МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Методические рекомендации
по организации самостоятельной работы
по дисциплине Безопасность информационных систем
Направление подготовки
09.03.02«Информационные системы и технологии»
Квалификация выпускника бакалавр

Пятигорск 2020г.

Рассмотрено и утверждено на заседании кафедры систем управления и информационных технологий, протокол № ___ от _____2020 г.

Зав.кафедройСУИТ _____И.М. Першин

Содержание

ВВЕДЕНИЕ

Самостоятельная работа студента (СРС) наряду с аудиторной представляет одну из форм учебного процесса и является существенной его частью. СРС – это планируемая работа студентов, выполняемая по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

СРС предназначена не только для овладения каждой дисциплиной, но и для формирования навыков самостоятельной работы вообще, в учебной, научной, профессиональной деятельности, способности принимать на себя ответственность, самостоятельно решить проблему, находить конструктивные решения.

Количество часов на самостоятельную работу по программе предусмотрено по направлению 09.03.02–94,5 часа

1. Общая характеристика самостоятельной работы при изучении дисциплины «Безопасность информационных систем»

Самостоятельная работа предусматривает следующие виды: Изучение литературы по темам, вынесенным на самостоятельную работу, Подготовка к лабораторным работам.

Цель самостоятельной работы:

1. углублять и расширять профессиональные знания;
2. формировать у студентов интерес к учебно-познавательной деятельности;
3. научить студентов овладевать приемами процесса познания.

Задачи самостоятельной работы:

1. развивать у студентов самостоятельность, активность, ответственность;
2. развивать познавательные способности будущих специалистов.

Формируемые компетенции

2.План график выполнения самостоятельной работы

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-3	Самостоятельное изучение литературы по темам № 1 - 9	Конспект	Собеседование	77,76	8,64	86,4
ОПК-3	Подготовки к лабораторным занятиям	*Решение проблемных задач*	Отчет письменный	7,29	0,81	8,1
Итого за 7 семестр				85,05	9,45	94,5
Итого				85,05	9,45	94,5

3. Контрольные точки и виды отчетности по ним

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
1.	Собеседование по темам	5-ая неделя	15
2.	Лабораторные работы 1-7	7-ая неделя	15
3.	Лабораторные работы 8-12	12 –ая неделя	25
	Итого за 7 семестр		**55**

4. Методические указания по изучению теоретического материала

4.1 Вид самостоятельной работы: самостоятельное изучение литературы

Изучать учебную дисциплину рекомендуется по темам, предварительно ознакомившись с содержанием каждой из них в программе дисциплины. При теоретическом изучении дисциплины студент должен пользоваться соответствующей литературой. Примерный перечень литературы приведен в рабочей программе

Для более полного освоения учебного материала студентам читаются лекции по важнейшим разделам и темам учебной дисциплины. На лекциях излагаются и детально рассматриваются наиболее важные вопросы, составляющие теоретический и практический фундамент дисциплины. В процессе изучения учебной дисциплины студент должен выполнить контрольную работу, целью которой является приобретение практических навыков нормирования и оценки эффективности технологических решений.

Итоговый продукт: Конспект статей

Средства и технологии оценки: Собеседование

Критерии оценивания: Оценка «отлично» выставляется студенту, если в полном объеме изучен курс данной дисциплины и выполнены практические задания

Оценка «хорошо» выставляется студенту, если достаточно полно изучен курс данной дисциплины и выполнены практические задания

Оценка «удовлетворительно» выставляется студенту, недостаточно если полно изучен курс данной дисциплины и выполнены практические задания

Оценка «неудовлетворительно» выставляется студенту, если отсутствуют знания и практические навыки по данной дисциплине

Темы для самостоятельного изучения

Тема 1. Основы сетевых технологий и обеспечение безопасности информационных систем

1) Основы сетевой безопасности.
2) Сеть как объект защиты.
3) Уязвимость компонентов распределенных АС.
4) Рабочие станции,
5) Серверы и коммуникационное оборудование,
6) Каналы связи.
7) Виды угроз информационной безопасности.
8) Классификация угроз информационной безопасности в КС: Естественные угрозы, Искусственные угрозы, Основные непреднамеренные искусственные угрозы,
9) Основные преднамеренные искусственные угрозы,
10) Классификация каналов проникновения в систему и утечки информации,
11) Неформальная модель киберпреступника,
12) Европейская конвенция о киберпреступности.

Тема 2. Возможные уязвимости, угрозы и атаки на информационные системы

1. Угроза, уязвимость, атака.
2. Классификация уязвимостей,
3. Источники возникновения уязвимостей,
4. Классификация уязвимостей по уровню в инфраструктуре АС,
5. Классификация уязвимостей по степени риска,
6. CommonVulnerabilitiesandExposures,
7. Классификация атак по целям,
8. Классификация атак по мотивации действий,

9. Местонахождение нарушителя,
10. Механизмы реализации атак,
11. Статистика по уязвимостям и атакам,
12. Примеры атак.

Тема 3. Классификация атак по уровням иерархической модели OSI.

1. Уровни модели OSI.
2. Фрагментация данных.
3. Атака Pingflooding.
4. Нестандартные протоколы, инкапсулированные в IP.
5. Атака smurf.
6. Атака DNS spoofing.
7. Атака IP spoofing.
8. Навязывание пакетов.
9. Sniffing — прослушивание канала.
10. Перехват пакетов на маршрутизаторе.
11. Навязывание хосту ложного маршрута с помощью протокола ICMP.
12. WinNuke.
13. Подмена доверенного хоста.
14. Технологии обнаружения атак.

Тема 4. Мониторинг и анализ трафика в сети.

1. Обзор методов анализа и мониторинга сетевого трафика.
2. Важность мониторинга и анализа сети.
3. Способы мониторинга и анализа.
4. Методы мониторинга, основанные на маршрутизаторе.
5. Протокол простого сетевого мониторинга,
6. Удалённый мониторинг,
7. Netflow,
8. Технологии не основанные на маршрутизаторах,
9. Активный мониторинг,
10. Пассивный мониторинг,
11. Комбинированный мониторинг,
12. Просмотр ресурсов на концах сети,
13. Сетевой монитор с собственной конфигурацией,
14. Атакуемые сетевые компоненты: Сервера, Рабочие станции, Среда передачи информации, Узлы коммутации сетей.

Тема 5. Атаки на беспроводные устройства и защита от них.

1. Организация сетей Wi-Fi . Угрозы.
2. Прямые угрозы.
3. Чужаки.
4. Нефиксированная природа связи.
5. Уязвимости сетей и устройств.
6. Некорректно сконфигурированные точки доступа.
7. Некорректно сконфигурированные беспроводные клиенты.
8. Взлом шифрования.
9. Имперсонация и IdentityTheft.

10. Отказы в обслуживании.
11. Косвенные угрозы.
12. Утечки информации из проводной сети.
13. Особенности функционирования беспроводных сетей.
14. Методы ограничения доступа.
15. Методы аутентификации .
16. Методы шифрования.
17. Атаки на сети wi-fi.

Тема 6. Основные типы уязвимостей информационных систем. Защита от уязвимостей.

1. Классификация уязвимостей: технологические, организационные, эксплуатационные.
2. Типовые уязвимости.
3. Неподдерживаемые версии операционных систем и системного программного обеспечения,
4. Уязвимости веб-серверов,
5. Использование небезопасных протоколов управления,
6. Использование небезопасных протоколов SSL и TLS,
7. Слабые пароли WPA/WPA2-PSK,
8. Использование протокола разрешения имен NetBIOS по TCP/IP,
9. Межсайтовый скриптинг.
10. Устранение выявленных уязвимостей.

Тема 7. Атаки в виртуальной среде и защита от них.

1. Разведка.
2. Атаки на сети с WEP-шифрованием.
3. Пассивные сетевые атаки.
4. Активные сетевые атаки.
5. Повторное использование вектора инициализации (InitializationVectorReplayAttacks).
6. Манипуляциябитами (Bit-Flipping Attacks).
7. Атаки на сети с WPA/WPA2-шифрованием.
8. Атака по словарю на WPA/WPA2 PSK.
9. Атака переустановки ключа в WPA и WPA2 (KRACK)

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Принципы работы межсетевых экранов.
2. Конфигурирование межсетевого экрана Windows.
3. Классификация.
4. Профиль брандмауэра – домен, частный, общий.
5. Состояние брандмауэра.
6. Правила для исходящих и входящих соединений.
7. Мастер создания правила для нового исходящего подключения.

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?

3. Чем отличаются пассивные и активные IDS?
4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

4.2 Вид самостоятельной работы:Подготовка к лабораторным работам
Итоговый продукт: Лабораторная работа
Средства и технологии оценки: Отчет письменный
Критерии оценивания: Оценка «отлично» выставляется студенту, если в полном объеме изучен курс данной дисциплины и выполнены лабораторные задания

Оценка «хорошо» выставляется студенту, если достаточно полно изучен курс данной дисциплины и выполнены лабораторные задания

Оценка «удовлетворительно» выставляется студенту, недостаточно, если полно изучен курс данной дисциплины и выполнены лабораторные задания

Оценка «неудовлетворительно» выставляется студенту, если отсутствуют знания и практические навыки по данной дисциплине

Вопросы по темам лабораторных работ

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Принципы работы межсетевых экранов.
2. Конфигурирование межсетевого экрана Windows.
3. Классификация.
4. Профиль брандмауэра – домен, частный, общий.
5. Состояние брандмауэра.
6. Правила для исходящих и входящих соединений.
7. Мастер создания правила для нового исходящего подключения.

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системыобнаружения вторжений.

11. Что такое IDS?
12. Что такое сетевая система обнаружения вторжений?
13. Чем отличаются пассивные и активные IDS?
14. Что такое SNORT?
15. Какие задачи выполняет SNORT?
16. Как работают правила SNORT?
17. Как писать правила для SNORT?
18. Зачем писать собственные правила SNORT?
19. Зачем загружать обновление правил SNORT?

20. Как в SNORT создавать логи?

Тема 10. Базовое администрирование и разрешение сетевыхпроблем с использованием утилит командной строки Windows.

1. Использование базовых команд командной строки Windows, применяемых для поиска проблем в сети.
2. Проверка настроек IP. проверка соединения на уровне протокола IP с использованием команды Ping.
3. Определение маршрута (трассировка) пакетов с использованием команды tracert.
4. Разрешение доменных имен с использованием команды nslookup.
5. Проверка вашей сетевой конфигурации и сетевой статистики командой netstat.

Тема11. Анализ и изучение заголовков различных сетевых пакетов.

1. Анализ различных пакетов такие как TCP, HTTP, ICMP, DNS с использованием Wireshark.
2. Установка Wireshark.
3. Файл с захваченным трафиком.
4. Исследование заголовка ARP.
5. Исследование заголовка TCP.
6. Исследование заголовка HTTP.
7. Исследование заголовка ICMP.
8. Исследование заголовка DNS.

Тема 12. Сканирование и исследования безопасности сети с помощью сканера Nmap.

1. Какими способами можно задать диапазон сканируемых хостов? Как задать несколько адресов?
2. Какие существуют способы поиска активных (включённых) хостов в сети?
3. Какие способы сканирования портов существуют в Nmap? Какими ключами они задаются?
4. Как задать диапазон портов? Как просканировать все порты? Как просканировать UDP порты? Как просканировать порты 21,80,8080?
5. Как с помощью nmap определить операционную систему, установленную на удаленном хосте?
6. Для чего используются ключи –v –O –sV –sT –sU –sS -A?

Тема 13. Методы анализа сетевого трафика с использованием WireShark.

1. Что такое неразборчивый режим сетевой карты?
2. Для чего используется WireShark?
3. Каковы основные элементы интерфейса программы Wireshark? Для чего они нужны?
4. Как задаются условия фильтрации трафика?
5. Как объединить условия фильтрации?
6. Что такое отслеживание соединения? Для чего оно используется?
7. Как извлечь файлы из перехваченного трафика?
8. Как определить какие протоколы используются в перехваченном трафике?

Тема 14. Установка и настройка VPN сервера.

1. Что такое VPN? Для чего он используется?
2. Какие виды VPN соединений существуют? Для чего они применяются?
3. Какие порты использует SoftEtherServer для входящих подключений?
4. Что такое NAT? Для чего он используется?
5. Что такое DHCP? Для чего он используется?
6. Что такое SecureNAT и для чего используется?

Тема 15. Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt.

1. Что такое шифрование?
2. Чем отличается симметричное шифрование от ассиметричного?
3. Что такое хэш-функция? Каковы ее свойства?
4. Что такое цифровая подпись? Для чего она используется?
5. Для чего используется приложение VeraCrypt? Какой тип шифрования она использует?
6. Для чего используется приложение GnuPG? Какой тип шифрования она использует?

Тема 16. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft BaselineSecurity.

1. Автоматическое сканирование по заданным шаблонам.
2. Проверка продуктов Microsoft на наличие уязвимостей – MicrosotBaselineSecurityAnalyzer.
3. Составление сценария сканирования по определенным требованиям.
4. Автоматизация проверки.

Тема 17. Системы разграничения доступа.

1. Какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?
2. В чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа (приведите примеры)?
3. Как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?
4. Какие дополнительные возможности разграничения доступа к информационным ресурсам предоставляет шифрующая файловая система?
5. Насколько, на Ваш взгляд, удобно использование шифрующей файловой системы (в том числе при необходимости совместной работы над документами)?
6. Какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

Тема 18. Управление доступом.

1. Какие типы групп могут быть созданы в домене?
2. Чем отличаются группы безопасности от групп распространения?

3. Назовите порядок размещения пользователей и групп в группах домена большого предприятия с несколькими доменами.
4. В чем главное отличие групп локального компьютера от групп домена?
5. Почему уровень безопасности сети на основе домена выше, чем в одноранговой сети?
6. В чем отличие глобальных и локальных доменных групп?
7. Какие группы могут быть отнесены к универсальным группам домена?
8. Как создается учетная запись компьютера в домене?
9. Как создается учетная запись пользователя домена?
10. Какими учетными записями должен обладать пользователь для того, чтобы он мог выполнить первоначальное присоединение компьютера к домену?

Тема 19. Аудит и журналы безопасности.

1. Какова роль аудита в обеспечении безопасности компьютерной системы?
2. Где и каким образом формируется информация о событиях аудита?
3. Какая информация может быть получена в результате аудита?
4. Какие типы аудита вы знаете и для чего предназначен каждый из них?
5. Каким образом активизируется политика аудита?
6. Каким образом политика аудита применяется для выбранных объектов и пользователей?
7. В каких случаях целесообразно учитывать Успех, а когда целесообразно фиксировать Отказ?
8. Как пользоваться журналами безопасности?
9. Какие учетные записи дают право на настройку аудита и проверку результатов аудита?
10. Каким образом администратор может использовать информацию об аудите для повышения безопасности системы?

Список литературы

Основная литература

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон.текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 c.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. 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.

Дополнительная литература:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. : [учебник] / В.Г. Олифер, Н.А. Олифер. - 4-е изд. - СПб. : Питер, 2011. - 944 с.
2. Таненбаум, Э. Компьютерные сети : [учеб. пособие] / Э. Таненбаум ; пер. с англ. В. Шрага. - 4-е изд. - СПб. : Питер, 2007. - 992 с. .

3. Сети и телекоммуникации : учеб.пособие / Б.В. Соболь, А.А. Манин, М.С. Герасименко. - Ростов н/Д : Феникс, 2015. - 191 с. .
4. 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.

Интернет-ресурсы

Для проработки теоретического материала и выполнения самостоятельных работ рекомендуется использовать следующие Интернет-ресурсы:

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»
3. http://www.intuit.ru - Национальный открытый университет «ИНТУИТ»;
4. http://www.window.edu.ru - Единое окно доступа к образовательным ресурсам.

Программное обеспечение

1. Windows 7.
2. Nmap.
3. Microsoft BaselineSecurity.
4. Wireshark.
5. VeraCrypt.