ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Цифровых технологий

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Е.С. Сахарчук
«27» апреля 2022 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ОСВОЕНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Б1.О.08 «Дисциплины (модули)», Обязательная часть

Профиль подготовки
прикладная информатика в информационной сфере

Квалификация (степень) выпускника:
Магистр
Форма обучения: очная

Курс 2 семестр 3

Москва 2022

Методические рекомендации разработаны на основании федерального государственного образовательного стандарта высшего образования направления подготовки 09.04.03 Прикладная информатика (уровень магистратуры), утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 916 Зарегистрировано в Минюсте России 10 октября 2017 г. №48495.

Разработчики методических рекомендаций: МГГЭУ, доцент кафедры цифровых технологий
место работы, занимаемая должность

_____ Перепелкина Ю.В. 14.03 2022 г
подпись Ф.И.О. Дата

Методические рекомендации утверждены на заседании кафедры цифровых технологий (протокол № 4 от «29» 03 2022 г.)

на заседании Учебно-методического совета МГГЭУ
(протокол № 1 от «27» 04 2022 г.)

Заведующий кафедрой
«29» 03 2022 г. _____ Шипрофонов Е.П.
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО:

Начальник учебно-методического управления
_____И.Г. Дмитриева
«27» 04 2022 г.

Начальник методического отдела
_____Д.Е. Гапеенок
«27» 04 2022 г.

Декан факультета ПМиИ
_____ Е.П. Петрунина
«27» 04 2022 г.

Содержание

1. Методические рекомендации для студентов по изучению дисциплины «Программно-аппаратные средства защиты информации»

Методические рекомендации призваны обеспечить эффективность самостоятельной работы студентов с литературой, на основе рациональной организации е изучения, сориентировать их в направлении изучения материала по поставленным вопросам, дать возможность отработать навыки составления и оформления различных видов документов, как под контролем преподавателя, так и самостоятельно.

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.

3. Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	6 семестр		
1.	Сдача отчетов по лабораторным работам 1,2. Собеседование по темам 1-3	5-ая неделя	15
2.	Сдача отчетов по лабораторным работам 3,4. Собеседование по темам 4-6.	12-ая неделя	15
3.	Сдача отчетов по лабораторным работам 5. Собеседование по темам 7,8.	16 –ая неделя	25
	Итого за 6 семестр		**55**

3.1 Работа с литературой

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Тема 1. Предмет и задачи программно-аппаратной защиты информации.	1-2	1-2	1-3	1-2
2	Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.	1-2	1-2	1-3	1-2

4.Методические рекомендации 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.

Средства и технологии оценки: собеседование.

Темы для самостоятельного изучения

Тема 1. Предмет и задачи программно-аппаратной защиты информации.

Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.

4.2 Вид самостоятельной работы: подготовка к практическим занятиям

Итоговый продукт: устный отчет

Средства и технологии оценки: собеседование

Задачи для практического решения

Практическое занятие 1

Сбор данных об информационной системе с помощью средств администрирования Windows.

Вопросы:

1. Линии связей локальных сетей.
2. Обеспечение секретности передаваемой информации в локальных сетях.
3. Типы линий связи локальных сетей.
4. Бескабельные каналы связи локальных сетей.
5. Базовые технологии локальных сетей.
6. Нестандартные топологии локальных сетей.
7. Согласование и экранирование линий связи.

Практическое занятие 2.

Сбор данных о топологии сети с помощью средства администрирования сетей.

Вопросы:

1. С помощью *3Com Network Supervisor* постройте карту сети учебной лаборатории.
2. Опишите узлы сети, используемые типы соединений.
3. Опишите доступные средства *удаленного администрирования*.
4. Перечислите используемые сетевые устройства.
5. Укажите, какие последствия будут при выходе из строя (или некорректной работе) каждого из сетевого устройства.

Практическое занятие 3

Идентификация и аутентификация систем семейства Microsoft Windows.

Вопросы:

1. Система идентификации и аутентификации.
2. Утилиты Microsoft Baseline Security Analyzer.
3. Двухфакторная аутентификация.
4. Парольные системы аутентификации.
5. Учетная запись пользователя.
6. Задание минимальной длины используемых в системе паролей.
7. Проверка администраторами безопасности качества используемых паролей путем имитации атак.
8. Ограничение числа неудачных попыток ввода пароля.
9. Журнал истории паролей.

Практическое занятие 4
Аутентификация по протоколу Kerberos.
Вопросы:
1. Центр распределения ключей (серверная часть Kerberos).
2. Порядок взаимной *регистрации* серверов Kerberos.
3. Основные этапы реализации протокола Kerberos в *Windows*.
4. Служба Kerberos Key Distribution Center.
5. Как осуществляется взаимодействие между Kerberos-областями.
6. Централизованное распределение ключей симметричного шифрования

Практическое занятие 5.
Настройка локальной политики парольной безопасности операционной системы.
Вопросы:
1. Что такое политика парольной безопасности?
2. Локальная политика безопасности операционной системы.
3. Администрирование парольной системы.
4. Свойства учетной записи.
5. Особенности простых и групповых учетных записей.
6. Администрирование парольной системы.

Практическое занятие 6.
Инфраструктура открытых ключей. Цифровые сертификаты.
Вопросы:
1. Инфраструктура открытых ключей (*Public* Key *Infrastructure*, сокр. *PKI*).
2. Центры распределения ключей.
3. Инфраструктура открытых ключей.
4. Цифровые сертификаты.
5. Криптографический протокол.
6. Атака типа "человек посередине" (man in the middle).
7. Структура Key Infrastructure.
8. Иерархия центров сертификации и клиентов.
9. Сертификат формата X.509 v.3.
10. Структура списка отозванных сертификатов.

Задания для практической работы

1. Выполните проверку компьютера с помощью Microsoft Baseline security analyzer.
2. Как оценен уровень уязвимости Вашего компьютера
3. Какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей
4. Опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере
5. Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.
6. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.
7. Выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или IP-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров.

8. Выберите из архива, созданного в предыдущей части работы, группу файлов для восстановления. Восстановите их в первый раз *по* исходному пути с сохранением копий, во второй раз - *по* альтернативному пути. Опишите, в чем разница в полученных результатах.

9. Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений:

1) n=55, e=3: <7,28>, <22,15>,<16,36>
2) n=65, e=5: <6,42>, <10,30>,<6,41>
3) n=77, e=7: <13,41>, <11,28>,<5,26>
4) n=91, e=5: <15,71>, <11,46>,<16,74>
5) n=33, e=3: <10,14>, <24,18>,<17,8>

10 . Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами p=23, g=5. Для указанных секретных параметров абонентов найти открытый ключ (y) и построить подпись для сообщения m:

1) x=11, k=3, m=15
2) x=10, k=15, m=5
3) x=3, k=13, m=8
4) x=18, k=7, m=5
5) x=9, k=19, m=15

Во всех вариантах будем предполагать, что h(m)=m для всех значений m.

4.3 Вид самостоятельной работы: подготовка к лабораторным работам

Итоговый продукт: отчет письменный

Средства и технологии оценки: собеседование

Вопросы к лабораторным работам:

Лабораторная работа 1

Межсетевые экраны

Вопросы:

1. Что такое межсетевой экран?
2. Для чего используется межсетевой экран?
3. Принцип работы Netfilter.
4. Таблицы межсетевого экрана Netfilter. Для чего они используются?
5. Что такое правила межсетевого экрана?
6. Как создавать правила для межсетевого экрана утилитой Iptables?
7. Как сохранить правила для последующей автозагрузки?
8. Что такое Web Application Firewall?
9. Как настроить правила в WAF mod_security?

Лабораторная работа №2

Программное восстановление данных.

Вопросы:

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?
2. Какие файловые системы поддерживает PhotoRec?
3. Какие форматы поддерживает PhotoRec?
4. Как Foremost восстанавливает файлы?
5. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?
6. Все ли данные скопированные с каталога /var/log/ восстановились?
7. Все ли данные скопированные с каталога /etc/ восстановились?

Лабораторная работа №3
Обнаружение и предотвращение вторжений.
Вопросы:

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 лог?

Лабораторная работа №4
Электронная цифровая подпись.
Вопросы:

1. Основные методы построения схем ЭЦП.
2. Шифрование окончательного результата обработки ЭД хэш-функцией при помощи асимметричного алгоритма.
3. Процессы генерации ЭЦП.
4. Электронная подпись RSA.
5. Алгоритм Эль-Гамаля.

Лабораторная работа № 5
Программно-аппаратное шифрование данных при их хранении.
Вопросы:

1. Шифрующая *файловая система* (Encrypting File *System* - *EFS*).
2. Работа шифрующей системы (Encrypting File System - EFS).
3. Шифрование ф*айла* с помощью симметричного криптоалгоритма.
4. Какой *пользователь* является агентом восстановления

5. Учебно-методическое и информационное обеспечение дисциплины
5.1. Рекомендуемая литература
5.1.1. Основная литература:

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

5.1.2. Дополнительная литература:

1. Айдинян, А.Р. Аппаратные средства вычислительной техники: учебник / А.Р. Айдинян. - М.; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

5.1.3. Перечень учебно-методического обеспечения

1. Методические указания по выполнению лабораторных работ по дисциплине «Программно-аппаратные средства защиты информации».
2. Методические указания по выполнению практических работ по дисциплине «Программно-аппаратные средства защиты информации».
3. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине дисциплине «Программно-аппаратные средства защиты информации».

5.1.4. Интернет-ресурсы

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»