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__» 08 __________ 2023 г.

Теоретические основы компьютерной безопасности

Методические указания по организации самостоятельной работы по дисциплине «Теоретические основы компьютерной безопасности» 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

Теоретические основы компьютерной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 9 с.: Библиогр.: с. 9.

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

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	Основные аспекты построения системы информационной безопасности	1. Исследуйте и составьте список основных компонентов системы информационной безопасности. 2. Разработайте документ, описывающий политику безопасности компании. 3. Исследуйте и опишите методы обеспечения защиты данных в сетевом окружении. 4. Создайте план восстановления после сбоев и чрезвычайных ситуаций.
2	Угрозы информационной безопасности, оценка риска их возникновения	1. Составьте список наиболее распространенных угроз информационной безопасности и опишите их характеристики. 2. Исследуйте методы оценки риска информационной безопасности и выберите наиболее подходящий для вашей ситуации. 3. Проведите анализ риска конкретной системы или организации и определите наиболее вероятные и воздействующие угрозы. 4. Разработайте планы митигации угроз, опасность которых была выявлена в процессе анализа риска.
3	Персональные данные, защита авторских прав	1. Изучите законы и регуляции, касающиеся защиты персональных данных в вашей стране или регионе. 2. Создайте политику конфиденциальности и защиты персональных данных для вашей организации или проекта. 3. Исследуйте методы шифрования и анонимизации персональных данных и предложите решение для их защиты. 4. Изучите международные правовые акты и рекомендации по защите авторских прав и опишите основные положения и требования.
4	Выявление контрафактной продукции	1. Исследуйте методы выявления контрафактной продукции. 2. Определите характеристики контрафактных товаров и разработайте систему признаков, по которым можно идентифицировать контрафакт. 3. Разработайте алгоритмы автоматизированной обработки данных для поиска и анализа контрафактных товаров. 4. Проведите исследование рынка и оцените степень распространенности контрафактной продукции в конкретной отрасли.

5	Криптографические методы защиты	1. Изучите принципы работы криптографических алгоритмов и методов шифрования. 2. Исследуйте различные криптографические протоколы и алгоритмы, такие как AES, RSA, и ECC. 3. Разработайте программу для шифрования и дешифрования данных с использованием выбранного криптографического метода. 4. Изучите атаки на криптографические системы и предложите методы защиты от них.
6	Методы выбора системы защиты информации	1. Исследуйте различные системы защиты информации, такие как фаерволы, интранеты и системы обнаружения вторжений. 2. Разработайте список требований и критериев, которые должна удовлетворять система защиты информации для вашей организации или проекта. 3. Сравните различные системы защиты информации на основе выбранных критериев и выберите наиболее подходящую систему. 4. Подготовьте презентацию, где вы объясните выбор выбранной системы защиты информации и обоснуйте его преимущества.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тема 1. Основные аспекты построения системы информационной безопасности.

1. Основные объекты информационной безопасности
2. Что является основными рисками информационной безопасности
3. Что относят к основным принципам обеспечения информационной безопасности
4. Что является принципом политики информационной безопасности
5. Какие основные цели должна преследовать система информационной безопасности организации?
6. Какие основные компоненты должны входить в систему информационной безопасности и как они взаимодействуют между собой?
7. Каким образом должны быть определены роли и полномочия людей, ответственных за обеспечение информационной безопасности в организации?
8. Как происходит процесс идентификации и классификации информационных активов, а также определение уровней их защиты?
9. Каким образом организация обеспечивает непрерывность бизнес-процессов и восстановление после сбоев или инцидентов в системе информационной безопасности?
10. Как проводится аудит и мониторинг системы информационной безопасности для выявления уязвимостей и своевременного реагирования на потенциальные угрозы?

Тема 2. Угрозы информационной безопасности, оценка риска их возникновения.

1. Что относят к правовым методам обеспечения информационной безопасности
2. Перечислите виды информационной безопасности
3. Цели информационной безопасности
4. Что является угрозой информационной системы
5. Какие основные типы угроз информационной безопасности существуют и как они могут нанести вред организации?
6. Как проводится оценка риска возникновения угроз информационной безопасности и какие факторы учитываются при этом?

7. Каким образом определяется вероятность возникновения угрозы информационной безопасности и какие критерии применяются для оценки её воздействия?

8. Какие меры безопасности могут быть предприняты для сокращения вероятности возникновения угроз информационной безопасности?

9. Как осуществляется мониторинг и обновление оценки риска, чтобы быть в курсе изменений угроз и принимать соответствующие меры?

10. Какие процедуры и планы чрезвычайных ситуаций разрабатываются для реагирования на угрозы информационной безопасности и смягчения их последствий?

Тема 3. Персональные данные, защита авторских прав.

1. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?

2. Что такое персональные данные в соответствии с ФЗ-152?

3. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?

4. Раскройте понятие "конфиденциальный документ"

5. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.

6. Какие данные считаются персональными и почему их защита является важной составляющей информационной безопасности?

7. Какие принципы и нормы регулируют обработку и хранение персональных данных в соответствии с требованиями конфиденциальности?

8. Каким образом организация может обеспечить безопасность персональных данных в процессе их сбора, хранения и передачи?

9. Какие меры и политики защиты авторских прав должны быть включены в систему информационной безопасности организации?

10. Как осуществляется мониторинг и контроль доступа к персональным данным и материалам с авторскими правами?

11. Каким образом происходит уничтожение или анонимизация персональных данных после их использования или устранения необходимости их хранения?

Тема 4. Выявление контрафактной продукции.

1. Какие преимущества и недостатки объективных и эвристических методов экспертизы?

2. Что понимается под сенсорным анализом и сенсорной чувствительностью?

3. Что такое порог чувствительности, распознавания?

4. Причины фальсификации продовольственных товаров в современных условиях

5. Место и роль идентификации при оценке степени соответствия товара

6. Какие методы и технологии могут быть использованы для выявления контрафактной продукции в информационной среде?

7. Как происходит мониторинг и идентификация поддельных или нелицензионных программных продуктов?

8. Каким образом проводится анализ и проверка подлинности цифровых документов и электронной печати для предотвращения контрафакции?

9. Какие методы могут быть применены для обнаружения плагиата или незаконного использования интеллектуальной собственности?

10. Как осуществляется сотрудничество с органами правопорядка и другими организациями в борьбе с контрафактной продукцией?

11. Какие проведены регулярные проверки и ревизии в организации, чтобы обнаруживать и предотвращать случаи контрафакции?

Тема 5. Криптографические методы защиты.

1. Что такое шифрование?

2. Что такое кодирование?

3. Для восстановления защитного текста требуется

4. Сколько лет назад появилось шифрование?

5. Как работают криптографические методы защиты и как они могут обеспечить конфиденциальность и целостность информации?

6. Какие алгоритмы шифрования и протоколы могут быть применены для защиты данных и обмена информацией?

7. Как осуществляется генерация и хранение криптографических ключей, и какие меры обеспечивают их конфиденциальность и защиту от несанкционированного использования?

8. Каким образом осуществляется аутентификация и проверка подлинности сообщений и данных с использованием криптографических методов?

9. Какие меры безопасности применяются для защиты криптографических систем от взлома или компрометации?

10. Как осуществляется управление и обновление криптографических протоколов и алгоритмов для обеспечения их актуальности и надежности?

Тема 6. Методы выбора системы защиты информации.

1. Какую длину имеет IP-адрес
2. Какую длину блока использует алгоритм DES
3. Какую длину ключа использует алгоритм DES
4. Для чего используется алгоритм Диффи-Хеллмана
5. Какие факторы следует учитывать при выборе системы защиты информации для организации?
6. Как происходит анализ требований и потребностей организации для определения необходимых функций и возможностей системы защиты информации?
7. Какие критерии принятия решения используются при выборе системы защиты информации, такие как совместимость, надежность, цена и поддержка?
8. Каким образом проводится сравнительный анализ различных вендоров и поставщиков систем защиты информации?
9. Как осуществляется тестирование и оценка производительности выбранной системы защиты информации перед ее внедрением?
10. Как осуществляется обучение и подготовка сотрудников организации для работы с выбранной системой защиты информации?

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

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. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. 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.

4. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5. Системы защиты информации в ведущих зарубежных странах : учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. – URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.