тема диплома, посвященная исследованию и защите ИТКС, атакуемых сетевым вредоносным обеспечением типа IRC-Worm является актуальной.

Соответствие темы диплома специальности

Данная работа посвящена построению вероятностной модели информационно-телекоммуникационной системы, адекватно отражающей процесс воздействия на нее сетевых атак типа IRC-Worm, а также разработке методики оценки и управления возникающими в данном случае информационными рисками ИТКС. Поэтому тема данной работы соответствует специальности Безопасность телекоммуникаций.

Объектом исследованияявляются ИТКС, в отношении которых реализуются сетевые атаки типа «IRC-Worm», оказывающие деструктивное воздействие на субъекты защищаемой ИТКС.

Предметом исследованияявляется риск-оценка информационной устойчивости информационно-телекоммуникационных систем в условиях реализации сетевых атак типа «IRC-Worm».

Цель и задачи исследования

Цель работысостоит в риск-анализеинформационно-телекоммуникационных систем (ИТКС) как объекта защиты от сетевых атак типа «IRC-Worm», направленных на нарушение целостности, доступности и конфиденциальности защищаемой в ИТКС информации.

Для реализации данной цели необходимо решить следующие задачи:

1. Проанализировать различные модификации исследуемого вредоносного программного обеспечения IRC-Worm и способы проникновения в ИТКС.
2. Разработать аналитическую модель атаки программы класса IRC-Worm на ИТКС.
3. Разработать аналитическую модель рисков ИТКС, подвергающейся атаке программы класса IRC-Worm.

4 Разработать алгоритм управления рисками ИТКС, подвергающейся сетевой атаки типа «IRC-Worm».

5 Провести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;

Методы исследования

Для решения поставленных задач необходимо использовать методы теории вероятности, математической статистики, теории риска, теории чувствительности, теории управления, элементы теории сложных систем, элементы теории экономического планирования.

Обоснование математической модели

Для исследования воздействия червей типа IRC-Worm на ИТКС в дипломном проекте будет проводиться математическое моделирование. Из-за того, что на практике часто точный вид плотностей распределения вероятности реальных процессов не известен, для аппроксимации используется экспоненциальное распределение. Применимость данного распределения при решении поставленных в работе задач обосновывается в работе.

На защиту выносятсяследующие основные положения работы:

1. Классификация вредоносного программного обеспечения типа «IRC-Worm», способов их проникновения на компьютеры пользователей;
2. Аналитическая модель атак программ класса IRC-Worm на ИТКС;
3. Риск-модель ИТКС, подвергающейся атаке программы класса IRC-Worm;
4. Алгоритм управления рисками ИТКС, подвергающейся атаке программы класса IRC-Worm;

5. Оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования.

Научнаяновизнаисследования

1. Классификация вредоносного программного обеспечения, способов проникновения в ИТКС, отличается от известных тем, что классификация проведена для ПО типа «IRC-Worm». На основе предложенной классификации выработана их обобщенная структура.

2. Аналитическая модель атак чатовых червей на ИТКС, основанная на экспоненциальном распределении, отличается тем, что в основу разработки моделей положен принцип предлагаемой классификации.

3. Алгоритм управления рисками ИТКС, подвергающейся атакам вредоносного программного обеспечения типа «IRC-Worm», отличается тем, что минимизация риска ИТКС проводится путем моделирования разработанной в проекте аналитической модели.

4. Оценка экономической эффективности предложенного алгоритма управления рисками ИТКС, подвергающейся атакам программ класса IRC-Worm, отличается тем, что проведена для вариантов построения систем защиты на основе предложенных моделей и алгоритма.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена исследованию и защите ИТКС, атакуемых сетевым вредоносным программным обеспечением типа «IRC-Worm». В ходе ее выполнения были получены следующие основные результаты:

1. На основании выполненных исследований, разработан новый подход к регулированию интегрального риска реализации асинхронных атак в информационно-телекоммуникационной системе путем корректировки среднего значения ущерба и среднеквадратического отклонения в компонентах системы через

изменение параметров экспоненциального распределения и параметров эпидемиологической SIS-модели ущерба.

2. Предложены суждения по оценке интегрального риска и его экстремумов для случая асинхронных сетевых атак типа «IRC-Worm» в информационно-телекоммуникационной системах, плотность вероятности наступления ущерба, в компонентах которых имеет экспоненциальное распределение.

3. Предложенная оценка экстремумов интегрального риска является перспективным подходом для улучшения качества построения риск-моделейИТКС, регулирования рисков и повышения защищенности систем.

4. Путем математического моделирования была обоснована применимость подхода по регулированию риска ИТКС, плотность вероятности наступления ущерба,в компонентах которых имеет экспоненциальноераспределение.

5. При решении задач, применительно к проблематике работы, результативно использовались методы теории сетей Петри-Маркова, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

6. В работе изложенподход к описанию ущерба наносимого ИТКС сетевой атакой типа «IRC-Worm» при помощи эпидемиологической SIS-модели.

7. Выявлены проблемы защиты ИТКС от сетевых атак типа «IRC-Worm», связанные с неэффективным применением средств защиты от атак данного типа. Решением этой проблемы является построение риск-модели, способных выявить уязвимые компоненты систем и снизить риски реализаций сетевых атак типа «IRC-Worm».

8. В работе изучен генезис процесса подготовки и реализации сетевых атак типа «IRC-Worm», при помощи построения сетей Петри-Маркова и анализа данных поведения червя в системе.

9. На основе оценки экстремумов интегрального риска для систем, состоящих из двух компонентов, была произведена оценка экстремумов