РЕФЕРАТ

Ключевые слова: автоматизированная информационная система, модель SIR, email-worm, живучесть.

Объектом исследования являются рабочие станции автоматизированной информационной системы, в отношении которых реализуются атаки с использованием email-worm.

Предметом исследования является риск-модель управления живучестью автоматизированной информационной системы, в отношении которой реализуются атаки с использованием email-worm.

Цели и задачи исследования.

Цель настоящей работы заключается в оценке живучести автоматизированной информационной системы как объекта защиты от деструктивных воздействий атак с использованием email-worm.

В исследовании используются методы из аппарата теории вероятности, теория графов, методы системного анализа, теории рисков, а так же теории надёжности.

Полученные результаты и их новизна:

1. В исследовании основных угроз, связанных с работой автоматизированных информационных систем, были учтены результаты их количественного и качественного развития, а также особенности реализации атак с использованием email-worm при различных;
2. В отличие от аналогичных работ, полученная риск-модель автоматизированных информационных систем системы включает в себя выражения для управления живучестью АИС при реализации атак с использованием email-worm;
3. Отличительной особенностью подхода к изучению безопасности автоматизированных информационных систем, в отношении которых реализуются атаки с использованием email-worm является изучение и управление живучестью

системы с разработкой методических рекомендаций по увеличению живучести системы.

Практическая ценность работы заключается в том, что:

1. Анализ основных видов угроз, воздействующих на компоненты автоматизированных информационных систем, позволяет выявить наиболее опасные их виды и дает возможность уделить особое внимание защите от атак с использованием email-worm.
2. Построенная математическая модель отражает этапы распространения вредоносной информации и позволяет всесторонне оценивать процесс развития негативного события
3. Построенная риск-модель может применяться для оценки рисков в предприятиях, использующих распределенные автоматизированные информационные системы как основное средство для обмена информацией и контроля работы, а также построения систем, устойчивых к воздействию атак с использованием email-worm.
4. Полученные выражения для живучести автоматизированных информационных систем позволяют оценить эффективность обеспечения защиты от реализации атак с использованием email-worm и выявить наиболее уязвимые компоненты системы.

Область применения – научные исследования и разработки.

Проведенная исследовательская работа является экономически эффективной.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена оценке рисков и живучести автоматизированной информационной системы, рабочие станции которой подвержены воздействию атаки с использованием email-worm. В ходе ее выполнения были получены следующие основные результаты:

1 Разработана модель реализации атак на рабочие станции автоматизированной информационной системы, учитывающая особенности протекания атаки с использованием email-worm.

2 Разработана итерационная модель для автоматизированной информационной системы, рабочие станции которой подвержены воздействию атаки с использованием email-worm.

3 Исследованы параметры распространения email-worm, получены формулы вычисления живучести автоматизированной информационной системы с учетом возможности реализации повторного заражения и наличием нескольких источников инфицирования.

4 Получены модели реализации атаки с использованием email-worm при различных начальных условиях. Исследовано влияние изменения различных параметров распространения червя, произведен анализ эффективности таких изменений на живучесть системы.

5 Разработан новый подход к регулированию функции живучести для автоматизированной информационной системы, рабочие станции которой подвержены воздействию атаки с использованием email-worm. Спрогнозирована ожидаемая живучесть автоматизированной информационной системы, выработаны рекомендации по минимизации ущерба на основе управления живучестью и предупреждению распространения червя.

6 Проведена оценка экономических показателей эффективности управления живучестью автоматизированной информационной системы, рабочие станции которой подвергаются атакам с использованием email-worm.

7. Управление живучестью автоматизированной информационной системы рассмотрено в контексте обеспечения безопасности жизнедеятельности.

Построенный математический аппарат, а также приведенные методики и алгоритмы управления живучестью автоматизированной информационной системы позволят проектировать и строить АИС, устойчивые к атакам с использованием email-worm, а также адекватные системы предупреждения и защиты автоматизированной информационной системы.