробным описанием каждого процесса.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1

Тема самостоятельного изучения № 4 Основные способы выявления фишинг атак.

Вид деятельности студентов: самостоятельное изучение литературы

Итоговый продукт самостоятельной работы: конспект **Средства и технологии оценки:** отчет **План конспекта:**

Используя полученные навыки работы с поисковой системой, определить наиболее актуальные методы фишинг атак и представить их в отчете

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1

Тема самостоятельного изучения № 5 Моделирование поведения злоумышленника в момент проведения социальной инженерии.

Вид деятельности студентов: самостоятельное изучение литературы

Итоговый продукт самостоятельной работы: конспект **Средства и технологии оценки:** отчет **План конспекта:**

Используя поисковые службы составить отчет об актуальных методах защиты от социальной инженерии.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы

1-2	1-2	1-2	1
-----	-----	-----	---

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Текущая аттестация студентов проводится преподавателем, ведущим практические занятия по дисциплине «Профессиональная кибербезопасность» в форме собеседования, выполнения индивидуальных заданий. Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме устного ответа студента по выполненной работе и ответов на вопросы преподавателя. При оценивании ответа студентов учитывается полнота и степень раскрытия темы, владение материалом, ответов на дополнительные вопросы.

Максимальное количество баллов студент получает, если он активно участвует в работе, владеет материалом, умеет логично и четко излагать мысли, творчески подходит к решению основных вопросов темы, показывает самостоятельность мышления.

Основанием для снижения оценки являются:

- слабое знание темы и основной терминологии;
- пассивность участия в групповой работе;
- отсутствие умения применить теоретические знания для решения практических задач;
- несвоевременность предоставления выполненных работ.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методическое и информационное обеспечение дисциплины	
Основная литература	1. Старостина, Е. В. Защита от компьютерных преступлений и кибертерроризма : вопросы и ответы / Е.В. Старостина, Д.Б. Фролов. - М. : Эксмо, 2005. - 192 с. 2. Словарь-справочник терминов в области кибербезопасности : [около 2000 терминов] / М-во образования и науки Рос. Федерации, Федер. гос. автоном. науч. учреждение "Центр информационных технологий и систем органов исполнительной власти" ; [авт.-сост.: И.М. Воронков, А. В. Дроздов, С. В. Петров и др.] ; [рук. проекта А. В. Старовойтов]. - Москва : Сам полиграфист, 2014. - 229 с.
Дополнительная литература	1. Курушин, В. Д. Компьютерные преступления и информационная безопасность : Справочник. - М. : Новый Юрист, 1998. - 256с. 2. Кевин Митник, Вильям Саймон Искусство вторжения: ДМК пресс, Компания АйТи, 2005. – 337с.
Методическая литература	1. Методические указания по выполнению практических работ по дисциплине Профессиональная кибербезопасность; 2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине Профессиональная кибербезопасность.
Интернет-ресурсы	1. Современные уязвимости программного обеспечения [Электронный ресурс] / https://www.securitylab.ru/vulnerability/ Обновляемые списки вредоносного ПО [Электронный ресурс] : https://www.securitylab.ru/virus/

Программное обеспечение	Последние версии популярных WEB браузеров; Антивирусные приложения; Сканеры портов.
Материально-техническое обеспечение	Учебные аудитории, оборудованные учебной мебелью, интерактивной доской, персональными компьютерами, мультимедийным проектором для проведения лекционных и практических занятий.