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

УДК 004.056

Алланазаров Дидар

Система мониторинга и противодействие компьютерным вирусам

АВТОРЕФЕРАТ
магистерской диссертации на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Рыбак В.А.
кандидат технических наук, доцент

Минск 2019

ВВЕДЕНИЕ

Защита компьютерных систем от вредоносных программ в настоящее время является одной из наиболее актуальных задач в области защиты информации. Ежегодные потери от компьютерных вирусов оцениваются в десятки и сотни миллиардов долларов. В этом документе анализируются существующие решения для обнаружения вредоносных программ.

В настоящее время мониторинг компьютеров и контроль за их использованием становится все более популярным. На рынке существуют программы с расширенным мониторингом активности пользовательских рабочих станций, позволяющие системным администраторам на предприятиях контролировать сетевую активность сотрудников в режиме реального времени, а также проверять конфигурацию установленных устройств и программного обеспечения на компьютерах, подключенных к локальной сети, без необходимости управлять удаленными компьютерами.

Под мониторингом компьютерных сетей обычно понимают работу системы, проводя постоянный мониторинг их работы с целью выявления медленно работающих или неработающих систем или лечения вирусов. Задача мониторинга включает в случае обнаружения неисправностей администратора сети уведомление о них заранее определенным способом - с использованием сообщения электронной почты, мессенджера, пейджера и т. д. Выполнение этой задачи является одним из основных аспектов управления компьютерной сетью.

Если система обнаружения вторжений должна отслеживать появление внешних угроз, то мониторинг компьютерных сетей необходим для их мониторинга при поиске сбоев, которые были вызваны перегрузкой и / или отказом серверов, других устройств и сетевых подключений. Например, чтобы определить текущее состояние веб-сервера, программа мониторинга может отправлять HTTP-запрос на получение тестовой страницы через равные промежутки времени; почтовые серверы проверяются путем отправки тестового сообщения по SMPT и получения POP3 или IMAP.

В настоящее время существуют различные противодействия и программы для мониторинга компьютерных вирусов, а именно:

- антивирусные подходы;
- передовые антивирусные методы.

Исходя из вышеизложенного, целью данной работы является разработка методологии мониторинга любой сети и разработка мер противодействия вирусным угрозам в сети или системе. Кроме того, конечной целью автора является изучение эффективности существующих программ или продуктов

мониторинга с использованием разработанной методики тестирования. Для мониторинга системы было выбрано следующее программное обеспечение: СёрчИнформ.

Автор изучил и систематизировал определенный объем информации по теме диссертационной работы. Разработана и обоснована методика тестирования программного продукта.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетным направлениям научных исследований Беларуси на 2016-2020 годы, утвержденным Постановлением Совета министров Беларуси от 12 марта 2015 года, № 190. Работа выполнена в образовании «Белорусский государственный университет информатики и радиоэлектроники».

Цель исследования работы

Цель состоит в том, чтобы рассмотреть модели угроз безопасности системы и способы их реализации, проанализировать критерии уязвимости и устойчивости системы к разрушительным воздействиям, описать инструменты мониторинга для выявления использования несанкционированных информационных воздействий, рассмотреть характер разработки методологий и методологий для оценка ущерба от угроз информационной безопасности.

Для достижения этой цели необходимо решить следующие задачи:

- опишите основные модели угроз безопасности системы и способы их реализации;
- систематически анализировать критерии уязвимости систем к разрушительным воздействиям;
- опишите некоторые инструменты мониторинга для обнаружения использования несанкционированных информационных эффектов;
- принесите читателю информацию о методологии оценки ущерба от воздействия угроз информационной безопасности.

Личный вклад заявителя

Результаты исследований получены автором самостоятельно. Научный руководитель принимал участие в определении целей и задач исследования, интерпретации промежуточных результатов.

Положения, выносимые на защиту

Методы контроля сохранности личной информации используют программы, позволяющие определить эффективность применения и обнаруженных вредоносных файлов, количество удаленных и вылеченных файлов. признание средств и методов работы вируса

Применение различных методов противодействия вирусным угрозам информационной безопасности в ИТ-секторе.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 76 страницы, 17 наименования в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится аналитический обзор существующих методов и средств обнаружение и противодействия вирусным угрозам. Описана научные подходы обнаружения вирусных угроз, статические и динамические методы обнаружения. Также описана аппаратные и программные средства защиты информации. Рассматриваются антивирусные подходы, передовые антивирусные технологии.

Вторая глава посвящена проектированию и реализации системы мониторинга вирусных угроз. Подробно рассмотрена, модель реализации и цели угроз информационной безопасности. Подробно рассмотрены архитектура усовершенствованной системы мониторинга и анализа вирусов в реальной среде.

В третьей главе описывается апробация системы и разработка мероприятий по противодействию вирусным атакам. Выявлены результаты испытании системы. Описывается разработка мероприятий. Показана возможность использования программы СёрчИнформ SIEM для организации системы мониторинга безопасности. С использованием программы в этой работе были разработаны алгоритм и модуль мониторинга безопасности программного обеспечения с использованием существующих методов.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Компьютерные вирусы в настоящее время являются одной из наиболее серьезных угроз информационной безопасности, о чем свидетельствуют многочисленные данные о ежегодных финансовых потерях компаний в результате последствий вирусных атак. В то же время традиционные меры по борьбе с вредоносным ПО, основанные на простой установке средств антивирусной защиты на рабочих станциях и серверах, недостаточно эффективны. Поэтому использование комплексного подхода к противодействию вирусным атакам, рассмотренного в этой статье, позволит повысить эффективность тех мер, которые компании используют в настоящее время.

Развитие информационных систем сопровождается появлением новых и новых угроз. Поэтому разработка аппаратно-программных систем мониторинга безопасности КС не только не сильно отстает, но иногда даже защищает информационные системы.

С каждым днем использование систем мониторинга безопасности становится все более распространенным, и поэтому актуальность описанных задач защиты систем от атак, контроля распространения вирусов и несанкционированной сетевой активности пользователей и снижения неэффективного использования ресурсов растет. Основными результатами работы являются:

- Рассмотрены методы защиты ИС, сбора и анализа трафика для выявления вредоносных и нежелательных объектов и разработки интегрированной системы мониторинга безопасности ИС.
- Рассмотрены методы мониторинга безопасности, направленные на решение проблем непрерывного мониторинга компьютерных сетей при выявлении внутренних и внешних воздействий на ресурсы компьютерных сетей.
- Анализ существующих аппаратных и программных средств мониторинга безопасности с целью определения основных компонентов позволил выявить уязвимости до их использования.