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

УДК 004.056:629.4

Вагуро Павел Александрович

Разработка методики антивирусной защиты компьютерных сетей на железнодорожном транспорте

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 98 80 01 "Методы и системы защиты информации, информационная безопасность"

_____

Научный руководитель
Лыньков Леонид Михайлович
д.т.н., профессор

_____

Минск 2015

Введение

В течение нескольких лет на Белорусской железной дороге реализуются крупные проекты, ориентированные на переход к современным программно-техническим решениям и поэтапной реализации концепции корпоративной информационной системы дороги.

Большая протяженность сетей, сложность применяемых устройств и АСУ, а также требования к обеспечению безопасности и надежности перевозок в совокупности с участившимися инцидентами эксплуатации угроз информационной безопасности, - диктуют необходимость создания мощной системы защиты информации.

С развитием компьютерных сетей, и в частности сети интернет, широкое распространение получают сетевые атаки, в том числе и с помощью вредоносного программного обеспечение – вирусов. Именно приложения, содержащие вредоносный исполняемый код, являются на сегодняшний день наиболее популярным в среде злоумышленников средством нанесения ущерба не только частным пользователям, но и информационным системам и сетям предприятий.

Формирование единого информационного пространства требует решения проблем безопасности. Данная работа призвана последовательно описать методику антивирусной защиты сетей предприятий Белорусской железной дороги с учетом физических особенностей сетей, перспектив их развития и применяемых в отрасли технологий.

Общая характеристика работы

Тема диссертационной работы соответствует подразделу 5.5 "Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передачи данных с использованием криптографии, квантово-криптографические системы" приоритетных направлений фундаментальных и прикладных исследований Республики Беларусь на 2011-2015 гг., утвержденных Постановлением Совета Министров Республики Беларусь №585 от 19 апреля 2010 г.

Работа выполнялась в учреждении образования "Белорусский государственный университет информатики и радиоэлектроники".

Цели и задачи исследования

Цель диссертационной работы заключалась в создании базисной методики построения системы обеспечения антивирусной защиты компьютерных сетей предприятий железнодорожного транспорта.

Для достижения поставленной цели необходимо было решить следующие задачи:

1. Исследование современных угроз информационной безопасности и вредоносных программ в компьютерных сетях.
2. Анализ актуальных методов и средств антивирусной защиты компьютерных сетей.
3. Разработка методики антивирусной защиты компьютерных сетей на железнодорожном транспорте.

Краткое содержание работы

Диссертационная работа разделена на 3 главы, посвященных решению конкретных задач.

В первой главе приведены основные теоретические положения, даны ключевые определения. Описана классификация современных угроз по нескольким признакам. Проведен анализ современных угроз информационной безопасности, рассмотрены и кратко описаны методы и приемы социальной инженерии.

Вторая глава посвящена методам и средствам обеспечения информационной безопасности и антивирусной защиты. Проанализированы и классифицированы основные методики и средства защиты. Подробно описаны современные программные средства обнаружения вредоносного программного кода. Один раздел главы также посвящен организационным методам защиты информации и роли организационных мероприятий в обеспечении антивирусной защиты предприятий железнодорожного транспорта. Подробно рассмотрены и описаны базовые принципы построения системы централизованного управления антивирусной защиты, как основного средства обеспечения информационной безопасности распределенной компьютерной сети. предприятия.

Следущая глава посвящена непосредственно разработке методике антивирусной защиты. Приведена базисная модель (модель жизненного цикла безопасности), описаны ее основные компоненты и их связи. На основе представленной модели проанализированы наиболее значимые особенности компьютерных сетей предприятий железнодорожного транспорта, рассмотрены перспективы их дальнейшего развития. Приведен

анализ рисков и угроз. Изложен краткий план построения системы антивирусной защиты.

На основе обобщенной интегрированной оценки эффективности осуществлен выбор программного средства антивирусной защиты. Приведены рекомендации по практическому внедрению комплекса централизованного управления антивирусной защитой. Кратко описана схема организации инфраструктуры открытых ключей в сети предприятий железной дороги.

Последний раздел третьей главы посвящен совершенствованию организационной защиты информации и содержит краткие рекомендации и описание основных мероприятий организационной защиты информации.

Заключение

Все основные результаты, изложенные в диссертационной работе, получены автором самостоятельно. Автору принадлежит определение целей и постановка задач, выбор методов исследования, непосредственное в них участие, а также обработка, анализ и интерпретация полученных результатов, формулировка выводов.

Основные положения диссертации обсуждались на научно-техническая конференции аспирантов, магистрантов и студентов БГУИР (2014). По результатам исследований в печать отправлена 1 работа.

Публикации

Особенности использования антивирусной сетевой защиты для железнодорожного транспорта. Тезисы доклада международной научно-технической конференции "Технические средства защиты информации". Май, 2015 (в печати).