Приложение 1 к РПД Защита информации
01.03.02 Прикладная математика и информатика
направленность (профиль)
Управление данными и машинное обучение
Форма обучения – очная
Год набора – 2021

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.	Кафедра	Математики, физики и информационных технологий
2.	Направление подготовки	01.03.02 Прикладная математика и информатика
3.	Направленность (профиль)	Управление данными и машинное обучение
4.	Дисциплина (модуль)	Б1.О.17.04 Защита информации
5.	Форма обучения	Очная
6.	Год набора	2021

I. Методические рекомендации по организации работы студентов во время проведения лекционных занятий

Приступая к изучению дисциплины, студенту необходимо внимательно ознакомиться с тематическим планом занятий, списком рекомендованной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий. Самостоятельная работа студента предполагает работу с научной и учебной литературой, справочниками по программам компьютерной графики. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий и лабораторных работ.

В процессе освоения дисциплины студенты:

- изучают рекомендованную научно-практическую и учебную литературу;
- выполняют задания, предусмотренные для самостоятельной работы.

Основными видами аудиторной работы студентов являются лекции и лабораторные работы.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на семинарское занятие и указания на самостоятельную работу.

Лабораторные работы служат для закрепления изученного теоретического материала, применения полученных знаний для выполнения индивидуальных заданий, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Качество учебной работы студентов преподаватель оценивает с использованием технологической карты дисциплины, размещенной на сайте МАГУ.

II. Планы лабораторных работ

Лабораторная работа № 1 «Реализация дискреционной политики безопасности» (4 часа)

План

1. Изучение различных моделей и реализаций политик безопасности на примере дискреционной политики.
2. Реализация программного модуля на известном языке программирования, создающий матрицу доступа субъектов информационной безопасности (ИБ) к объектам ИБ.
3. Реализация системы контроля доступа для выполнения требований ИБ.

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

Лабораторная работа № 2 «Количественная оценка стойкости парольной защиты» (4 часа)

План

1. Изучение основных подходов к генерации паролей, минимальных требований и подходов к обеспечению требуемого уровня ИБ.
2. Реализация программы генерации паролей с требуемыми параметрами безопасности.
3. Оценка качества сгенерированного пароля.

Контрольные вопросы

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 течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Лабораторная работа № 3 «Ассиметричные алгоритмы шифрования данных» (4 часа)

План

1. (по вариантам) Разработка консольного/графического приложения для шифрования/дешифрования произвольных файлов по алгоритму RSA.
2. (по вариантам) Разработать визуальное приложение для шифрования/дешифрования произвольных файлов.
3. (по вариантам) Разработать клиент-серверное приложение для защищённой передачи файлов по сети.
4. (по вариантам) Разработать клиент-серверное приложение для защищённого обмена сообщениями по сети.

Контрольные вопросы

1. Дайте определение алгоритма с открытым ключом.
2. Сколько этапов содержит алгоритм RSA?
3. В чем заключается вычисление ключей алгоритма RSA?
4. Как происходит шифрование в алгоритме RSA?
5. Как происходит дешифрование в алгоритме RSA?

Лабораторная работа № 4 «Стандарт DES» (4 часа)

План

1. Изучение алгоритма симметричного шифрования DES.
2. Реализация модуля шифрования текста.
3. Реализация модуля дешифрования текста.

Контрольные вопросы

1. Общая схема алгоритма шифрования DES.
2. Почему длина ключа для алгоритма DES равна 56 бит?
3. В чём заключается процесс расшифрования данных в DES?

Лабораторная работа № 5 «Шифры и криптоанализ»

План

1. Изучение шифра Цезаря. (по вариантам) Шифрование текста и анализ.
2. Изучение иных подстановочных шифров. Расшифровка текста при помощи частотного анализа.

Контрольные вопросы

1. В чем заключается шифр простого сдвига?
2. Как изменяются частоты проявления символов шифротекста по сравнению с открытым текстом?
3. Что делать, если размер ключа меньше размера текста?
4. Видно ли из сравнения алфавитов, что сдвиг символов – циклический?
5. Должен ли быть секретным шифр (алгоритм шифрования)?

Лабораторная работа № 6 «Электронная цифровая подпись»

План

1. Изучение свободного ПО GnuPG для шифрования и создания цифровой подписи.
2. Создание, проверка ЭЦП и попытка модификации защищенного сообщения.
3. Цифровая подпись RSA.

Контрольные вопросы

1. Для чего нужна цифровая подпись?

2. Назовите основные свойства цифровой подписи.
3. Какие схемы цифровой подписи существуют?
4. Какая схема самая распространенная? Почему?
5. Как осуществляется подпись RSA? Какое отличие подписи RSA от шифра RSA?
6. Как осуществляется подпись Эль-Гамаля?
7. Как осуществляется проверка на подлинность подписи Эль-Гамаля?

III.Методические рекомендации по подготовке доклада

Алгоритм создания доклада:
1 этап – определение темы доклада
2 этап – определение цели доклада
3 этап − подробное раскрытие информации
4 этап − формулирование основных тезисов и выводов.

Типовые темы докладов (защита модуля):
Темы докладов формулируются таким образом, чтобы расширить знания студента о конкретном программном продукте или компьютерном устройстве, а также дать представление о возможности и использования в профессиональной деятельности, например:
1. Атаки типа «DDoS – отказ в обслуживании». Разновидности, способы защиты.
2. Способы обеспечения конфиденциальности передаваемой информации через Интернет.
3. Устранение проблем с возможным вмешательством третьих лиц в процесс электронного обмена.

Требования к оформлению доклада:
1. Объем доклада – 5 страниц (без титульного листа и списка источников).
2. Титульный лист должен быть оформлен по образцу (имеется файл с образцом).
3. Основной текст работы оформлен в соответствии с требованиями, указанными ниже.
4. В случае использования в тексте таблиц и/или рисунков на каждый объект должна быть ссылка в тексте работы. Например, «... основные виды программных средств представлены ниже (см. Таблица 1)» или «... схему передачи информации можно увидеть на рис. 1».
5. Количество источников должно быть не менее трех, на все должны быть ссылки внутри текста.
6. Список используемых источников должен быть оформлен в соответствии с требованиями, указанными ниже.

Для оформления основного текста работы:
1. Шрифт – TimesNewRoman, размер – 14 пт.
2. Абзац: междустрочный интервал – 1,5; выравнивание – «по ширине»; абзацный отступ – 1,25 см.
3. Оформление рисунков (при необходимости): выравнивание рисунка – «по центру», подпись рисунка – «Рис. №. Название рисунка»; шрифт для подписи рисунка – TimesNewRoman, размер – 12 пт.
4. Оформление таблиц (при необходимости): выравнивание таблицы – «по центру»; шрифт внутри таблицы – TimesNewRoman, размер – 11-12 пт.; выравнивание текста внутри таблицы – на усмотрение пользователя; подпись таблицы располагается над таблицей и состоит из двух частей: «Таблица №» – выравнивание по правому краю и «Название таблицы» – выравнивание по правому краю или по центру.

Для оформления источников (в соответствии с ГОСТ 2008):
1. Источники должны быть расположены в алфавитном порядке и пронумерованы.
2. В тексте доклада ссылка на источник выполняется в виде: [№], где № – номер источника в общем списке.
3. Если в тексте используется дословная цитата, то она должна быть взята в кавычки, а в ссылке на источник указана страница: [5, с.15].

Самостоятельная работа: Изучение литературы, подготовка доклада.