Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5:004.732

Климов
Дмитрий Александрович

Безопасность операционных систем в корпоративных информационных сетях

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

Научный руководитель
Ширинский Валерий Павлович
канд. техн. наук, доцент

Минск 2020

ВВЕДЕНИЕ

Задачи построения информационного общества в Республике Беларусь выдвигают вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности государства. Роль информационной безопасности становится всё значительнее в силу следующих причин:

– проникновение технических средств обработки и передачи данных практически во все сферы человеческой деятельности;

– национальные интересы, угрозы им и обеспечение защиты от этих угроз во всех областях национальной безопасности выражаются, реализуются и осуществляются через информацию и информационную сферу;

– человек, его права, информация и информационные системы и права на них – это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях;

– проблемы национальной безопасности имеют ярко выраженный информационный характер.

Работа по информационной безопасности посвящена проведению риск-анализа защищаемой системы или объекта информатизации, которые могут быть подвержены деструктивным воздействиям того или иного вида атак. Другими словами, цель магистерской диссертации по безопасности заключается в оценке рисков и живучести защищаемой системы, компоненты которой подвержены воздействию информационных атак.

Для этого необходимо привести основные понятия и определения в области защиты операционных систем от информационных атак, провести обзор и анализ основных уязвимостей, на основе которых могут быть реализованы атаки в корпоративных сетях, изучить подсистему защиты операционных систем от информационных атак чтобы в итоге получить достоверную картину проведения мероприятий по защите информационной безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование и выбор средств для обеспечения безопасности операционных систем в корпоративных информационных сетях.

Для достижения данной цели следует решить следующие задачи:

1 Привести основные понятия и определения в области защиты операционных систем от информационных атак.

2 Провести обзор и анализ основных эксплуатационных и технологических уязвимостей, на основе которых могут быть реализованы атаки в корпоративных сетях.

3 Подготовить и изучить данные о современных способах и методах защиты операционных систем.

4 Изучить подсистему защиты операционных систем от информационных атак.

5 Провести аудит подсистемы защиты операционной системы от информационных атак.

Объект исследования:

Операционные и автоматизированные системы.

Предмет исследования:

Безопасность операционных систем в корпоративных информационных сетях.

Положения, выносимые на защиту

1 Определение угроз и уязвимостей, которым могут быть подвергнуты активы, способы и методы обеспечения безопасности операционных систем в корпоративных сетях.

2 Оценка влияния, которое может иметь место в результате нарушений безопасности, реальная возможность реализации угроз безопасности и представление возможного ущерба, и реализованные в настоящее время меры обеспечения безопасности.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует подразделам 5.2 «Системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и систем, их информационная безопасность» и 5.5 «методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь 19.04.2010 г. № 585.

В данной работе рассмотрены и доработаны аспекты безопасности операционных систем в корпоративных информационных сетях.

Апробация диссертации и информация об использовании её результатов

Основные положения и результаты исследований докладывались и обсуждались на 56 СНТК БГУИР (Минск, 18.05.2020 – 20.05.2020),

а также на XVIII научно-технической конференции «Технические средства защиты информации» (Минск, 09.06.2020г.)

По результатам исследований, представленных в диссертации, опубликовано 2 работы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, дается краткая характеристика ее разработанности, также определяются цели и задачи, указывается теоретическая основа, отмечаются элементы научной новизны, формулируются основные положения диссертации, выносимые на защиту.

Первая глава носит теоретический характер, состоит из 5 разделов. Она посвящена основным понятиям и определениям в области защиты операционных систем от информационных атак.

Вторая глава носит теоретический характер, состоит из 3 разделов. В ней произведен обзор и анализ основных эксплуатационных и технологических уязвимостей, на основе которых могут быть реализованы атаки в корпоративных сетях. Анализируются угрозы информационной безопасности и типы уязвимостей информационных и операционных систем.

Третья глава носит теоретический характер, состоит из 2 разделов. В ней производится подготовка и изучение данных о современных способах защиты

операционных систем, рассмотрена безопасность на уровне операционной системы.

Четвертая глава носит теоретический характер, состоит из 2 разделов. В ней рассмотрены подсистемы защиты операционных систем, приводятся примеры операционных систем и используемых в них методов и средств защиты.

Пятая глава носит практико-ориентированный характер, состоит из 4 разделов. В ней подробно рассматривается понятие аудита, проводится пример рассмотрения уязвимости операционных систем с помощью соответствующих инструментов и утилит. Делаются выводы на основе полученной информации.

В приложении предоставлены команды Unix-подобной системы, используемые для проверки безопасности.

ЗАКЛЮЧЕНИЕ

В работе получены следующие основные результаты.

Определено, что информационная безопасность операционных систем на данный момент является неотъемлемой частью в работе корпоративной сети любого предприятия. Учитывая многообразие угроз, следует уделять информационной безопасности особое внимание.

Осуществлена классификация угроз информационной безопасности корпоративной сети и её компонентов, рассмотрены различные типы уязвимостей и возможных недостатков защиты операционных систем и сетей.

Подготовлены и изучены данные о современных способах и методах защиты операционных систем, их классификация и технические средства, необходимые для обеспечения сетевой и серверной инфраструктуры, систем электропитания, защиты физической и информационной среды.

Рассмотрена подсистема защиты операционных систем от информационных атак, проведен пример сканирования на наличие уязвимостей и проведен аудит подсистемы защиты ОС. В качестве инструментов, используемых для проведения проверки информационной безопасности, были взяты операционная система Kali Linux и свободная утилита nmap.

Была получена достоверная картина проведения мероприятий по защите информационной безопасности.