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
«__8__» ____04_____2023 г.

Защищенные информационные системы

Методические указания по организации самостоятельной работы по дисциплине «Защищенные информационные системы» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Защищенные информационные системы: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 11 с.: Библиогр.: с. 11.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание самостоятельной работы

	Тема СРС	Задание
1	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	Напишите эссе, в котором вы определите понятие информационной системы и рассмотрите различные архитектуры, используемые при проектировании и разработке информационных систем. Объясните каждую архитектуру, приведите примеры и обсудите их преимущества и недостатки. В вашем эссе укажите на следующие пункты: 1. Определение информационной системы и ее основные составляющие. 2. Архитектура клиент-сервер. 3. Архитектура распределенных систем. 4. Архитектура многоуровневых систем. 5. Архитектура SOA (Service-Oriented Architecture) или архитектура, ориентированная на услуги. 6. Сравнительный анализ всех рассмотренных архитектур, их достоинства и недостатки. Убедитесь, что в вашем эссе присутствует четкая логическая структура, а также ясное и последовательное изложение информации.
2	Основные аспекты построения ЗИС	Напишите исследовательскую статью, в которой вы рассмотрите основные аспекты построения защищенных информационных систем. Статья должна охватить следующие пункты: Определение понятия защищенной информационной системы и постановка проблемы безопасности данных. 1. Рассмотрение угроз информационной безопасности, таких как несанкционированный доступ, атаки злоумышленников, утечки информации и вредоносное программное обеспечение. 2. Обзор основных принципов защиты информационных систем, таких как конфиденциальность, целостность и доступность данных. 3. Идентификация и аутентификация пользователей, включая методы авторизации и механизмы контроля доступа. 4. Защита сетевой инфраструктуры, включая

		использование брандмауэров, виртуальных частных сетей (VPN) и систем обнаружения вторжений (IDS). 5. Криптографические методы и алгоритмы для обеспечения конфиденциальности и целостности данных. 6. Защита от вредоносного программного обеспечения, включая использование антивирусных программ, системы обнаружения вредоносного ПО (Malware Detection) и регулярное обновление программного обеспечения. 7. Резервное копирование и восстановление данных для обеспечения возможности восстановления после сбоя или атаки. 8. Обучение и осведомленность пользователей об информационной безопасности, включая правила создания паролей, обращение с конфиденциальной информацией и распознавание социальной инженерии. 9. Соблюдение правовых и регуляторных требований, таких как законодательство о защите персональных данных (например, GDPR). В статье следует представить актуальные исследования, примеры и лучшие практики по каждому аспекту безопасности информационных систем, а также оценить их эффективность и потенциальные ограничения.
3	Описание информационной системы и особенностей ее функционирования	Напишите описание информационной системы с учетом ее основных компонентов и рассмотрите особенности ее функционирования. В вашем описании укажите на следующие пункты: 1. Введение: • Определение понятия информационной системы. • Объяснение роли информационной системы в организационном контексте. 2. Компоненты информационной системы: • Аппаратные компоненты: описание физических устройств, используемых для хранения, обработки и передачи данных (например, серверы, компьютеры, сетевое оборудование). • Программное обеспечение: объяснение

		различных типов программного обеспечения, необходимого для работы информационной системы (операционные системы, базы данных, приложения). • Данные: описание хранящихся и обрабатываемых данных в информационной системе (структура, формат, объем, источники данных). • Люди: роль пользователей информационной системы и их взаимодействие с системой (администраторы, аналитики, конечные пользователи). 3. Особенности функционирования информационной системы: • Обработка данных: объяснение процесса сбора, хранения, обработки и передачи данных в рамках информационной системы. • Контроль доступа: описание механизмов защиты данных и обеспечения конфиденциальности, целостности и доступности (авторизация, аутентификация, шифрование). • Масштабируемость: рассмотрение возможности системы изменять свою емкость и приспосабливаться к увеличению объема данных или нагрузки. • Надежность: объяснение мер, принимаемых для обеспечения непрерывной работы системы и предотвращения сбоев или потерь данных. • Интеграция: рассмотрение способов интеграции информационной системы с другими системами или компонентами (API, протоколы обмена данными). 4. Примеры информационных систем: предоставьте примеры реальных информационных систем, которые могут быть использованы для подтверждения и пояснения описанных компонентов и особенностей функционирования. В вашем описании информационной системы следует уделить внимание ясности и последовательности изложения информации, а также привести конкретные примеры для наглядности.
4	Перечень потенциальны	Составьте техническую документацию: составите перечень потенциальных источников атак на

	х источников атак и определение их возможностей (модель нарушителя	информационные системы и определите их возможности с помощью модели нарушителя. Работа должна охватить следующие пункты: 1. Введение: • Объяснение важности понимания потенциальных источников атак для обеспечения информационной безопасности. • Определение модели нарушителя и ее роль в анализе уязвимостей информационных систем. 2. Перечень потенциальных источников атак: • Внутренний нарушитель: объяснение возможности атак со стороны сотрудников или пользователей внутри организации (несанкционированный доступ, утечка данных). • Внешний нарушитель: рассмотрение атак со стороны злоумышленников вне организации (взлом, фишинг, межсетевые атаки). • Поставщики услуг и внешние контрагенты: обозначение рисков, связанных с нарушителями, имеющими доступ к информационным системам через поставщиков услуг или внешних контрагентов. • Физические угрозы: описание возможных атак, связанных с физическим доступом к оборудованию или помещениям (кража, уничтожение данных). • Социальная инженерия: объяснение методов манипуляции людьми для получения несанкционированного доступа к информации. 3. Модель нарушителя: • Определение различных типов нарушителей в модели (начинающий хакер, опытный хакер, специалист по социальной инженерии, организованная преступная группа). • Каждому типу нарушителя сопоставьте характеристики и возможности, такие как технические знания, доступ к ресурсам, цели и мотивацию. • Приведите конкретные примеры атак, которые каждый тип нарушителя может осуществить. 4. Защитные меры: • Обсуждение мер, которые можно принять для снижения риска от каждого потенциального источника атаки.

		• Рассмотрение превентивных и реактивных мер безопасности (например, обучение сотрудников, использование средств защиты информации, регулярные аудиты системы).
5	Определение уровня защищенности данных в информационной системе	Напишите практическое руководство, в котором вы проведете анализ фишинговых атак и предложите меры для защиты от них. Ваше руководство должно охватить следующие пункты: 1. Введение: Определение фишинга и его важность в контексте информационной безопасности. Объяснение распространенных форм фишинговых атак (подделка электронной почты, поддельные веб-сайты, социальные сети). 2. Анализ фишинговых атак: Обозначение основных характеристик фишинговых атак, таких как маскировка под легитимные организации, создание чувства срочности или страха, использование манипулятивных техник. Приведение примеров известных фишинговых атак и объяснение, как они могут обмануть пользователей и получить доступ к их конфиденциальной информации. 3. Меры для защиты от фишинга: Предоставление рекомендаций для пользователей по распознаванию фишинговых писем и веб-сайтов (проверка URL-адресов, подозрительных ссылок, неправильных грамматических конструкций). Обсуждение использования антивирусного программного обеспечения и фильтров электронной почты для обнаружения и блокировки фишинговых писем. Рассмотрение важности обучения сотрудников организации основам информационной безопасности и способам предотвращения фишинга. Объяснение значимости двухфакторной аутентификации для защиты от фишинговых атак. 4. Следующие шаги: Написание плана действий для применения описанных мер безопасности в реальной среде. Рассмотрение необходимости постоянного обновления мер безопасности и осведомленности о новых методах фишинга.

		В вашем руководстве следует предоставить четкое понимание фишинговых атак и методов, которые могут быть использованы для их предотвращения. Используйте актуальные примеры фишинговых атак и демонстрации для улучшения наглядности.
6	Описание угроз безопасности информации (модель угроз безопасности информации)	Составьте реферат на тему "Описание угроз безопасности информации и модель угроз безопасности информации". Ваш реферат должен включать следующие аспекты: 1. Определение и общее описание понятия "угрозы безопасности информации". Объясните, что подразумевается под угрозами безопасности информации и почему это является актуальной проблемой в современном информационном обществе. 2. Классификация угроз безопасности информации. Рассмотрите различные типы угроз, такие как вирусы, вредоносное программное обеспечение, фишинг, социальная инженерия и другие. Поясните каждый тип угрозы и приведите примеры. 3. Модель угроз безопасности информации. Объясните, что такое модель угроз безопасности информации и как она помогает в анализе и предотвращении угроз. Рассмотрите основные компоненты модели угроз, такие как уязвимости, потенциальные угрозы, вероятность и воздействие угроз. 4. Методы защиты от угроз безопасности информации. Дайте обзор основных методов и стратегий, используемых для защиты информации от угроз. Упомяните такие методы, как аутентификация, шифрование, межсетевые экраны, обучение сотрудников и другие. 5. Заключение. Подведите итоги реферата, подчеркните важность эффективной защиты информации от угроз безопасности и возможные последствия небрежного подхода к этой проблеме. Обратите внимание на структуру реферата, ясное и логическое изложение материала, приведение примеров и использование актуальных источников информации.

7	Методы выбора системы защиты информации	Сделайте презентацию на тему "Методы выбора системы защиты информации". Ваша презентация должна включать следующие слайды: 1. Интро: Краткое введение в проблематику защиты информации и необходимость выбора подходящей системы защиты. 2. Оценка потребностей: Объясните, почему важно начать с оценки потребностей организации в области защиты информации. Рассмотрите факторы, которые следует учитывать при определении требований к системе защиты. 3. Анализ рисков: Объясните, что такое анализ рисков и как он помогает в выборе системы защиты информации. Рассмотрите различные методы и подходы к проведению анализа рисков, такие как оценка вероятности и воздействия угроз, учет стоимости потерь и другие факторы. 4. Типы систем защиты: Представьте различные типы систем защиты информации, такие как брандмауэры, системы обнаружения вторжений (IDS), системы управления доступом (ACS), системы шифрования данных и другие. Опишите каждый тип системы и объясните, в каких случаях они могут быть наиболее эффективными. 5. Сравнительный анализ: Проведите сравнительный анализ различных систем защиты информации на основе их возможностей, преимуществ, недостатков, стоимости и других факторов. Представьте таблицу или графики для наглядного сравнения. 6. Выбор оптимальной системы: Объясните, какие факторы следует учитывать при выборе оптимальной системы защиты информации. Упомяните такие факторы, как соответствие требованиям организации, бюджетные ограничения, удобство использования, потенциал для будущего развития и другие. 7. Реализация и поддержка: Обсудите вопросы реализации выбранной системы защиты информации, включая процесс внедрения, обучение персонала и мониторинг работы системы. Также обсудите важность систематической поддержки и обновления системы защиты для обеспечения ее эффективности в долгосрочной перспективе. 8. Заключение: Подведите итоги презентации,

		подчеркните важность правильного выбора системы защиты информации и ее роли в обеспечении безопасности данных организации.
8	Руководящие документы ФСТЭК России	Изучите руководящие документы Федеральной службы технического и экспортного контроля (ФСТЭК России) и подготовьте краткий обзор, в котором вы опишете основные принципы и нормативные требования, предусмотренные этими документами. Ваш обзор должен включать следующие пункты: 1. Общая информация о ФСТЭК России: цели, задачи, компетенция. 2. Описание руководящих документов ФСТЭК России: указать наиболее важные документы, их назначение и сферу применения. 3. Основные принципы и положения, установленные руководящими документами: например, требования к защите информации, стандарты безопасности, процедуры сертификации и аккредитации. 4. Примеры практического применения руководящих документов: описать случаи, когда эти документы были использованы для обеспечения безопасности информационных систем или защиты конфиденциальной информации. Обзор должен быть структурированным, содержательным и информативным. Используйте доступные ресурсы для изучения документов ФСТЭК России и анализа их содержания. Представьте ваш обзор в форме письменного доклада, применяя четкое изложение и академический стиль написания.

Перечень литературы

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. – Новосибирск : Новосибирский государственный технический университет, 2018. – 80 с. – URL: https://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4.Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

5.Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.