Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Кафедра телекоммуникационных технологий и сетей

Гладких Анатолий Афанасьевич

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
для семинарских (практических) занятий, лабораторного практикума
и самостоятельной работы
по дисциплине

«Обеспечение информационной безопасности в инфокоммуникациях»

для студентов направления
11.04.02 Инфокоммуникационные технологии и системы связи,

Ульяновск
2023

Методические рекомендации для семинарских (практических) занятий, лабораторного практикума и самостоятельной работы по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях» / составитель: А.А. Гладких - Ульяновск: УлГУ, 2023 – 21 с.

Настоящие методические рекомендации предназначены для студентов направления обучения 11.04.02 Инфокоммуникационные технологии и системы связи. В работе приведены литература по дисциплине, темы дисциплины и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля, задания для самостоятельной работы, задачи и упражнения для самостоятельной подготовки к семинарам или полностью самостоятельного освоения практических навыков, задания для лабораторного практикума и рекомендации по их выполнению.

Студентам всех форм обучения следует использовать данные методические рекомендации при подготовке к семинарам, самостоятельной подготовке, а также промежуточной аттестации по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях».

Рекомендованы к введению в образовательный процесс

Учёным советом факультета математики, информационных и авиационных технологий УлГУ

протокол № 4/23 от «16» мая 2023 г.

СОДЕРЖАНИЕ

ОБЩИЕ ВОПРОСЫ

В результате изучения дисциплины «Обеспечение информационной безопасности в инфокоммуникациях» студенты:

должны знать:

- модели угроз несанкционированных действий (НСД) к сетям телекоммуникаций;
- методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним;
- национальные, межгосударственные и международные стандарты в области защиты информации состояние и перспективы развития систем защиты сетей телекоммуникаций от НСД;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;;

должны уметь:

- выявлять и оценивать угрозы НСД к сетям телекоммуникаций;
- проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей телекоммуникаций от НСД;

должны владеть:

- навыками выявления угроз НСД к сетям телекоммуникаций;
- навыком оценки уязвимостей телекоммуникационных систем с точки зрения возможности НСД к ним;
- навыком выработки предложений по предотвращению и нейтрализации угроз НСД к сетям телекоммуникаций.

Методические рекомендации предлагают указания по всем темам дисциплины. Методические рекомендации разбиты по темам и содержат набор вопросов для систематизации теоретического материала, полученного на лекционных занятиях, и самостоятельного изучения теории, вопросы (тесты) для текущего контроля на практических занятиях (семинарах), задачи для усвоения практических навыков. Для лабораторного практикума приведены задания, варианты и рекомендации по выполнению лабораторных работ.

Список литературы и информационного обеспечения, приведённый в конце методических указаний, может служить основой для изучения всех рассматриваемых тем.

Дополнительная и учебно-методическая литература могут быть использованы обучающимися для закрепления изучаемого материала.

РЕКОМЕНДАЦИИ ПО ОТДЕЛЬНЫМ ТЕМАМ ДИСЦИПЛИНЫ

Тема 1. Защита информации. Основные понятия.

Основные вопросы темы

1. Понятие и сущность защиты информации.
2. Угрозы безопасности информации в комплексах средств автоматизации.

Рекомендации по изучению темы

Вопрос 1 в основном изложен в литературе [2] на с. 8-39.

Вопрос 2 в основном изложен в литературе [3] на с. 16-37.

Вопросы для самоподготовки

Рекомендуется после изучения материалов лекций, рекомендованной литературы и ресурсов информационно-коммуникационной сети Интернет подготовить ответы на следующие вопросы:

1. Основные определения.
2. Понятие защиты информации.
3. Сущность защиты информации.
4. Перечислить угрозы безопасности информации в комплексах средств автоматизации.
5. Дать краткую характеристику угрозам безопасности информации в комплексах средств автоматизации..

Тема 2. Алгоритмы шифрования данных.

Основные вопросы темы

1. Симметричные алгоритмы шифрования.
2. Ассиметричные алгоритмы шифрования
3. Понятие ключевой документации. Инфраструктура открытых ключей.
4. Новые направления в криптографии: мультибазисная криптография, квантовое распределение ключей.

Рекомендации по изучению темы

Вопрос 1 в основном изложен в литературе [2] на с. 50-74.

Вопрос 2 в основном изложен в литературе [3] на с. 20-43.

Вопрос 3 в основном изложен в литературе [3] на с. 44-60.

Вопрос 4 в основном изложен в литературе [5] на с. 24-30.

Вопросы для самоподготовки

Рекомендуется после изучения материалов лекций, рекомендованной литературы и ресурсов информационно-коммуникационной сети Интернет подготовить ответы на следующие вопросы:

1. Перечислить основные симметричные алгоритмы шифрования.
2. Перечислить основные ассиметричные алгоритмы шифрования
3. Дать понятие ключевой документации.
4. Раскрыть понятие «инфраструктура открытых ключей».
5. Обьяснить в чем смысл мультибазисной криптографии,
6. Пояснить понятие «квантовое распределение ключей».

Тема 3. Информационная безопасность.

Основные вопросы темы

1. Особенности построения защиты информации в АСУ.
2. Особенности построения защиты информации в системах телекоммуникации.
3. Принципы комплексирования средств защиты информации.

Рекомендации по изучению темы

Вопрос 1 в основном изложен в литературе [3] на с. 71-89.

Вопрос 2 в основном изложен в литературе [4] на с. 42-50.

Вопрос 3 в основном изложен в литературе [4] на с. 73-82

Вопросы для самоподготовки

Рекомендуется после изучения материалов лекций, рекомендованной литературы и ресурсов информационно-коммуникационной сети Интернет подготовить ответы на следующие вопросы:

1. Перечислить основные особенности построения защиты информации в АСУ.
2. Назвать особенности построения защиты информации в системах телекоммуникации.
3. Раскрыть смысл комплексирования средств защиты информации.
4. Перечислить основные характеристики используемых в настоящее время средств защиты информации.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Общие методические указания к лабораторным работам.

Представленный ниже порядок выполнения лабораторных работ является рекомендуемым, однако, на усмотрение обучающегося может быть изменен исходя из его индивидуальной траектории обучения.

При выполнении работы рекомендуется воспользоваться предлагаемой литературой из списка. Однако, в современных условиях обучения, характеризующихся взрывном ростом технологий дистанционного обучения и стремительным развитием образовательных ресурсов и сервисов, материалы с официальных сайтов информационно-коммуникационной сети Интернет всегда являются более предпочтительными.

Благодаря своей новизне, возможности открыто обсуждать недостатки изложенного материала и своевременному его обновлению предпочтение целесообразно отдавать именно ему. Также достоинством использования материала из Интернет, является возможность создания собственной библиотеки необходимого учебного материала и возможность делиться ею с коллегами в отсутствие оплаты за данные ресурсы.

При использовании библиотечных ресурсов, необходимо принимать во внимание отсутствие оффлайн доступа и период доступа к библиотечным сервисам, ограниченный необходимостью платной подписки. Подписка на конкретный ресурс не гарантируется на весь период обучения, а альтернативный вариант может не содержать необходимого литературного источника.

Так как современные поисковые сервисы осуществляют доставку ссылок на интересующий контент в режиме реального времени, студентам рекомендуется развивать в себе способности и формировать компетенции быстрого поиска интересующий их технической информации, реферативной выборки из найденной информации главной и изложение её в форме, способствующей её пониманию и усвоению с учетом индивидуальных особенностей каждого обучающегося. Тем более, что построение индивидуальной траектории обучения в современных условиях просто невозможно осуществить, опираясь только на изучение рекомендованных страниц из списка рекомендованной литературы с избранных библиотечных сайтов и сайтов отдельных издательств.

Так же, режим изучения материала по рекомендованным диапазонам страниц не предполагает альтернативных вариантов рассмотрения поставленных вопросов и задач,

что также снижает творческую активность, сужает кругозор студента и лишает его возможности тренировки критического инженерного мышления.

Таким образом, при оценке работы будет обязательно учитываться способность студента самостоятельно осуществлять поиск необходимой технической информации, включая инструкции к используемым программам, умение использовать навыки чтения технического текста на английском языке и усвоения материала с различных видео- и стриминговых хостингов, включая англоязычные ресурсы для специалистов в области информационных технологий.

Лабораторная работа №1. Исследование морфологической модели информационной безопасности и защиты информации.

Цель работы: Получить практические навыки в исследование морфологической модели информационной безопасности и защиты информации.

Задание:

- осуществить исследование морфологической модели информационной безопасности
- провести исследование морфологической модели защиты информации,

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: морфологическая модель информационной безопасности и защиты информации. В отчёте по лабораторной работе должны описаны перечни работ, выполненных в ходе исследования.

Лабораторная работа №2. Исследование концептуальной модели информационной безопасности.

Цель работы: Получить практические навыки в аисследовании концептуальной модели информационной безопасности.

Задание:

- осуществить исследование концептуальной модели информационной безопасности.
- Провести сравнение с морфологической моделью защиты информации,

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: концептуальная модель информационной безопасности и защиты информации. В отчёте по лабораторной работе должны описаны перечни работ, выполненных в ходе исследования.

Лабораторная работа №3. Исследование шифра замены.

Цель работы: Получить практические навыки в исследовании шифра замены.

Задание:

- Изучить шифра замены.
- Исследовать шифр замены.
- Сделать выводы о стойкости шифра замены.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: шифр замены, стойкость шифра замены. В отчёте по лабораторной работе должны описаны перечни работ, выполненных в ходе исследования.

Лабораторная работа №4. Исследование принципа тотальной пробы ключей.

Цель работы: Получить практические навыки в исследовании тотальной пробы ключей.

Задание:

- Изучить принцип тотальной пробы ключей.
- Исследовать принцип тотальной пробы ключей.
- Сделать выводы об особенностях использования метода тотальной пробы ключей.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: принцип тотальной пробы ключей.

В отчёте по лабораторной работе должны описаны действия по исследованию принципа тотальной пробы ключей и особенностях использования метода тотальной пробы ключей.

Выбор приложений для осуществления лабораторной работы должен быть осуществлён студентом самостоятельно. Рекомендуется в первую очередь использовать приложения из состава операционных систем (при их наличии).

Лабораторная работа №5. Принцип получения шифра гаммирования.

Цель работы: Получить практические навыки в исследовании шифра гаммирования.

Задание:

- Изучить шифра гаммирования.
- Исследовать шифр гаммирования.
- Сделать выводы о стойкости шифра гаммирования.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: шифр гаммирования, стойкость шифра гаммирования. В отчёте по лабораторной работе должны описаны перечни работ, выполненных в ходе исследования.

Лабораторная работа №6. Оценка расстояния единственности на примере шифра замены.

Цель работы: Получить практические навыки в оценке расстояния единственности на примере шифра замены.

Задание:

- Изучить понятие расстояния единственности.
- Изучить вопросы оценки расстояния единственности.
- Осуществить оценку расстояния единственности на примере шифра замены.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: расстояние единственности, оценка расстояния единственности . В отчёте по лабораторной работе должны описаны перечни работ, выполненных в ходе исследования.

Результаты полученного поиска и выбора приложений описать в отчёте с выводами, показывающими особенности оценки расстояния единственности на примере шифра замены.

Лабораторная работа №7. Алгоритм Шора и его особенности.

Цель работы: Получить практические навыки в исследовании алгоритма Шора.

Задание:

- Изучить алгоритм Шора.
- Исследовать особенности алгоритма Шора.
- Сделать выводы о стойкости алгоритма Шора.
- Зашифровать и расшифровать информацию алгоритмом Шора.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: алгоритм Шора.

В отчёте по лабораторной работе должны описаны действия по исследованию принципа тотальной пробы ключей и особенностях использования метода тотальной пробы ключе функционирования алгоритм Шора.

Выбор приложений для осуществления лабораторной работы должен быть осуществлён студентом самостоятельно. Рекомендуется в первую очередь использовать приложения из состава операционных систем (при их наличии).

Лабораторная работа №8. Принцип составления и анализа матриц инцидентности в системе информационной безопасности.

Цель работы: Получить практические навыки в составлении и анализе матриц инцидентности в системе информационной безопасности.

Задание:

- Составить матрицу инцидентности в системе информационной безопасности.
- Провести анализ матрицы инцидентности в системе информационной безопасности.
- Сформировать выводы по проделанной работе.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: матрицы инцидентности в системе информационной безопасности, анализ матрицы инцидентности в системе информационной безопасности.

В отчёте по лабораторной работе должны описаны действия по анализу матрицы инцидентности в системе информационной безопасности.

Выбор приложений для осуществления лабораторной работы должен быть осуществлён студентом самостоятельно. Рекомендуется в первую очередь использовать приложения из состава операционных систем (при их наличии).

Лабораторная работа №9. Исследование матриц инцидентности на основе принципов искусственного интеллекта.

Цель работы: Получить практические навыки в составлении и анализе матриц инцидентности на основе принципов искусственного интеллекта.

Задание:

- Составить матрицу инцидентности в системе информационной безопасности.
- Провести анализ матрицы инцидентности в системе информационной безопасности на основе принципов искусственного интеллекта.
- Сформировать выводы по проделанной работе.

Отчет по лабораторной работе должен содержать:

1. Фамилию и номер группы учащегося, задание
2. Краткое описание порядка выполнения работы с подтверждением в виде фотографий или скриншотов.
3. Выводы, полученными в результате выполнения работы.
4. Отчёт должен быть размещен в Электронной информационно-образоватлеьной среде УлГУ (https://portal.ulsu.ru).

Методические указания по выполнению лабораторной работы

Для выполнения лабораторной работы студенту необходимо изучить материалы согласно предложенного списка литературы и ресурсов информационно-коммуникационной сети Интернет. Осуществить поиск по ключевым словам: матрицы инцидентности в системе информационной безопасности, анализ матрицы инцидентности в системе информационной безопасности на основе принципов искусственного интеллекта.

В отчёте по лабораторной работе должны описаны действия по анализу матрицы инцидентности в системе информационной безопасности на основе принципов искусственного интеллекта.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Список рекомендуемой литературы

основная

1) Гатченко, Н.А. Криптографическая защита информации [Электронный ресурс]: Учебное пособие / Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев - СПб.: НИУ ИТМО, 2012. - 142 с. – Режим доступа: http://window.edu.ru/resource/614/78614/files/itmo929.pdf. – Заглавие с экрана.
2) Гладких А.А. Основы современных криптографических систем и перспективы их развития. А.А. Гладких , В.Е. Дементьев, Н.Ю. Чилихин. – Ульяновск : УлГТУ, 2020. – 214 с.

дополнительная

3) Федеральный портал Единое окно доступа к образовательным ресурсам http://window.edu.ru/library
4) Научная электронная библиотека http://elibrary.ru/defaultx.asp
5) РГБ фонд диссертаций http://diss.rsl.ru/
6) Портал об управленческом менеджменте, консалтинге и маркетинге http://www.cfin.ru
7) Федеральный образовательный портал Экономика. Социология. Менеджмент http://ecsocman.edu.ru/
8) Портал по экономике http://economicus.ru
9) Научно-образовательный портал http://eup.ru/

учебно-методическая

10) Администрирование инфокоммуникационных сетей: лабораторный практикум/ В.А. Лукьянов, В.П. Смолеха. – Ульяновск: УлГУ, 2014 – 198 с.

Программное обеспечение

1. ОС Windows.
2. ОС Linux.
3. Sublime Text
4. Visual Studio
5. Kaggle (https://www.kaggle.com/),(open source).
6. IDE Google Colaboratory (https://colab.research.google.com/) (open source).
7. Official repositories open source software.
8. Отечественные ОС и прикладное ПО с российских репозиториев.