МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«11» 04 2023 г.

Безопасность в компьютерных сетях

Методические указания по выполнению самостоятельной работы
для студентов направления подготовки 11.03.02
«Инфокоммуникационные технологии и системы связи»

Курск 2023

УДК 004

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры «Вычислительная техника» А.В. Киселев

Безопасность в компьютерных сетях: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 17 с.: Библиогр.: с. 17.

Содержатся сведения о темах для самостоятельного изучения по дисциплине «Безопасность в компьютерных сетях», необходимые для успешного освоения дисциплины. Указывается порядок выполнения самостоятельной работы всех предусмотренных учебным планом видов, приводятся рекомендации по оформлению результатов работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи всех форм обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. Заказ. Бесплатно. 238
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

Введение

Самостоятельная работа - это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, но по его заданиям и под его контролем.

Самостоятельная работа студентов включает:

- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- отработку изучаемого материала по печатным и электронным источникам, конспектам лекций;
- подготовку к выполнению лабораторных работ;
- выполнение отчетов по лабораторным работам и подготовку к их защите;
- индивидуальные задания (решение задач, подготовка сообщений, докладов, исследовательские работы и т.п.);
- работу над творческими заданиями;
- подготовку кратких сообщений, докладов, рефератов, самостоятельное составление задач по изучаемой теме (по указанию преподавателя).

Назначение самостоятельной работы студентов.

- ***Овладение знаниями***, что достигается:

чтением текста (учебника, первоисточника, дополнительной литературы), составлением плана текста, графическим структурированием текста, конспектированием текста, выписками из текста, работой со словарями и справочниками, поиском информации в сети Интернет и т.п.;

- ***закрепление знаний,*** что достигается:

работой с конспектом лекций, обработкой текста, повторной работой над учебным материалом (учебником, первоисточником, дополнительнойлитературой), составлением плана, составлением таблиц для систематизации учебного материала, ответами на контрольные вопросы, заполнением рабочей тетради, аналитической обработкой текста (аннотирование, рецензирование, реферирование, конспект-анализ и др), составлением библиографии и т.п.;

- ***формирование навыков и умений***, что достигается:

решением задач и упражнений по образцу, решением вариативных задач, выполнением схем, выполнением расчетов, решением ситуационных задач, подготовкой к дискуссиям, проектированием и моделированием

разных видов и компонентов профессиональной деятельности, математическим описанием опытно экспериментальной работой и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от поставленной цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Текущий контроль качества выполнения самостоятельной работы может осуществляться с помощью:

- контрольного опроса;
- собеседования;
- автоматизированного программированного контроля (машинного контроля, тестирования с применением ЭВМ).

Содержание самостоятельной работы

№	Наименование раздела учебной дисциплины	Задание	Алгоритм выполнения задания	Форма представления выполненного задания
1.	Сетевая аутентификация	Подготовить реферат по определенной теме. Тематика рефератов указана в Приложении 1	1. Найти информацию по любому из источников или с помощью сети Интернет по выбранной теме (Приложение 1) 2. Оформить реферат	Реферат, оформленный в соответствии с Приложением 4
2.	Подсистема аутентификации	Подготовить реферат по определенной теме. Тематика рефератов указана в Приложении 1	1. Найти информацию по любому из источников или с помощью сети Интернет по выбранной теме (Приложение 4) 2. Оформить реферат	Реферат, оформленный в соответствии с Приложением 4
3.	Функции межсетевых экранов, профили защиты	Составить сводную таблицу функций межсетевых экранов;	1. Задание 2. Источники: УМК по дисциплине	Ссылка на файл
4.	Типы межсетевых экранов	Создать компьютерную презентацию	Используя УМК по дисциплине найти информацию о методах доступа к сети, их характеристиках, принципах работы**;** Проанализировать информацию и оформить презентацию согласно требованиям к презентации, указанным в Приложении 2	Ссылка на презентацию
5.	Основные	Составить сводную	1. Задание 2. Источники: УМК	Ссылка на файл

	компоненты межсетевых экранов, схемы подключения	таблицу основных компонентов межсетевых экранов;	по дисциплине	
6.	Программные и аппаратные средства криптографической защиты	Создание презентации «Программные и аппаратные средства криптографической защиты»	Используя УМК по дисциплине найти информацию по аппаратному обеспечению компьютерных сетей с помощью средств криптографической защиты	Ссылка на презентацию
7.	Критерии оценки защищенности криптографических модулей	Составить сводную таблицу критериев оценки защищенности криптографических модулей	3. Задание 4. Источники: УМК по дисциплине	Сводная таблица, оформленная в тетради или ссылка на файл
8.	Построение VPN	Создание презентации «Методики построения VPN»	Используя УМК по дисциплине найти информацию по методикам построения VPN	Ссылка на презентацию
9.	Туннелирование в VPN	Создание презентации «Методики туннелирования VPN»	Используя УМК по дисциплине найти информацию по методикам туннелирования VPN	Ссылка на презентацию
10.	Политики безопасности для VPN	Выполнить сравнительный анализ политик безопасности VPN	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
11.	Стандартные протоколы построения VPN	Выполнить сравнительный анализ протоколов VPN	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
12.	Проблемы и уязвимости VPN	Составьте сводную таблицу по проблемам и уязвимостям VPN	Источники: УМК по дисциплине	Сводная таблица, оформленная в тетради или ссылка на файл

13.	Аудит и мониторинг информационной безопасности	Создание презентации «Аудит в информационной безопасность компьютерных сетей»	Используя УМК по дисциплине найти информацию по методикам аудита в информационной безопасность компьютерных сетей	Ссылка на презентацию
14.	Классификация систем анализа защищенности	Выполнить сравнительный анализ систем анализа защищенности	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
15.	Критерии выбора сканеров безопасности	Составить сводную таблицу критериев выбора сканеров безопасности	Источники: УМК по дисциплине	Сводная таблица, оформленная в тетради или ссылка на файл
16.	Методы отражений вторжений	Выполнить сравнительный анализ методов отражения вторжений	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
17.	Основы построения систем обнаружения вторжений	Создание презентации «Основы построения систем обнаружения вторжений»	Используя УМК по дисциплине найти информацию по методикам построения систем обнаружения вторжений	Ссылка на презентацию
18.	Многофункциональные устройства защиты от сетевых атак	Выполнить сравнительный анализ многофункциональных устройств защиты от сетевых атак	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл

Приложение 1

Темы рефератов

№ п/п	Название темы
1	Технология Bluetooth. Архитектура, принцип работы
2	Безопасность сети. Брандмауэры
3	Безопасность веб-серверов
4	Электронная почта. История создания, структура электронной почты
5	История развития глобальной сети
6	Аппаратное обеспечение компьютерных сетей
7	Технологии локальных сетей. Сравнительная характеристика
8	Сетевые атаки. Классы атак
9	Технологии глобальных сетей. Сравнительная характеристика
10	Базы данных в Интернете
11	Алгоритмы и протоколы маршрутизации
12	Сравнительный анализ поисковых систем Интернет
13	Администрирование локальных сетей
14	Каналы связи. Спутниковая связь
15	Организация сетей. Проводная и беспроводная передача данных
16	Организация корпоративной компьютерной сети на предприятии
17	Поисковые системы
18	Проектирование локально-вычислительной сети
19	Сетевые операционные системы
20	Основы построения сетей

Текст реферата необходимо набирать в текстовом процессоре с соблюдением следующих правил:

1. Формат документа А4.
2. Ориентация: книжная.
3. Поля: верхнее — 2 см, нижнее — 2 см, левое — 2,5 см, правое — 1 см.
4. Выравнивание текста по ширине.
5. Выравнивание заголовков либо по центру, либо по левому краю

(единообразно для всей работы).

6. Установка переносов автоматическая.

7. Абзацный отступ — 1,5 см.

8. Интервал одинарный.

9. Интервал после заголовка до подзаголовка — 12 пт., до текста — 18 пт.

10. Шрифт для заголовков и подзаголовков Arial —14 пт.,

11. Шрифт для текста Times New Roman — 12 пт.

12. Начертание: для заголовка и подзаголовка — полужирный, для текста — обычный.

13. Нумерация страниц вставляется в нижний колонтитул без черточек и точек, размер шрифта 12 пт., начинается со второго листа.

14. Оформление оглавления автоматическое, располагается перед введением.

15. Переход на новую страницу необходимо делать с помощью комбинации клавиш Ctrl + Enter.

16. Нумерованные и многоуровневые списки оформляются с точкой после каждой цифры.

17. Использование маркированных списков с помощью символов:

▪ (квадратик);

• (кружочек);

- (дефис).

18. Стиль маркеров единообразный для всей работы.

19. Список использованных источников (книги, статьи, Интернет-ресурс) не менее

Требования по содержанию реферата:

1. реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

2. реферат, кроме текста, может дополнительно содержать: качественные цветные иллюстрации, фрагменты программ, исполняемые модули, фрагменты информационных систем, презентации и другие материалы качественно дополняющие основную часть реферата.

Приложение 2

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ПРЕЗЕНТАЦИИ

Электронная презентация — электронный документ, представляющий набор слайдов, предназначенный для демонстрации проделанной работы.

Целью любой презентации является визуальное представление замысла автора, максимально удобное для восприятия. Электронная презентация должна показать то, что трудно объяснить на словах.

Задачи презентации:

- привлечение внимания аудитории;
- предоставление необходимой информации, достаточной для восприятия результатов проделанной работы без пояснений;
- предоставление информации в максимально комфортном виде;
- акцентирование внимания на наиболее существенных информационных разделах.

Схема презентации:

1. Титульный слайд
2. Введение (содержание)
3. Основная часть
4. Заключение
5. Список использованных источников

Требования к оформлению слайдов:

Средний расчет времени, необходимого на презентацию ведется исходя из количества слайдов. Обычно на один слайд необходимо не более двух-трех минут.

- Необходимо использовать максимальное пространство экрана (слайда) - например, растянув рисунки. По возможности используйте верхние ¾площади экрана (слайда), т.к. с последних рядов нижняя часть экрана обычно не видна.
- Дизайн должен быть простым и лаконичным.
- Каждый слайд должен иметь заголовок.
- Слайды могут быть пронумерованы с указанием общего количества слайдов в презентации.
- Завершать презентацию следует кратким резюме, содержащим ее основные положения, важные данные, прозвучавшие в докладе, и т. д.

Оформление заголовков:

Назначение заголовка — однозначное информирование аудитории о содержании слайда. Сделать это можно, по меньшей мере, тремя способами:

озвучив тему слайда, лаконично изложив самую значимую информацию слайда или сформулировав основной вопрос слайда. В заголовке нужно указать основную мысль слайда. Из одного слайда можно вынести много смыслов и тезис в заголовке делается для того, чтобы слушатель понял, что именно он должен понять. Все заголовки должны быть выполнены в едином стиле (цвет, шрифт,размер, начертание).

- Текст слайда для заголовков должен быть размером 24 — 36 пунктов.
- Точку в конце заголовков не ставить. А между предложениями ставить.
- Не писать длинные заголовки.
- Слайды не могут иметь одинаковые заголовки. Если хочется назвать одинаково — желательно писать в конце (1), (2), (3) или Продолжение 1, Продолжение 2.

Выбор шрифтов:

Для оформления презентации следует использовать стандартные, широко распространенные пропорциональные шрифты, такие как Arial, Tahoma, Verdana, Times New Roman, Georgia и др.

Кроме того, большинство дизайнерских шрифтов, используемых обычно для набора крупных заголовков в печатных изданиях, оформления фирменного стиля, упаковок и т. д., в рамках презентации смотрятся слишком броско, отвлекают внимание от ее содержания, а порой и просто вызывают раздражение аудитории.

В одной презентации допускается использовать не более 2 – 3 различных шрифтов, хотя в большинстве случаев вполне достаточно и одного. Размер шрифта для информационного текста 18 – 22 пункта.

Цветовая гамма, текстовое наполнение:

Для презентации изначально необходимо подобрать цветовую гамму: обычно это три—пять цветов, среди которых есть как теплые, так и холодные. Очевидно, любой из этих цветов должен отлично читаться на выбранном ранее фоне; малейшее подозрение на то, что цвет шрифта хотя бы немного сливается с фоном — и что-то одно из этого подлежит немедленной замене: не вынуждайте тех, для кого делается презентация, портить зрение. Назначив каждому из текстовых элементов свой цвет, например: крупным заголовкам — красный, мелким за- головкам — зеленый, подрисуночным

подписям — оранжевый и т. п., нужно следовать такой схеме на всех слайдах.

Ни в коем случае не стоит стараться разместить на одном слайде как можно больше текста. Так как мелкий текст плохо воспринимается.

Использование рисунков, диаграмм, схем:

Обязательно иллюстрируйте презентацию рисунками, фотографиями, наглядными схемами, графиками и диаграммами. Яркие картинки привлекают внимание куда эффективнее, чем сплошной текст или. Изображению всегда следует придавать как можно больший раз- мер; если это возможно, иллюстрации стоит распределить по нескольким слайдам, нежели размещать их на одном но в уменьшенном виде. Подписи вполне допустимо располагать не над и не под изображением, а сбоку, если оно, например, имеет вертикальную ориентацию. Не следует перегружать слайд графическими объектами.

Контрольные вопросы для самоконтроля

Тема 1. Сетевая аутентификация.

1) Что называют сетевой аутентификацией?

2) Что такое авторизация?

3) Перечислите объекты воздействия в информационных системах.

4) Что входит в задачи межсетевых экранов?

5) Что называют контролируемой зоной?

Тема 2. Подсистема аутентификации.

1) Чем определяется стойкость подсистемы идентификации и аутентификации?

2) Перечислить минимальные требования к выбору пароля.

3) Перечислить минимальные требования к подсистеме парольной аутентификации.

4) Как определить вероятность подбора пароля злоумышленником в течении срока его действия?

Тема 3. Функции межсетевых экранов, профили защиты.

1) Функции межсетевых экранов.

2) Фильтрация трафика.

3) Выполнение функций посредничества.

4) Дополнительные возможности МЭ.

5) Перечень профилей защиты межсетевых экранов.

Тема 4. Типы межсетевых экранов.

1) Выделите два основных типа межсетевых экранов.

2) Какие действия по умолчанию осуществляются межсетевым экраном в

отношении трафика?

3) Является ли один из типов межсетевых экранов более безопасным, нежели другой?

4) Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?

Тема 5. Основные компоненты межсетевых экранов, схемы подключения

1) В чем заключается механизм межсетевого экранирования?

2) Дайте определение межсетевого экрана.

3) Принцип функционирования межсетевых экранов с фильтрацией пакетов.

4) На уровне каких протоколов работает «шлюз сеансового уровня»?

5) В чем особенность межсетевых экранов экспертного уровня?

Тема 6. Программные и аппаратные средства криптографической защиты.

1) Какие свойства присущи информации?

2) Дайте понятие объекта защиты информации.

3) Что относят к информационным процессам?

4) Что понимают под информационной системой?

5) Что называют информационными ресурсами?

Тема 7. Критерии оценки защищенности криптографических модулей.

1) Наиболее значимыми нормативными документами в области информационной безопасности являются?

2) Что включает в себя методика анализа защищённости?

3) Какие спецификации (шаблоны) для конфигурации наиболее распространенных системных программных средств известны?

4) Что определяют спецификации 1 и 2 уровней?

Тема 8-9. Построение VPN.Туннелирование в VPN.

1) Каким образом сети VPN обеспечивают безопасную передачу пакетов?

2) Назовите виды VPN-соединений.

3) Перечислите достоинства и недостатки протоколов PPTP и L2TP.

4) Что такое RADIUS?

Тема 10-11. Политики безопасности для VPN. Стандартные протоколы построения VPN

1)Что включает в себя защита информации в понимании VPN?

2)Что такое идентификация?

3) Как осуществляется шифрование данных?

4) Что лежит в основе технологии шифрования с открытым ключом?

Тема 12. Проблемы и уязвимости VPN.

1) Чтотакое Virtual Private Network?

2) Основные угрозы использования VPN?

3) В чем заключается атака Man-in- the-middle?

4) В чем заключается атака IdentityTheft ?

Тема 13. Аудит и мониторинг информационной.

1) Что такое аудит безопасности?

2) На какие вопросы отвечает аудит безопасности?

3) Какие функции выполняет мониторинг безопасности?

4) Для чего используется модели адаптивного управления безопасности

сети?

Тема 14. Классификация систем анализа защищенности.

1) Какими факторами определяется уровень защищенности компьютерных

систем от угроз безопасности

2) Что используют современных АС для анализа конфигурационных

параметров системного и прикладного ПО, технических средств и средств

защиты информации?

3) Какие Вам известны спецификации (SecurityBenchmarks)?

4) Что такое защищённость АС**?**

Тема 15. Критерии выбора сканеров безопасности.

1) Для чего необходим сканер уязвимости?

2) Какие сканеры уязвимости Вы знаете?

3) Что включают в себя многофункциональные сканеры уязвимости?

4) Основные функции сканера SymantecSecurityCheck?

5) Недостатки сканера Nessus?

Тема 16. Методы отражений вторжений.

1) Какие методы обнаружения Вам известны?

2) Преимущество способа обнаружения аномалий?

3) Какие атаки могут выполнять злоумышленники?

4) Могут ли сетевые системы обнаружения вторжений взаимодействовать с другими системами безопасности?

Тема 17. Основы построения систем обнаружения вторжений.

1) Что такое системы обнаружения вторжения?

2) Основные элементы системы обнаружения?

3) Какие типы датчиков Вам известны?

4) Что такое анализатор?

Тема 18. Многофункциональные устройства защиты от сетевых атак

1) Перечислите функциональные возможности устройств защиты от сетевых атак.

2) Что такое многоуровневая защита?

3) Что такое упрощенное управление и сокращение расходов?

4) Что такое унифицированные сервисы обеспечения безопасности и автоматизация задач?

Список литературы

1) Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 частях / А. В. Пролубников. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2020. – Ч. 1. – 116 с. – URL: https://biblioclub.ru/index.php?page=book&id=614062 . – Режим доступа: по подписке. – Текст : электронный.

2) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.– URL: https://biblioclub.ru/index.php?page=book&id=429035. –Режим доступа: по подписке. – Текст : электронный.

3) Васяева, Н. С. Проектирование локальных вычислительных сетей: учебное пособие для курсового проектирования / Н. С. Васяева, Е. С. Васяева. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 94 с.– URL: https://biblioclub.ru/index.php?page=book&id=560566. – Режим доступа: по подписке. – Текст : электронный.

4) Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. – Минск : РИПО, 2019. – 180 с.– URL: https://biblioclub.ru/index.php?page=book&id=599948. – Режим доступа: по подписке. – Текст : электронный.

5) Сети и системы телекоммуникаций: учебное электронное издание / В. А. Погонин, А. А. Третьяков, И. А. Елизаров, В. Н. Назаров. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 197 с.– URL: https://biblioclub.ru/index.php?page=book&id=570531 . – Режим доступа : по подписке. – Текст : электронный.

6) Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.– URL: https://biblioclub.ru/index.php?page=book&id=429032. – Режим доступа: по подписке. – Текст : электронный.