Цель исследования состоит в риск-анализе распределенных автоматизированных систем(РАС) как объекта защиты от DDoS-атак, направленных на нарушение доступа к защищаемой в РАС информации.

Для реализации цели необходимо решить следующие **задачи**:

1. Проанализировать атаки,направленные наРАС, типа «отказ в обслуживании» и, в частности,DDoS-атаки направленные на РАС, а также механизмы защиты от DDoS-атак.

2. Построитьстатическую и динамическую риск-моделиDDoS-атакина защищаемую РАС.

3. На основе построенной модели разработать рекомендации по повышению защищенности РАС, в отношении которой производятся DDoS-атаки.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

В исследовании используются методы теории графов, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

На защиту выносятся следующие основные результаты работы:

1. Результаты анализа процесса реализации DDoS-атак в отношении РАС имеханизмов защиты от атак данного типа.

2. Результаты этапов построения статической и динамическойриск-модели DDoS-атаки на защищаемую распределенную автоматизированную систему.

3.Рекомендации по повышению защищенности РАС, на которую производятся DDoS-атаки.

Научная новизна результатов исследования заключается в следующем:

1. В отличие от аналогов, при исследовании распределенных атак типа «отказ в обслуживании» направленные на РАС, учитывалась степень автоматизации процесса подготовки и реализации атаки, а также учитывался способ распространения вредоносного программного обеспечения, посредством которого производится атака.

2. В отличие от аналогичных моделей, при построениириск-моделейDDoS-атак направленных на распределенные автоматизированные системы, произведена оценка экстремумов интегрального рискав общем виде для РАС в целом.

3. В отличие ранее проведенных исследований, на основании полученной риск-модели,предложены рекомендаций по повышению защищенности РАС путем регулирования рисков посредством изменения параметров распределения ущербов, связанных с реализацией распределенных атак типа «отказ в обслуживании».

Практическая ценность работызаключается в том, что:

1. Анализ механизмов реализации распределенных атак типа «отказ в обслуживании» в коммерческих и государственных организациях, использующих в своей работе сетевые технологии, позволяет выявить наиболее опасные атаки для конкретно взятой системы и на основании этого построить более эффективную риск-модель. Анализ механизмов защиты от DDoS-атак позволяет подобрать наиболее эффективные для данной организации механизмы защиты от конкретных атак.

2. Полученные статическая и динамическая риск-модели могут быть использованы для построения в государственных и коммерческих организациях систем, устойчивых к DDoS-атакам, оценки эффективности обеспечения защиты от DDoS-атак в данных организациях, выявления наиболее уязвимых к атакам ресурсов организаций.

3. Предложенные рекомендации по регулированию рисков позволяют снизить риски для наиболее уязвимых компонент систем,а также диапазон ущербов для системы в целом, что открывает возможности по повышениюзащищенности организаций от распределенных атак типа «отказ в обслуживании», использующих в своей работе сетевые технологии.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена исследованию DDoS-атак на распределенные автоматизированные системы посредством анализа рисков. В ходе ее выполнения были получены следующие основные результаты:

1. На основании выполненных исследований, разработанновый подход к регулированию интегрального риска реализации асинхронных атак в распределенной автоматизированной системе путем корректировки среднего значения ущерба и среднеквадратического отклонения в компонентах системы через изменение параметров гамма-распределения.

2. Предложены оригинальные суждения по оценке интегрального риска и его экстремумов для случая асинхронных распределенных атак типа «отказ в обслуживании» в распределенных автоматизированных системах, плотность вероятности наступления ущерба, в компонентах которых имеет гамма-распределение.

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

4. Изменена трактовка понятия распределенной атаки типа «отказ в обслуживании» с точки зрения учета степени автоматизации процесса подготовки и реализации атаки, а также способа распространения вредоносного программного обеспечения, посредством которого производится атака.

5. Путем математического моделирования была обоснована применимость подхода по регулированию риска РАС, плотность вероятности наступления ущерба,в компонентах которых имеет гамма-распределение.

6. При решении задач, применительно к проблематике работы, результативно использовались методытеории графов, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

7. В работе изложены отличающиеся от аналогичных подходы к оценке и регулированию рисков в РАС, подвергающимсяDDoS-атакам, плотность