РЕФЕРАТ

Ключевые слова: сеть Next Generation Network, атаки «IP-спуфинг», защита информации, риск-модель, защищенность сети, алгоритм повышения защищённости.

Объектом исследования являются компоненты сети NGN, в отношении которых совершаются сетевые атаки.

Предметом исследования является оценка рисков реализации атак «IP-спуфинг» на компоненты сети NGN.

Цель настоящей работы заключается в разработке и исследовании методов защиты информации при организации интеллектуальных сетей.

В исследовании предполагается использовать методы теории вероятностей, математической статистики и статистического анализа, а также методы теории графов.

Научная новизна исследования заключается в том, что в разработанной модели ущерба реализации удаленной атаки «IP-спуфинг» отражены особенности сети NGN, позволившие исследовать действия злоумышленника и оценить ущерб как на уровне единичного компонента, так и на уровне сети в целом.

Практическая ценность работы заключается в том, что разработанные методические рекомендации могут быть внедрены в корпоративные и государственные организации с целью повышения защищенности в отношении противодействия атакам «IP-спуфинг» при переходе на сетевую технологию NGN.

Рисунок П1 - Функциональная архитектура сети NGN

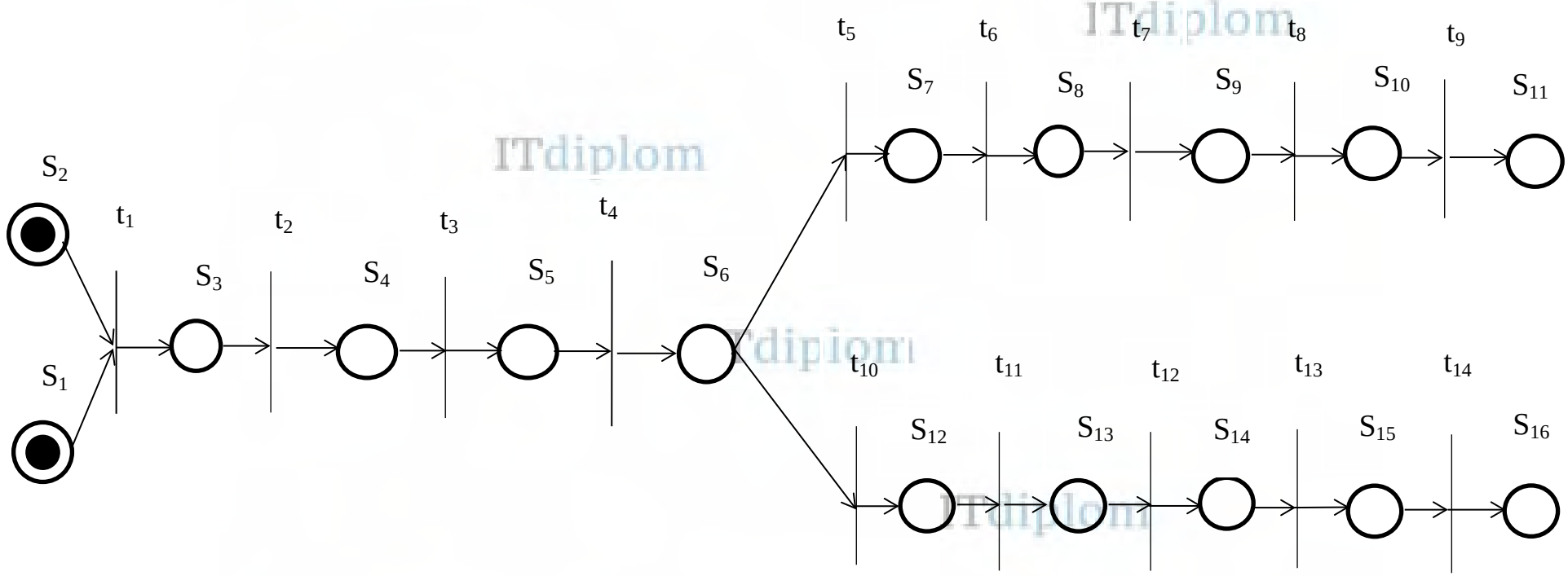

Рисунок П2 - Граф реализации удаленной атаки «IP-спуфинг» в NGN сети

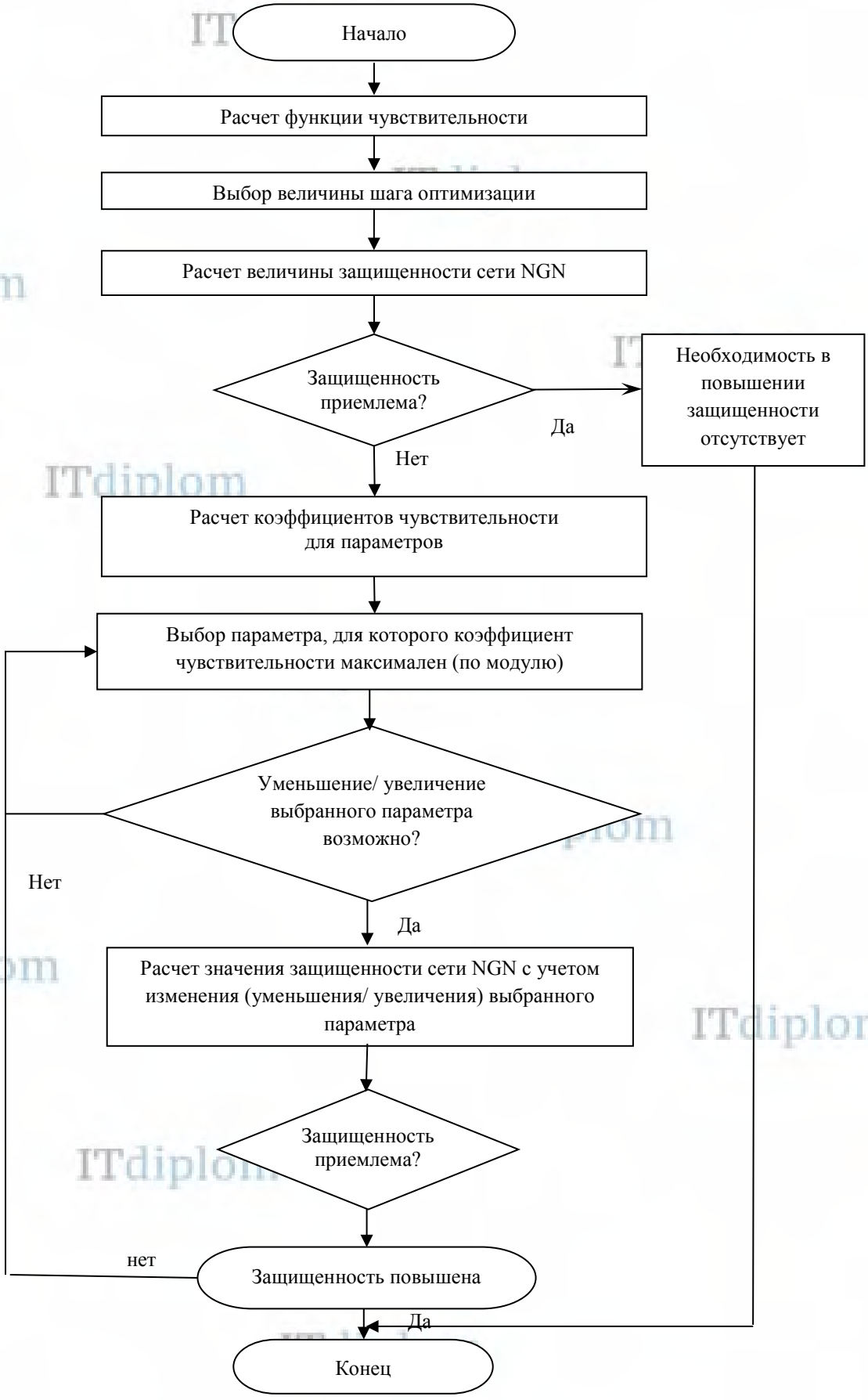

Рисунок П3 - Алгоритм управления защищенностью сети NGN