Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра аналитических и цифровых технологий

«Утверждаю»
Проректор по учебно-методической
работе_____ Ю.А.Устименко
« 30» июня 2022 г.

Рабочая программа дисциплины
Б1.В.ДВ.7.1 Основы информационной безопасности

Направление подготовки: 38.03.02 Менеджмент
Направленность (профиль): Цифровой маркетинг и бренд-менеджмент
Форма обучения: очная
Курс – 4
Семестр – 8
Всего зачетных единиц – 4, часов – 144.

Форма отчетности: зачет – 8 семестр.

Программу разработал
кандидат физико-математических наук, доцент Д.С.Букачев

Одобрена на заседании кафедры аналитических и цифровых технологий
«23» июня 2022 года, протокол № 10

Заведующий кафедрой _____ Д.С. Букачев

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору образовательной программы подготовки 38.03.02 Менеджмент, направленность (профиль): Цифровой маркетинг и бренд-менеджмент.

Изучение дисциплины предполагает сочетание фундаментальной подготовки с освоением технологии применения специализированных программных продуктов и систем, ориентированных на защиту экономической и служебной информации, базируется на компетенциях, сформированных при изучении дисциплины «Информатика».

При подготовке студентов по направлению 38.03.02 Менеджмент информационная подготовка имеет большое значение. Выбранная ими сфера будущей деятельности связана, как правило, с необходимостью работы с информационными системами для хранения, обработки, передачи и защиты значительных объемов экономической и служебной информации, с необходимостью принимать управленческие решения и совершать юридические действия в точном соответствии с законом, поэтому изучение соответствующих информационных технологий и систем, а также нормативно-правовой базы для их грамотного использования в обязательном порядке входит в программу обучения студентов.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индикаторы достижения
ПК-3. Способен проводить анализ, разработку и осуществление маркетинговой стратегии, стратегии развития бренда и медийной стратегии продвижения в информационно-коммуникационной сети «Интернет», направленной на обеспечение конкурентоспособности	**Знать:** основные базовые понятия стратегического менеджмента и основы осуществления маркетинговых стратегий; основные направления представления компании в сети Интернет, теоретические основы интернет-рекламы, ключевые аспекты поисковой оптимизации сайта, основы SMM-маркетинга и контекстной рекламы; основы веб-программирования и веб-дизайна; международное и российское законодательство в сфере защиты информации; основные способы безопасного хранения данных. **Уметь:** проводить анализ и разрабатывать маркетинговые стратегии, стратегии развития бренда и медийной стратегии продвижения в информационно-коммуникационной сети «Интернет»; использовать процессы внедрения информационных технологий для представления компании в интернет-среде, реализовывать организацию веб-представительства компании и его сопровождение в сети; разрабатывать и внедрять рекламные стратегии в сети Интернет, анализировать эффективность маркетинговых инструментов в Интернет-среде; разрабатывать динамические веб-страницы, проектировать дизайн веб-страниц, управлять веб-контентом; оценивать ущерб от угроз информационной безопасности и осуществлять мероприятия, направленные на профилактику правонарушений в сфере информационной безопасности.

	Владеть: навыками стратегического мышления и практического осуществления маркетинговой стратегии, стратегии развития бренда и медийной стратегии продвижения в информационно-коммуникационной сети «Интернет»; навыками работы с информационными средствами для управления различными направлениями деятельности организации в сети Интернет с целью повышения её конкурентоспособности; навыками программирования, разметки и дизайна веб-страниц с использованием специализированных программных средств; навыками обеспечения локальной и сетевой информационной безопасности, программными средствами журналирования и анализа событий безопасности.

3. Содержание дисциплины

Тема 1. Информационная безопасность и уровни ее обеспечения. Понятие «информационная безопасность». Составляющие информационной безопасности. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности». Анализ угроз информационной безопасности.

Тема 2. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов.

Тема 3. Информационная безопасность в компьютерных сетях. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.

Тема 4. Механизмы обеспечения информационной безопасности. Идентификация и аутентификация. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			Лекции	Практич. занятия	Лаборатор. занятия	Самостоя-тельная работа
1.	Информационная безопасность и уровни ее обеспечения.	34	12	0	4	18
2.	Компьютерные вирусы и защита	36	6	0	12	18

	от них.					
3.	Информационная безопасность в компьютерных сетях.	40	12	0	10	18
4.	Механизмы обеспечения информационной безопасности	34	6	0	10	18
	Всего за семестр	144	36	0	36	72

5. Виды образовательной деятельности

Занятия лекционного типа

Тема 1. Информационная безопасность и уровни ее обеспечения.

Лекция 1. Понятие «информационная безопасность». Составляющие информационной безопасности.

Лекция 2. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.

Лекция 3. Стандарты информационной безопасности: «Общие критерии».

Лекция 4. Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ.

Лекция 5. Административный уровень обеспечения информационной безопасности.

Лекция 6. Классификация угроз «информационной безопасности». Анализ угроз информационной безопасности.

Вопросы для самостоятельного изучения темы 1:

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
5. Перечислите уровни формирования режима информационной безопасности.
6. Перечислите основополагающие документы по «информационной безопасности».
7. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.
8. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
9. Какие виды требований включает стандарт ISO/IEC 15408?
10. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
11. Перечислите основные механизмы безопасности.
12. Что понимается под администрированием средств безопасности?
13. Классы защищенности межсетевых экранов.
14. Содержание административного уровня обеспечения «информационной безопасности».
15. Дайте определение политики безопасности.
16. Направления разработки политики безопасности.
17. Перечислите классы угроз информационной безопасности.

18. Назовите причины и источники случайных воздействий на информационные системы.
19. Дайте характеристику преднамеренным угрозам.
20. Перечислите каналы несанкционированного доступа.
21. Что понимается под техническим каналом утечки информации?
22. Каковы причины возникновения электромагнитных каналов утечки информации?
23. Как образуется параметрический канал утечки информации?
24. Основные угрозы целостности информации.
25. Охарактеризуйте угрозы доступности информации.

Тема 2. Компьютерные вирусы и защита от них.

Лекция 7. Вирусы как угроза информационной безопасности.

Лекция 8. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ.

Лекция 9. Антивирусные программы. Профилактика компьютерных вирусов.

Вопросы для самостоятельного изучения темы 2:

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. Поясните понятия «сканирование на лету» и «сканирование по запросу».
11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?
15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
17. Характерные черты макровируса.
18. Как проверить систему на наличие макровируса?
19. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?

Тема 3. Информационная безопасность в компьютерных сетях.

Лекция 10. Особенности обеспечения информационной безопасности в компьютерных сетях.

Лекция 11. Сетевые модели передачи данных.

Лекция 12. Модель взаимодействия открытых систем OSI/ISO.

Лекция 13. Адресация в глобальных сетях.

Лекция 14. Классификация удаленных угроз в вычислительных сетях.

Лекция 15. Типовые удаленные атаки и их характеристика.

Вопросы для самостоятельного изучения темы 3:

1. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?
2. Дайте определение понятия «удаленная угроза».
3. В чем заключается специфика методов и средств защиты компьютерных сетей?
4. Поясните понятие «глобальная сетевая атака», приведите примеры.
5. Какие протоколы образуют модель TCP/IP?
6. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?
7. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.
8. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?
9. Для чего предназначен DNS-сервер?
10. Перечислите классы удаленных угроз.
11. Как классифицируются удаленные угрозы «по характеру воздействия»?
12. Охарактеризуйте удаленные угрозы «по цели воздействия».
13. Может ли пассивная угроза привести к нарушению целостности информации?
14. Дайте определение типовой удаленной атаки.
15. Что является целью злоумышленников при «анализе сетевого трафика»?
16. Назовите причины успеха удаленной атаки «ложный объект».

Тема 4. Механизмы обеспечения информационной безопасности.

Лекция 16. Идентификация и аутентификация.

Лекция 17. Методы разграничение доступа. Регистрация и аудит.

Лекция 18. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).

Вопросы для самостоятельного изучения темы 4:

1. Что понимается под идентификацией и аутентификацией пользователя?
2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.
3. Что такое «электронный ключ»?
4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
5. Что входит в состав криптосистемы?
6. Как реализуются симметричный и асимметричный методы шифрования?
7. Что такое электронная цифровая подпись?
8. Перечислите методы разграничения доступа.
9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?
10. На чем основан механизм регистрации?
11. Какие события, связанные с безопасностью, подлежат регистрации?
12. Чем отличаются механизмы регистрации и аудита?
13. Какие этапы предусматривают механизмы регистрации и аудита?
14. В чем заключается принцип межсетевого экранирования?
15. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
16. Какие сервисы безопасности включает технология виртуальных частных сетей?
17. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
18. Чем определяется политика безопасности виртуальной частной сети?

Задания семинарского типа (лабораторные занятия)

Лабораторная работа №1 (4 часа).

Цель: научиться восстанавливать файлы, зараженные макровирусом.

Программное обеспечение и материалы: актуальная версия MS Office.

Решаемые задачи: устранение макросов из документа, работа с зараженным документом в защищенном режиме, настройка компонентов безопасности MS Office.

Задания для самостоятельного выполнения:

1. Создайте файл virus.doc (содержание – чистый лист) и выполните алгоритм восстанов-ления файла (в предположении его заражения макровирусом).
2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры (скопированные таким образом файлы вставьте в новый Word-документ для отчета преподавателю).
3. Сравните размеры файлов virus.doc и virus.rtf, используя пункт контекстного меню Свойства (для этого выделить в Проводнике файл, нажмите правую кнопку мыши и выберите пункт Свойства).

Контрольные вопросы к лабораторной работе №1:

1. Какие файлы заражают макровирусы?
2. Как просмотреть код макровируса?
3. Как восстановить файл, зараженный макровирусом?

Лабораторная работа №2 (4 часа).

Цель: осуществить профилактику заражения ОС троянскими программами.

Программное обеспечение и материалы: Regedit.

Решаемые задачи: работа с реестром операционной системы, работа с разделами реестра, отвечающими за автозапуск от имени пользователей и системы.

Задание для самостоятельного выполнения:

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE \Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\System(REG_SZ).
2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.
3. Составьте отчет о результатах проверки.

Контрольные вопросы к лабораторной работе №2:

1. Что такое реестр?
2. Поясните особенности «троянских программ».
3. Почему профилактика «троянских программ» связана с системным реестром?
4. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

Лабораторная работа №3 (4 часа).

Цель: научиться администрировать почтовый клиент Outlook Express.

Программное обеспечение и материалы: Outlook Express.

Решаемые задачи: разработка системы правил по управлению входящими сообщениями в Outlook Express и настройка Outlook Express для передачи сообщений с электронной подписью.

Задание для самостоятельного выполнения.

Создайте три новых правила (произвольных) управления сообщениями электронной почты и опишите их безопасные свойства, как и от каких угроз можно ими защитить компьютер. Составьте отчет.

Контрольные вопросы к лабораторной работе №3:

1. Для чего используется механизм электронной цифровой подписи?

2. Что понимается под сертификатом?

3. Какой метод шифрования использует электронная цифровая подпись?

Лабораторная работа №4 (4 часа).

Цель: настроить параметры аутентификации Windows.

Программное обеспечение и материалы: панель управления MS Windows.

Решаемые задачи: настройка параметров локальной политики безопасности операционной системы Windows: политика паролей, блокировки учетных записей.

Задания для самостоятельного выполнения:

1. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.

2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароле укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

3. Проведите эксперименты с другими параметрами Политики учетных записей.

Контрольные вопросы к лабораторной работе №4:

1. Что такое аутентификация и идентификация?

2. Для чего применяются эти механизмы?

3. Что можно настроить с помощью оснастки Локальная политика безопасности.

Лабораторная работа №5 (4 часа).

Цель: научиться работать с шифрующей файловой системой EFS.

Программное обеспечение и материалы: MS Windows.

Решаемые задачи: включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Задания для самостоятельного выполнения:

1. Экспортируйте сертификат № 2 из папки Промежуточные центры сертификации Root Agency (сохраните иллюстрации для отчета).

2. Импортируйте экспортированный сертификат в папку Личные (сохраните иллюстрации для отчета).

Контрольные вопросы к лабораторной работе №5:

1. Что входит в криптосистему?

2. Сравните методы шифрования с открытым и закрытым ключом (асимметричное и симметричное шифрование).

3. Что такое mmc?

4. Назначение шифрующей файловой системы EFS.

Лабораторная работа №6 (4 часа).

Цель: назначить права пользователей при произвольном управлении доступом в Windows.

Программное обеспечение и материалы: MS Windows.

Решаемые задачи: создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе, блокировать учетную запись пользователя.

Задания для самостоятельного выполнения:

1. Создайте учетную запись с именем ЛР-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого, после нажатия клавиши Print Screen вставьте скопированное изображение в новый

документ Word) для представления в качестве отчета.

2. Создайте группу Информационная безопасность и сохраните окно со списком групп Вашего компьютера для отчета.

3. Заблокируйте учетную запись ЛР-6 и после этого удалите.

Контрольные вопросы к лабораторной работе №6:

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя СмолГУ4\1? Почему?

Лабораторная работа №7 (2 часа).

Цель: настройка параметров регистрации и аудита в Windows.

Программное обеспечение и материалы: MS Windows.

Решаемые задачи: активизировать механизмы регистрации и аудита операционной системы Windows, настроить параметры просмотра аудита папок и файлов.

Задания для самостоятельного выполнения:

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для отчета.
3. Удалите созданную ранее учетную запись ЛР-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Контрольные вопросы к лабораторной работе №7:

1. Чем отличаются регистрация и аудит?
2. Что является средствами регистрации и аудита?
3. Какие события фиксируются в системном журнале?
4. Что фиксирует система при регистрации событий?

Лабораторная работа №8 (4 часа).

Цель: научиться управлять шаблонами безопасности Windows.

Программное обеспечение и материалы: MS Windows.

Решаемые задачи: загрузить редактор Шаблона безопасности, отредактировать шаблон безопасности и сохранить его с новым именем.

Задание для самостоятельного выполнения. Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ЛР-8. После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер и далее в файл для отчета.

Контрольные вопросы к лабораторной работе №8:

1. Для чего используются Шаблоны безопасности?
2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?
3. Какие разделы включает стандартный Шаблон безопасности?

Лабораторная работа №9 (4 часа).

Цель: осуществить настройку и использование межсетевого экрана в Windows.

Программное обеспечение и материалы: брандмауэр Windows.

Решаемые задачи: активизировать встроенный брандмауэр операционной системы Windows, настроить его параметры.

Задания для самостоятельного выполнения:

1. Настройте брандмауэр на работу с Веб-сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь к Интернет и посетите любой веб-сервер.
4. Завершите работу в Интернет и просмотрите журнал безопасности.

5. Зафиксируйте записи журнала безопасности для отчета.

Контрольные вопросы к лабораторной работе №9:

1. Что такое брандмауэр?
2. Какие бывают брандмауэры?
3. Что фиксирует журнал безопасности брандмауэра?

Лабораторная работа №10 (2 часа).

Цель: создать VPN-подключение средствами Windows.

Программное обеспечение и материалы: MS Windows.

Решаемые задачи: создать VPN-подключение и выполнить его настройку.

Задание для самостоятельного выполнения. Создайте VPN-подключение к узлу с адресом 122.122.122.122 и зафиксируйте окно его свойств (Print Screen) на закладке Общие (как показано на рисунке 5) в качестве отчета.

Контрольные вопросы к лабораторной работе №10:

1. Какие механизмы безопасности используются при реализации VPN-подключения?
2. Что такое «туннель» и в чем состоит принцип «туннелирования»?
3. В чем заключаются защитные функции виртуальных частных сетей?

Самостоятельная работа

Самостоятельная работа студентов направлена на углубление и закрепление знаний, а также развитие практических умений и заключается в:

- работе с лекционным материалом, поиске и анализе литературы и электронных источников информации;
- выполнении домашних заданий (домашние задания представляют из себя перечень задач, с которыми студенты не справились в ходе выполнения лабораторных работ), заданий для самостоятельного выполнения к каждой лабораторной работе, подготовке ответов на контрольные вопросы к лабораторным работам;
- изучении теоретического материала к лабораторным занятиям.

Самостоятельная работа студента по настоящему курсу является гармоничным продолжением выполнения заданий, обозначенных в рамках лабораторных работ, а также работы с лекционным материалом по его расширению при поиске ответов на вопросы для самостоятельного изучения.

Проверка качества самостоятельной работы студентов проводится во время защиты лабораторных работ. Студент должен ориентироваться в теоретической базе, необходимой для выполнения текущей работы, выполнить все задания из лабораторной и самостоятельной частей, уметь отвечать на контрольные вопросы по направлению данной работы.

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Вопросы для самостоятельного изучения

Вопросы для самостоятельного изучения темы 1:

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
5. Перечислите уровни формирования режима информационной безопасности.
6. Перечислите основополагающие документы по «информационной безопасности».
7. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.
8. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
9. Какие виды требований включает стандарт ISO/IEC 15408?
10. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
11. Перечислите основные механизмы безопасности.
12. Что понимается под администрированием средств безопасности?
13. Классы защищенности межсетевых экранов.
14. Содержание административного уровня обеспечения «информационной безопасности».
15. Дайте определение политики безопасности.
16. Направления разработки политики безопасности.
17. Перечислите классы угроз информационной безопасности.
18. Назовите причины и источники случайных воздействий на информационные системы.
19. Дайте характеристику преднамеренным угрозам.
20. Перечислите каналы несанкционированного доступа.
21. Что понимается под техническим каналом утечки информации?
22. Каковы причины возникновения электромагнитных каналов утечки информации?
23. Как образуется параметрический канал утечки информации?
24. Основные угрозы целостности информации.
25. Охарактеризуйте угрозы доступности информации.

Вопросы для самостоятельного изучения темы 2:

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.

9. Поясните механизм функционирования «троянской программы» (логической бомбы).

10. Поясните понятия «сканирование на лету» и «сканирование по запросу».

11. Перечислите виды антивирусных программ.

12. Охарактеризуйте антивирусные сканеры.

13. В чем особенности эвристических сканеров?

14. Какие факторы определяют качество антивирусной программы?

15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.

16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.

17. Характерные черты макровируса.

18. Как проверить систему на наличие макровируса?

19. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?

Вопросы для самостоятельного изучения темы 3:

1. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?
2. Дайте определение понятия «удаленная угроза».
3. В чем заключается специфика методов и средств защиты компьютерных сетей?
4. Поясните понятие «глобальная сетевая атака», приведите примеры.
5. Какие протоколы образуют модель TCP/IP?
6. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?
7. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.
8. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?
9. Для чего предназначен DNS-сервер?
10. Перечислите классы удаленных угроз.
11. Как классифицируются удаленные угрозы «по характеру воздействия»?
12. Охарактеризуйте удаленные угрозы «по цели воздействия».
13. Может ли пассивная угроза привести к нарушению целостности информации?
14. Дайте определение типовой удаленной атаки.
15. Что является целью злоумышленников при «анализе сетевого трафика»?
16. Назовите причины успеха удаленной атаки «ложный объект».

Вопросы для самостоятельного изучения темы 4:

1. Что понимается под идентификацией и аутентификацией пользователя?
2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.
3. Что такое «электронный ключ»?
4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
5. Что входит в состав криптосистемы?
6. Как реализуются симметричный и асимметричный методы шифрования?
7. Что такое электронная цифровая подпись?
8. Перечислите методы разграничения доступа.
9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?
10. На чем основан механизм регистрации?

11. Какие события, связанные с безопасностью, подлежат регистрации?
12. Чем отличаются механизмы регистрации и аудита?
13. Какие этапы предусматривают механизмы регистрации и аудита?
14. В чем заключается принцип межсетевого экранирования?
15. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
16. Какие сервисы безопасности включает технология виртуальных частных сетей?
17. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
18. Чем определяется политика безопасности виртуальной частной сети?

Примеры заданий для самостоятельного выполнения

Задание 1.

1. Настройте брандмауэр на работу с Веб-сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь к Интернет и посетите любой веб-сервер.
4. Завершите работу в Интернет и просмотрите журнал безопасности.
5. Зафиксируйте записи журнала безопасности для отчета.

Задание 2.

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для отчета.
3. Удалите созданную ранее учетную запись ЛР-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Критерии оценивания заданий для самостоятельного выполнения.

Уровень выполнения	Оценка
Задача решена в полном объёме, алгоритмические и вычислительные ошибки отсутствуют, проведен анализ полученного решения.	5 (отлично)
Задача решена в полном объёме с незначительными техническими ошибками или отсутствует анализ результатов решения.	4 (хорошо)
Задача решена не полностью или в решении присутствуют ошибки алгоритмического характера, незначительно влияющие на ход решения.	3 (удовлетворительно)
Задача не решена или в решении присутствует значительное количество ошибок алгоритмического характера, существенно влияющих на ход решения.	2 (неудовлетворительно)

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Критерии получения зачета

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации студентов в

федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет».

Для получения зачета студент должен:

- выполнить задания лабораторных работ на оценку не ниже «удовлетворительно»;
- уметь отвечать на вопросы для самостоятельного изучения на оценку не ниже «удовлетворительно»;
- выполнить задания для самостоятельного выполнения на оценку не ниже «удовлетворительно»;

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966

7.2. Дополнительная литература

1. Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие [для студентов вузов] / Е. К. Баранова, А. В. Бабаш .— 2-е изд .— М. : Риор : Инфра-М, 2014 .— 254 с.
2. . Галатенко В.А. «Основы информационной безопасности. Интернет-университет информационных технологий» – ИНТУИТ.ру, 2018.
3. Лапонина О.Р. «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Интернет-университет информационных технологий» – ИНТУИТ.ру, 2015.
4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) "Об информации, информационных технологиях и о защите информации".
5. Руководящие документы ФСТЭК и ГОСТы Российской Федерации по защите информации, а также другая литература по анализу требований к информационной безопасности, размещенные на сайте http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty
   - ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
   - ГОСТ Р ИСО/МЭК 15408-2-2013. Национальный стандарт Российской Федерации (ISO/IEC-15408)
   - Документ Гостехкомиссии РФ «Защита от несанкционированного доступа к информации. Термины и определения»

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Свободно доступные курсы Интернет-университета информационных технологий (ИНТУИТ) http://www.intuit.ru/;
2. Портал государственных и муниципальных услуг. http://www.gosuslugi.ru/;
3. Официальный сайт ЗАО «Консультант Плюс» – www.consultant.ru;
4. Официальный сайт ООО «НПП Гарант-Сервис» – www.garant.ru;
5. www.compress.ru – Сайт журнала «КомпьютерПресс».

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа. Аудитория 124 уч.к. № 2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).
Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – компьютерный класс. Аудитория 124 уч.к. №2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 16 шт., колонки Genius – 16 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).
Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ. Аудитория 124 уч.к. №2.
Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.
Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.
Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

9. Программное обеспечение

Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66920993 от 24.05.2016
Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66975477 от 03.06.2016
Dr. Web Server/Desktop Security Suite (Антивирус) Лицензия EE4E-QN5S-6FG2-N76B (Ежегодное обновление)
Kaspersky Endpoint Security для бизнеса – Стандартный, Лицензия 1FB6151216081242, ежегодное обновление.

СКЗИ КриптоПро (лицензия, интегрированная в сертификат для образовательных курсов в рамках программы академического партнерства с СКБ Контур).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 03B6A3C600B7ADA9B742A1E041DE7D81B0
Владелец: Артеменков Михаил Николаевич
Действителен: с 04.10.2021 до 07.10.2022