МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК»
(ФИЦ КНЦ РАН)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

По дисциплине Б1.В.07 Информационная безопасность организации
указывается цикл (раздел) ОП, к которому относится дисциплина, название дисциплины

для направления подготовки (специальности) 09.04.02 Информационные системы и технологии
код и наименование направления подготовки (специальности)

направленность программы (профиль) Информационные системы предприятий и учреждений
наименование профиля /специализаций/образовательной программы

Квалификация выпускника, уровень подготовки
магистр
(указывается квалификация (степень) выпускника в соответствии с ФГОС ВО)

Апатиты

2020

Лист согласования

1 Разработчик:

доцент УАиМ А.М. Федоров
должность подпись И.О. Фамилия

2 Методические указания рассмотрены и одобрены на заседании учебно-методической комиссии управления аспирантуры и магистратуры 29 июня 2020 г., протокол № 02.

Председатель УМК УАиМ

29.06.2020 Л.Д. Кириллова
дата подпись И.О.Фамилия

Пояснительная записка

1. Методические указания составлены в соответствии с требованиями федерального государственного образовательного стандарта по образовательной программе высшего образования – программе магистратуры по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Минобрнауки России № 917 от 19.09.2017.

2. **Цель дисциплины (модуля)** «Информационная безопасность организации» – сформировать у обучающихся комплексного представления о современного состояния сферы корпоративной информационной безопасности, в т.ч. в вопросах безопасности информационных систем и обрабатываемых в них персональных данных.

3. В результате освоения дисциплины «Информационная безопасность организации» обучающийся должен научиться анализировать и строить оценки и прогнозы в отношении процессов и объектов, входящих в состав системы информационной безопасности предприятия.

Задачи дисциплины:

- развить представление о современных проблемах информационной безопасности;
- научиться критически анализировать ситуации, связанные с защитой информации;
- получить представление способах организации и обеспечения информационной безопасности на предприятии.

4. **Требования к уровню подготовки обучающегося** в рамках данной дисциплины.

Процесс изучения дисциплины (модуля) «Информационная безопасность организации» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО 09.04.02 Информационные системы и технологии (уровень магистратуры), представленных в таблице 1.

Таблица 1 – Компетенции, формируемые в процессе изучения дисциплины «Информационная безопасность организации»

№ п/п	Код компетенции	Содержание компетенции
1.	ПК - 5	Способен анализировать и строить оценки и прогнозы в отношении процессов и объектов в профессиональной научной деятельности

5. Планируемые результаты обучения по дисциплине (модулю) «Информационная безопасность организации».

Результаты формирования компетенций и обучения представлены в таблице 2.

Таблица 2 – Планируемые результаты обучения

№ п/п	Код компетенции	Компоненты компетенции, степень их реализации	Результаты обучения

1.	ПК - 5	Компоненты компетенции соотносятся с содержанием дисциплины и компетенция реализуется полностью	***Знать:*** основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК-5.1). ***Уметь:*** с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК- 5.2). ***Владеть:*** навыками планирования, организации у управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК- 5.3).

Таблица 3 - Перечень практических работ

№ п/п	Наименование практических работ	Количество часов	Наименование темы по табл. 4 РП
1.	Обзор и анализ актуальной новостной повестки по теме информационная безопасность	4	3
2.	Типология и правила применения программно-технических средств обеспечения информационной безопасности	4	6
3.	Построение и использование средств извлечения и анализа открытых данных социальных сетей.	8	7
4.	Решение задач информационной безопасности при проектировании и разработке информационных систем и программных приложений	8	8
Итого часов		**24**	

Рекомендации к выполнению практических работ

Практическое занятие №1.
Тема: «Обзор и анализ актуальной новостной повестки по теме информационная безопасность».

При подготовке к практическому занятию студентам следует обратить на следующую информацию:

Один из актуальных вопросов реализации подсистемы защиты в современных информационных системах – это модель и алгоритмы обеспечения идентификации и аутентификации пользователей таких систем.

В новостной ленте по тематике «Безопасность информации» проблемы, связанные с идентификацией пользователей и обеспечением защиты на этом уровне, стоят на одном из первых мест.

Предлагается проанализировать и обобщить текущую новостную повестку (любой новостной источник) и выполнить практическое задание на тему «Аутентификация и идентификация пользователей»

Цель работы: реализовать в «командном процессоре» защиту на уровне пользователя с применением метода паролей или его модификаций; реализовать процедуру управления системой защиты на уровне пользователя

Ограничения.

1. Данная лабораторная работа выполняется на любом языке программирования (C/C++, Pascal, Assembler, Basic и т.д.) и в любой среде программирования (C++ Builder, Delphi, Visual C++, Visual Basic и т.д.). В работе также приветствуется (но совершенно не обязательно) использование современных средств моделирования ПО (Visual UML, Rational Rose, MS Visio и т.п.), а также современных методов получения, хранения и обработки и визуализации данных (ActiveX, ADO, и т.п.).
2. Разрабатываемый «командный процессор» является простым приложением ОС и должен «уметь» выполнять **не меньше** того, что написано в тексте лабораторной работы. Все реализуемые уровни защиты должны действовать ТОЛЬКО в рамках данного приложения, не распространяясь на работу других программ и самой ОС.

Структура командного процессора (блок «защита на уровне пользователя»)

Субъекты: Суперпользователь/администратор, другие пользователи
Объекты: база учетных записей пользователей

Минимальный набор команд

1. изменение своего пароля,
2. добавление нового пользователя,
3. удаление пользователя,
4. изменение учетной записи пользователя (изменение логина, дополнительных полей учетной записи (если они есть)),
5. просмотр информации о текущем пользователе,
6. просмотр разрешенной информации о существующих в системе пользователях,
7. несколько нейтральных команд (дата, время, список доступных команд системы и т.п.).

Минимальная функциональность

1. пароль не должен быть виден на экране,
2. в системе всегда присутствует хотя бы один суперпользователь,
3. обыкновенный пользователь ограничен в действиях,
4. создаёт новых пользователей (удаляет существующих) только суперпользователь,
5. суперпользователь может изменять пароли всех пользователей,
6. при изменении/добавлении пароля запрашивается его подтверждение,
7. имена пользователей в системе попарно различны (не повторяются),

8. возможность зайти под другим пользователем, не закрывая приложение,
9. работать в системе может только пользователь, успешно прошедший процедуру аутентификации.

Практическое занятие № 2.

Тема: «Типология и правила применения программно-технических средств обеспечения информационной безопасности».

При подготовке к практическому занятию студентам следует обратить на следующую информацию:

Существующие программно-технические средства по обеспечению информационной безопасности информационных систем предприятий представлены очень широко. Большая часть из них является проприетарным ПО, т.е. требующим покупки лицензии или платной подписки на использование программных продуктов.

В данной работе предлагается проанализировать наиболее востребованные на рынке защиты информации программные продукты (системы) и выполнить практическую работу «Криптографические алгоритмы» по самостоятельной разработке несложных базовых алгоритмов защиты.

Цель работы: освоение практических приемов криптографического преобразования информации.

Ограничения.

1. Данная работа является продолжение лаб. раб. №1 и выполняется в виде дополнения «командного процессора» новыми командами и возможностями.
2. Работа команд, созданных в рамках данной лабораторной работы, ни каким образом не должна мешать работе ОС.

Структура командного процессора - блок: «криптографическая защита».

Минимальный набор команд:

- Шифрование. В большинстве случаев необходимо указывать, что шифровать и ключ шифрования.
- Расшифрование. Необходимо указывать, что расшифровать и соответствующий ключ.

Детально логику работы данных команд необходимо выстроить в соответствии с выбранным вариантом.

Модель:

Алгоритмы работы каждого метода, используемого в вариантах данной лабораторной работы, подробно рассматриваются на лекционных занятиях.

Пример возможного алгоритма «Перестановка по матрице»:

0. Ограничения: S=2 – мин размер матрицы, I=7 – макс размер матрицы, E=’*’- символы для дополнения;
1. Исходный текст – P, длина текста N символов;
2. Если SQRT(N-1) <=S то переход к п.10;
3. Если SQRT(N-1) >= I, то K=I Иначе K=SQRT(N-1);
4. Используемый ключ: матрица перестановок R (K x K);
5. Выделить очередной блок исходного текста размером K*K;
6. Если блок полностью пустой, то переход к п.11;
7. Если блок не полный, то дополнить символами E;
8. Осуществить перестановку в блоке, согласно матрице R;
9. Переход к п.5;
10. Ошибка: размер сообщения слишком мал;

11. Конец.

Практическое занятие № 3.
Тема: «Построение и использование средств извлечения и анализа открытых данных социальных сетей.».

При подготовке к практическому занятию студентам следует обратить на следующую информацию.

Тема социальных сетей в настоящее время очень популярна.

Для работы с API социальной сети ВК необходимо подготовить соответствующие структуры данных, с помощью которых будет вестись авторизованный обмен информацией сервисами ВК.

Получение идентификационного токена и подобная работа с другими сторонними криптографическими подсистемами представлена в работе «Использование сторонних криптографических компонентов»

А. Цель работы: освоить практические приемы использования компонентов, не включенных в стандартную поставку сред разработки приложений.
Задача: создать приложение, выполняющее функции шифрования и дешифрования файла методом DES, реализованного в библиотеке DCPcrypt.

Ограничения.

1. Данная работа выполняется в среде программирования Delphi (или C++Builder).
2. Работа команд, созданных в рамках данной лабораторной работы, ни коим образом не должна мешать работе ОС.
3. Результатом выполнения данной лабораторной работы является работающее приложение и отчет по порядку выполнения работы (см. содержание_отчета)
4. Используемый пакет криптографических компонентов находится в dcpcrypt2.zip

Структура приложения.

1. Минимальный набор команд:

a. Шифрование файла методом DES.
b. Расшифрование файла методом DES.

Содержание отчета.

Отчет должен содержать **детальную** последовательность действий при выполнении лабораторной работы (вплоть до «Создаем папку с именем таким-то там-то и там-то»). Рекомендуется выделить два больших раздела «Установка пакета DCPcrypt» и «Создание приложения». Информацию по установке пакета можно найти в Readme.txt, находящегося в архиве *dcpcrypt2.zip*.
Если используется Borland Developer Studio, то рекомендуется устанавливать пакет в C++Builder.

При создании самого приложения, рекомендуется прочитать документацию к пакету.

Б. Работа с API социальной сети «Вконтакте»

1. Изучить материал по формированию идентификационного токена «ВК».
2. Получить токен «ВК»
3. Проверить работу токена, сделав простой запрос о получении данных со страницы открытых групп (пабликов) «ВК»

Практическое занятие № 4.
Тема: «Решение задач информационной безопасности при проектировании и разра-

ботке информационных систем и программных приложений».

При подготовке к практическому занятию студентам следует обратить на следующую информацию.

Обработка больших открытых данных в настоящее время представляет большой интерес для исследователей и инженеров. Примером таких данных являются открытые данные социальных сетей.

Для предприятий и организаций работа с данными социальных сетей является очень актуальной задачей. Такие данные являются и источником информации о новых потенциальных заказчиках и о появляющихся конкурентах. Также анализ данных социальных сетей позволяет отслеживать текущий информационный образ предприятия. Накапливаемые объемы подобной информации позволят от пассивного наблюдения перейти к активным действиям по формированию положительного информационного образа предприятия в онлайн среде.

Одним из средств решения описанной выше задачи является мониторинг. Особенностью мониторинга социальных сетей является обеспечение обработки персональных данных с учетом учет требований действующего законодательства и локальных правил самих социальных сетей. Все практические работы данного учебного курса ориентированы на работу исключительно с открытыми данными и не предполагают какую бы то ни было обработку прямых и косвенных персональных данных.

А. Цель: освоить практические приемы стеганографического преобразования информации.

Задача: создать приложение, выполняющее две функции: функцию упаковки исходного текста в контейнере стеганографическим методом и функцию извлечения текста из стеганографического контейнера.

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. В отличие от криптографии, где контрагент точно может определить, является ли передаваемое сообщение шифротекстом, методы стеганографии позволяют аккуратно встраивать передаваемые сообщения в открытые послания таким образом, чтобы было невозможным заподозрить существование самого встроенного послания.

Таким образом, если цель криптографии состоит в блокировании несанкционированного доступа к информации путём шифрования содержания секретных сообщений, то цель стеганографии – в скрытии самого факта существования секретного сообщения.

Классификация методов

Методы компьютерной стеганографии можно разделить в целом на два вида:

- методы, основанные на избыточности визуальной и аудиоинформации;
- методы, основанные на использовании специальных свойств компьютерных форматов.

Методы, основанные на избыточности визуальной и аудиоинформации, для скрытия информации используют младшие разряды цифровых отсчётов цифрового изображения и звука, которые содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и даёт возможность скрытия конфиденциальной информации.

Методы, основанные на использовании специальных свойств компьютерных форматов, делятся на:

- методы использования зарезервированных для расширения полей компьютерных форматов данных;
- методы специального форматирования текстовых файлов;
- методы скрытия в неиспользуемых местах гибких дисков;

• методы использования имитирующих функций;
• методы удаления идентифицирующего файл заголовка.

Методы специального форматирования текстовых файлов в свою очередь делятся на:

• методы использования известного смещения строк, слов, предложений, абзацев;
• методы выбора определённых позиций букв;
• методы использования специальных свойств, не отображаемых на экране полей форматов.

В. Цель: Разработка программно-алгоритмической системы мониторинга открытой группы (паблика) социальной сети «Вконтакте».

Задачи: 1) Использовать в качестве хранилища данных мониторинга NoSQL базу данных MongoDB; 2) Учесть ограничения, накладываемые социальной сетью на извлечение данных с помощью API или построить парсер для получения данных штатными средствами браузера по технологии http; 3) Средствами MongoDB или средствами собственных алгоритмов организовать агрегацию и визуализацию полученных данных с возможностью интерактивного управления.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная:

1. Галатенко, В.А. Основы информационной безопасности: Курс лекций / В.А. Галатенко ; под ред. В.Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=233063 (дата обращения: 02.12.2020). – ISBN 5-9556-0052-3. – Текст : электронный.
2. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 02.12.2020). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
3. Гультяева, Т.А. Основы защиты информации : учебное пособие : [16+] / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 15.12.2020). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

Дополнительная:

1. Философские проблемы информационного противоборства: учебное пособие для бакалавров, студентов, магистрантов и аспирантов / В.С. Поликарпов, В.Е. Шибанов, Е.В. Поликарпова, К.Е. Румянцев ; Южный федеральный

университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 211 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499981 (дата обращения: 02.12.2020). – Библиогр. в кн. – ISBN 978-5-9275-2716-8. – Текст : электронный.

2. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 02.12.2020). – Библиогр. в кн. – Текст : электронный.
3. Смолина, В.А. SMM С НУЛЯ: секреты продвижения в социальных сетях / В.А. Смолина. – Москва ; Вологда : Инфра-Инженерия, 2019. – 353 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=564678 (дата обращения: 15.12.2020). – ISBN 978-5-9729-0259-0. – Текст : электронный.
4. Шелудько, В.М. Основы программирования на языке высокого уровня Python : учебное пособие / В.М. Шелудько ; Министерство науки и высшего образования РФ, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 147 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500056 (дата обращения: 15.12.2020). – Библиогр. в кн. – ISBN 978-5-9275-2649-9. – Текст : электронный.
5. Защита персональных данных в информационных системах: лабораторный практикум / авт.-сост. В.И. Петренко, И.В. Мандрица ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 15.12.2020). – Текст : электронный.