МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ И ВОЗДЕЙСТВИЮ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

для студентов направления подготовки
02.04.01 Математика и компьютерные науки
направленность (профиль)
«Искусственный интеллект в кибербезопасности»

Ставрополь, 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины является формирование набора общепрофессиональных и профессиональных компетенций будущего магистра по направлению подготовки 02.04.01 Математика и компьютерные науки направленность (профиль) «Искусственный интеллект в кибербезопасности».

Задачи освоения дисциплины – ознакомление студентов с кругом задач в области искусственного интеллекта, а также знакомство с основными понятиями и методами машинного обучения и их применением к задачам, относящимся к профессиональной области.

Перечень осваиваемых компетенций:

Код	**Формулировка**
ПК-8	Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. Понятие и классификация компьютерных вирусов

Цель: изучить концептуальные основы проектирования в профессиональной сфере.

Теоретическая часть

Рассмотреть и определить роль проектного менеджмента в инновационном развитии различных систем и организаций. Рассмотреть подходы к определению понятия «проект», особенности и классификацию проектов в профессиональной сфере. Рассмотреть сущность проектирования в профессиональной сфере, его основные функции и факторы успеха. Рассмотреть суть понятия «управление проектом», проекционную схему управления проектом, а также отличия проектного управления от традиционного. Изучить состав окружающей среды и функциональные роли участников проекта. Изучить методы коллективной работы над проектом.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Раскройте роль проектного менеджмента в инновационном развитии различных систем и организаций.
2. Что собой представляет проект?
3. Раскройте особенности проектов в различной профессиональной сфере.
4. Какие выделяют виды проектов в различной профессиональной сфере?
5. Что собой представляет проектирование в различной профессиональной сфере?
6. Какие функции выполняет и на решение каких задач может быть направлено проектирование в различной профессиональной сфере?
7. В чем заключается суть управления проектом?
8. Что собой представляет проекционная схема управления проектом?
9. Укажите отличительные особенности проектного управления от традиционного.
10. Кто входит в состав участников проекта и каковы их функциональные роли?
11. Охарактеризуйте методы коллективной работы над проектом.

Практические задания

Задание 1. Напишите доклад на одну из тем:
«Сущность проектирования в сфере образования, его основные функции и факторы успеха»;
«Управление проектом»;
«Состав окружающей среды и функциональные роли участников проекта»;
«Методы коллективной работы над проектом».
Задание 2. Раскройте подходы к определению понятия «проект».
Задание 3. Отразите в виде схемы окружение и участников проекта
Задание 4. В виде таблицы осуществите сравнение традиционного управления и управления проектом.
Задание 5. Отразите в таблице существующие подходы к определению понятия «проектирование» в профессиональной сфере.
Задание 6. В таблице раскройте классификацию проектов в различной профессиональной сфере.

Задание 7. Составьте таблицу, отражающую классификацию вирусов по среде распространения:

Тип вируса	**Среда распространения**	**Особенности**
Файловые вирусы	Файлы исполняемых форматов	Заражают EXE, COM-файлы
Загрузочные вирусы	Сектор загрузки	Поражают загрузочный сектор
Сетевые вирусы	Компьютерные сети	Используют сетевые протоколы
Макровирусы	Документы и скрипты	Встраиваются в макрокоманды

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 2. Правовой статус лиц, занимающихся разработкой, публикацией и распространением компьютерных вирусов

Цель: изучить правовой статус лиц, участвующих в создании, распространении и публикации компьютерных вирусов, а также определить основные меры ответственности за данные деяния.

Теоретическая часть

Рассмотреть правовые нормы, регулирующие ответственность за разработку, распространение и использование компьютерных вирусов. Изучить национальное законодательство и международные правовые акты в области информационной безопасности. Определить состав преступлений, связанных с созданием и распространением вредоносного программного обеспечения. Рассмотреть понятие киберпреступлений и классификацию деяний, связанных с компьютерными вирусами. Изучить формы ответственности: уголовную, административную и гражданско-правовую. Рассмотреть особенности привлечения к ответственности несовершеннолетних лиц. Изучить практику судебных разбирательств по делам, связанным с созданием и распространением компьютерных вирусов.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Какие действия в отношении компьютерных вирусов запрещены законодательством?
2. Какой состав преступления включает разработку и распространение вредоносного программного обеспечения?

3. Какие правовые нормы регулируют ответственность за киберпреступления?
4. В чем заключается отличие административной ответственности от уголовной по таким делам?
5. Какие международные правовые акты касаются борьбы с распространением компьютерных вирусов?
6. Какова роль Конвенции о киберпреступности в регулировании вопросов информационной безопасности?
7. Какие особенности привлечения к ответственности несовершеннолетних лиц при совершении киберпреступлений?
8. Какие примеры судебной практики по делам о распространении вирусов можно привести?
9. В каких случаях возможно привлечение к гражданско-правовой ответственности за вред, причинённый вирусами?
10. Какие наказания предусмотрены законодательством за публикацию вредоносных программ?
11. Каким образом законодательство учитывает мотивацию и цели разработчиков вирусов?

Практические задания

Задание 1. Напишите доклад на одну из тем:
«Уголовная ответственность за разработку и распространение компьютерных вирусов»;
«Международное регулирование борьбы с киберпреступностью»;
«Особенности привлечения несовершеннолетних к ответственности за киберпреступления»;
«Гражданско-правовая ответственность за вред, причинённый вредоносными программами».

Задание 2. Подготовьте краткий обзор статей Уголовного кодекса Российской Федерации (или законодательства вашей страны), регулирующих ответственность за создание и распространение вирусов.

Задание 3. Постройте схему состава преступления, связанного с созданием и распространением вредоносных программ.

Задание 4. В виде таблицы сравните уголовную, административную и гражданско-правовую ответственность за киберпреступления.

Задание 5. В таблице приведите международные документы, регулирующие вопросы борьбы с киберпреступностью, и кратко охарактеризуйте их.

Задание 6. Подготовьте сравнительный анализ реальных дел о привлечении к ответственности за создание вирусов.

Задание 7. Подготовьте таблицу:

Правонарушение	**Статья УК РФ**	**Возможная мера наказания**
Несанкционированный доступ к информации	Статья 272	Штраф, исправительные работы
Создание, использование вирусов	Статья 273	Лишение свободы до 5 лет

Перечень основной литературы

3. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
4. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

7. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
8. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
9. https://spravochnick.ru/psihologiya/ – Справочник по психологии
10. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
11. http://www.myersbriggs.org
12. http://keirsey.com

Практическое занятие 3. COM-вирусы: особенности и методы борьбы

Цель: изучить особенности COM-вирусов, их механизм заражения, распространения и методы борьбы с ними.

Теоретическая часть

Рассмотреть определение COM-вирусов и их место среди других типов файловых вирусов. Изучить особенности заражения файлов с расширением .COM. Рассмотреть методы внедрения кода вируса в структуру исполняемых файлов и последствия заражения. Изучить механизмы распространения COM-вирусов в операционных системах DOS и Windows. Изучить примеры известных COM-вирусов, их принципы действия и влияние на работоспособность систем. Рассмотреть современные методы выявления и удаления COM-вирусов, а также особенности профилактики заражения.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что такое COM-вирусы и в чем их особенности?
2. Как происходит заражение файлов с расширением .COM?
3. Какие методы используют COM-вирусы для внедрения в исполняемые файлы?
4. Какие последствия может вызвать заражение COM-вирусом?
5. В каких операционных системах COM-вирусы были наиболее распространены?
6. Как COM-вирусы отличаются от EXE-вирусов?
7. Какие известные COM-вирусы существовали в истории развития компьютерных угроз?
8. Каковы особенности обнаружения COM-вирусов современными антивирусными средствами?
9. Какие методы удаления COM-вирусов наиболее эффективны?
10. Какие профилактические меры позволяют снизить риск заражения COM-вирусами?
11. Как эволюция операционных систем повлияла на актуальность угрозы COM-вирусов?

Практические задания

Задание 1. Напишите доклад на одну из тем: «История появления и распространения COM-вирусов»; «Методы заражения и распространения вирусов в файлах .COM»; «Известные примеры COM-вирусов и их характеристики»; «Современные методы борьбы с файловыми вирусами».

Задание 2. Сформулируйте определение понятия «COM-вирус» и опишите его особенности.

Задание 3. Постройте схему процесса заражения файла .COM COM-вирусом.

Задание 4. В таблице сравните COM-вирусы и EXE-вирусы по следующим критериям: способ заражения, распространение, последствия заражения, методы защиты.

Задание 5. Составьте перечень антивирусных мер, эффективных против COM-вирусов.

Задание 6. Подготовьте краткий обзор примеров COM-вирусов с описанием их способов заражения и последствий.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 4. EXE-вирусы: особенности заражения и защиты

Цель: изучить особенности EXE-вирусов, их механизмы заражения исполняемых файлов и способы защиты от них.

Теоретическая часть

Рассмотреть определение EXE-вирусов и их отличие от других видов файловых вирусов. Изучить способы заражения файлов с расширением .EXE. Рассмотреть различные механизмы внедрения вирусного кода в структуру исполняемых файлов. Изучить влияние заражения EXE-файлов на работу программного обеспечения и операционной системы. Рассмотреть примеры известных EXE-вирусов и их принцип действия. Изучить методы обнаружения EXE-вирусов, особенности антивирусной защиты и восстановления заражённых файлов. Рассмотреть эволюцию EXE-вирусов с развитием операционных систем.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что такое EXE-вирусы и в чем их отличия от других файловых вирусов?
2. Какие способы заражения применяются EXE-вирусами?
3. Какие существуют методы внедрения вирусного кода в EXE-файлы?
4. Какие последствия может вызвать заражение EXE-файлов?
5. В каких операционных системах EXE-вирусы были особенно распространены?
6. Чем EXE-вирусы отличаются от COM-вирусов?
7. Какие известные EXE-вирусы существуют в истории развития вредоносного ПО?
8. Как антивирусные программы обнаруживают EXE-вирусы?
9. Какие методы используются для удаления вирусов из заражённых EXE-файлов?
10. Какие профилактические меры позволяют избежать заражения EXE-вирусами?
11. Как развитие антивирусных технологий повлияло на распространение EXE-вирусов?

Практические задания

Задание 1. Напишите доклад на одну из тем: «Особенности заражения исполняемых файлов EXE-вирусами»; «История появления и эволюция EXE-вирусов»; «Обзор наиболее известных EXE-вирусов и их характеристика»; «Современные методы защиты от EXE-вирусов».

Задание 2. Сформулируйте определение понятия «EXE-вирус» и выделите его основные признаки.

Задание 3. Постройте схему процесса заражения EXE-файла вирусом.

Задание 4. В виде таблицы сравните EXE-вирусы и COM-вирусы по следующим критериям: структура заражаемого файла, способ внедрения, распространение, методы обнаружения и удаления.

Задание 5. Составьте перечень профилактических мер по защите от заражения EXE-вирусами.

Задание 6. Подготовьте краткий обзор примеров EXE-вирусов с описанием их способов действия и воздействия на системы.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 5. Команды обмена данными: роль в функционировании вирусов

Цель: изучить команды обмена данными, их роль в работе компьютерных вирусов и способы защиты информации от их использования.

Теоретическая часть

Рассмотреть понятие команд обмена данными и их применение в работе программного обеспечения. Изучить, как команды обмена данными используются вирусами для распространения, заражения и взаимодействия с заражённой системой. Рассмотреть примеры команд передачи данных в различных архитектурах (например, x86). Изучить роль команд копирования, перемещения, чтения и записи данных в жизненном цикле компьютерного вируса. Рассмотреть методы, с помощью которых вирусы получают доступ к системным ресурсам через команды обмена данными. Изучить способы обнаружения подозрительных операций обмена данными и меры по их блокированию.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что собой представляют команды обмена данными в архитектуре процессора?
2. Как команды обмена данными используются при разработке компьютерных вирусов?
3. Какие команды обмена данными наиболее часто применяются вирусами?
4. Как команды чтения и записи используются для распространения вирусов?
5. В чем состоит опасность неконтролируемого обмена данными в системе?
6. Какие примеры команд обмена данными существуют в архитектуре x86?
7. Как современные антивирусные программы выявляют подозрительный обмен данными?
8. Какие существуют методы защиты информации от использования вирусами команд обмена данными?
9. В чем отличие легитимного и вредоносного использования команд обмена данными?
10. Как вирусы могут перехватывать или модифицировать команды обмена данными?
11. Как минимизировать риски заражения через операции обмена данными?

Практические задания

Задание 1. Напишите доклад на одну из тем:
«Применение команд обмена данными в функционировании компьютерных вирусов»;
«Методы защиты информации от перехвата через команды обмена данными»;

«Анализ команд обмена данными в архитектуре x86»; «Выявление вредоносной активности через мониторинг операций обмена данными».

Задание 2. Опишите процесс заражения компьютера вирусом с использованием команд обмена данными.

Задание 3. Постройте схему жизненного цикла вируса, в которой отражены стадии применения команд обмена данными.

Задание 4. В таблице перечислите основные команды обмена данными и кратко опишите их функции.

Задание 5. Подготовьте сравнительный анализ легитимного и вредоносного использования команд обмена данными.

Задание 6. Составьте список мер защиты от несанкционированного обмена данными в информационных системах.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 6. Макровирусы: особенности заражения и методы защиты

Цель: изучить природу макровирусов, их механизмы заражения документов и способы защиты от них.

Теоретическая часть

Рассмотреть определение макровирусов и их отличие от других типов вирусов. Изучить механизмы заражения документов макровирусами на примере офисных приложений (Microsoft Word, Excel и других). Рассмотреть, как макровирусы используют встроенные языки макропрограммирования для выполнения вредоносных действий. Изучить примеры известных макровирусов, их принципы работы и способы распространения. Рассмотреть методы обнаружения макровирусов, особенности антивирусной защиты и рекомендации по безопасной работе с документами, содержащими макросы. Изучить роль настроек безопасности макросов в предотвращении заражений.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что такое макровирусы и в чем их особенности?
2. Какие офисные приложения наиболее уязвимы перед макровирусами?
3. Как макровирусы используют встроенные средства автоматизации приложений?
4. Какие последствия может вызвать заражение макровирусом?
5. Какие существуют пути распространения макровирусов?
6. Какие известные макровирусы повлияли на развитие антивирусных технологий?
7. Как современные антивирусные программы обнаруживают макровирусы?
8. Какие меры позволяют защититься от заражения макровирусами?
9. Как управление настройками безопасности макросов влияет на защиту системы?
10. Чем макровирусы отличаются от файловых вирусов?
11. Каковы современные тенденции использования макровирусов в киберугрозах?

Практические задания

Задание 1. Напишите доклад на одну из тем: «История появления и развития макровирусов»;

«Механизмы заражения документов макровирусами»; «Известные случаи массового распространения макровирусов»; «Настройки безопасности макросов как способ защиты от макровирусов».

Задание 2. Определите, что такое макрос и как его можно использовать в целях заражения.

Задание 3. Составьте схему заражения офисного документа макровирусом.

Задание 4. В таблице сравните макровирусы и файловые вирусы по следующим критериям: объект заражения, механизм внедрения, способы распространения, методы защиты.

Задание 5. Подготовьте перечень мер по настройке офисных приложений для защиты от макровирусов.

Задание 6. Выполните обзор современных антивирусных решений, предлагающих защиту от макровирусов.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 7. Маскировка вирусов: методы сокрытия и обнаружения

Цель: изучить методы маскировки компьютерных вирусов и способы их обнаружения.

Теоретическая часть
Рассмотреть понятие маскировки вирусов и её роль в успешном распространении вредоносного программного обеспечения. Изучить основные методы маскировки: полиморфизм, метаморфизм, стелс-технологии, использование упаковщиков и шифраторов. Рассмотреть, как вирусы изменяют собственный код или структуру для затруднения обнаружения антивирусными средствами. Изучить принципы работы полиморфных и метаморфных вирусов. Рассмотреть примеры известных вирусов, использующих методы маскировки. Изучить современные методы выявления замаскированных вирусов, включая анализ поведения и эмуляцию выполнения кода.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Что такое маскировка вирусов и для чего она используется?
2. В чем заключается суть полиморфизма в вирусах?
3. Как работает метаморфизм в контексте маскировки вирусов?
4. Что собой представляют стелс-вирусы?
5. Какие техники используют вирусы для сокрытия своей активности в операционной системе?
6. Как упаковщики и шифраторы помогают вирусам избегать обнаружения?
7. Приведите примеры вирусов, активно использующих методы маскировки.
8. Какие методы применяют антивирусные программы для выявления замаскированных вирусов?
9. Что такое эмуляция выполнения кода и как она помогает в обнаружении вирусов?
10. Чем полиморфные вирусы отличаются от метаморфных?
11. Какие современные вызовы существуют в борьбе с маскирующимися вирусами?

Практические задания

Задание 1. Напишите доклад на одну из тем: «Методы полиморфизма и их использование в вирусах»; «Метаморфизм как способ маскировки вредоносного кода»; «Стелс-технологии в вирусах: принципы работы и примеры»; «Эволюция методов маскировки вирусов и антивирусных технологий».

Задание 2. Определите основные признаки замаскированного вируса.

Задание 3. Составьте схему, иллюстрирующую процесс изменения кода полиморфного вируса.

Задание 4. В таблице сравните полиморфные, метаморфные и стелс-вирусы по следующим критериям: механизм изменения, цели, методы обнаружения.

Задание 5. Подготовьте список современных инструментов для анализа замаскированного вредоносного кода.

Задание 6. Выполните краткий обзор методов динамического анализа программ для выявления замаскированных вирусов.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 8. Методы борьбы с компьютерными вирусами

Цель: изучить основные методы борьбы с компьютерными вирусами, способы профилактики заражения и восстановления заражённых систем.

Теоретическая часть
Рассмотреть основные направления борьбы с компьютерными вирусами: профилактика, обнаружение, лечение и удаление заражений. Изучить роль антивирусных программ в защите информационных систем. Рассмотреть методы профилактики вирусных атак: настройка политики безопасности, регулярное обновление программного обеспечения, ограничение прав пользователей. Изучить методы обнаружения вирусов: сигнатурный анализ, эвристический анализ, анализ поведения. Рассмотреть процесс лечения и удаления вирусов из заражённых файлов и систем. Изучить принципы работы антивирусных сканеров, мониторинговых программ и сетевых экранов. Рассмотреть меры по восстановлению данных после вирусной атаки и особенности построения системы резервного копирования.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Какие основные этапы включает борьба с компьютерными вирусами?
2. Какую роль играют антивирусные программы в защите информации?
3. Какие существуют методы профилактики заражения компьютерными вирусами?
4. Что такое сигнатурный анализ и как он используется для обнаружения вирусов?
5. В чем заключается эвристический анализ вирусов?
6. Как осуществляется анализ поведения программ с целью выявления вирусов?
7. Как происходит лечение заражённых файлов?
8. В чем особенности удаления вирусов из системных областей?
9. Какие программы используются для постоянного мониторинга системы на наличие вирусов?
10. Как построение системы резервного копирования помогает в борьбе с вирусами?
11. Какие меры следует предпринять после вирусной атаки для восстановления работы системы?

Практические задания

Задание 1. Напишите доклад на одну из тем: «Сигнатурный и эвристический анализ в антивирусных системах»; «Меры профилактики компьютерных вирусов»; «Процесс восстановления данных после вирусной атаки»; «Роль резервного копирования в защите от вирусов».

Задание 2. Определите основные различия между сигнатурным и эвристическим методами обнаружения вирусов.

Задание 3. Составьте схему, иллюстрирующую процесс обнаружения и удаления вируса антивирусной программой.

Задание 4. В таблице сравните различные методы обнаружения вирусов по следующим критериям: скорость, точность, вероятность ложных срабатываний.

Задание 5. Подготовьте инструкцию по настройке системы резервного копирования для защиты от последствий вирусных атак.

Задание 6. Выполните обзор популярных антивирусных программ, выделив их ключевые особенности.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 9. Обзор антивирусных программ

Цель: изучить возможности современных антивирусных программ, их особенности, классификацию и критерии выбора.

Теоретическая часть

Рассмотреть назначение антивирусных программ и их роль в защите компьютерных систем. Изучить классификацию антивирусного программного обеспечения: сканеры, мониторы, ревизоры, фильтры. Рассмотреть принципы работы антивирусных сканеров, особенности антивирусных мониторов в реальном времени. Изучить различия между бесплатными и коммерческими антивирусами. Рассмотреть основные функции современных антивирусных решений: защита в реальном времени, сканирование по расписанию, эвристический анализ, обновление баз данных, защита электронной почты и интернета. Изучить критерии выбора антивирусной программы: эффективность обнаружения угроз, производительность, удобство использования, стоимость. Провести обзор популярных антивирусных программ, их плюсы и минусы.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Какова основная задача антивирусных программ?
2. Какие существуют виды антивирусных программ и в чем их особенности?
3. В чем разница между антивирусным сканером и монитором?
4. Какие функции выполняют современные антивирусные программы?
5. В чем особенности работы антивирусных фильтров и ревизоров?
6. Какие преимущества и недостатки имеют бесплатные антивирусные решения?
7. Какие параметры следует учитывать при выборе антивирусной программы?
8. Почему регулярное обновление антивирусных баз так важно?
9. Как осуществляется защита электронной почты антивирусными программами?
10. Чем антивирусные программы отличаются от комплексных систем обеспечения безопасности?
11. Назовите примеры известных антивирусных программ и их особенности.

Практические задания

Задание 1. Напишите доклад на одну из тем: «Сравнение бесплатных и коммерческих антивирусных программ»; «Роль антивирусных мониторов в обеспечении защиты системы»; «Эвристический анализ в современных антивирусных решениях»; «Критерии выбора антивирусной программы для домашнего и корпоративного использования».

Задание 2. Определите основные различия между антивирусными сканерами, мониторами и ревизорами.

Задание 3. Составьте схему классификации антивирусных программ.

Задание 4. В таблице сравните несколько популярных антивирусных программ по следующим критериям: функциональные возможности, производительность, стоимость, удобство использования.

Задание 5. Подготовьте перечень обязательных функций, которые должна поддерживать современная антивирусная программа.

Задание 6. Выполните обзор трёх наиболее популярных антивирусных решений, выделив их ключевые особенности, преимущества и недостатки.

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя

3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com