РЕФЕРАТ

Ключевые слова: медицинское учреждение, персональные данные, атаки подмены IP-адреса, лабораторный комплекс, распределенная система защиты информации, риск-модель, алгоритм повышения защищённости.

Объектом исследования являются компоненты информационных систем медицинских учреждений, в отношении которых реализуются атаки подмены IP-адреса.

Цель настоящей работы заключается в разработке лабораторного комплекса по формированию распределенной системы защиты информации, использование которого позволяет повысить защищенность медицинского учреждения.

В работе предложен подход к разработке лабораторного комплекса по формированию распределенной системы защиты информации медицинского учреждения, отражающий алгоритм управления функцией защищенности, а также влияние методов защиты информации и мероприятий по повышению защищенности информационной системы медицинского учреждения. Разработанный лабораторный комплекс управления защищенностью не просто представляет собой теоритических подход, но и содержит рекомендации к повышению защищенности, а также пригоден к внедрению в распределенную систему защиты информационной системы медицинского учреждения.

В работе используются методы теории вероятностей, математической статистики и статистического анализа, а также методы теории графов.

Практическая ценность работы заключается в том, что разработанные методические рекомендации могут быть внедрены в корпоративные и государственные медицинские учреждения с целью повышения защищенности в отношении противодействия атакам подмены IP-адреса.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 6
1 ИССЛЕДОВАНИЕ ВОПРОСА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ 10
1.1 Выявление и анализ информации, подлежащей защите в медицинском учреждении 10
1.2 Разработка модели потенциального злоумышленника информационной безопасности медицинского учреждения 14
1.3 Оценка актуальности угроз безопасности информационных систем медицинских учреждений 17
1.4 Требования безопасности, предъявляемые к информационным системам медицинских учреждений 27
1.5 Постановка задач исследования 29
2 РИСК-МОДЕЛИРОВАНИЕ АТАК ПОДМЕНЫ IP-АДРЕСА НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ 31
2.1 Действия злоумышленника и последствия реализации атаки подмены IP-адреса 31
2.2 Разработка математической модели реализации атаки подмены IP-адреса . 35
2.3Оценка функции ущерба реализации атаки подмены IP-адреса, направленной на получение персональных данных и вывод из строя медицинского оборудования 41
2.4 Оценка функции ущерба реализации атаки подмены IP-адреса, направленной на замедление работы информационной системы медицинского учреждения 48
2.5 Обоснование выбора аналитического выражения функций риска и защищенности информационной системы медицинского учреждения 55
2.6 Основные выводы по главе 60

3 РАЗРАБОТКА ЛАБОРАТОРНОГО КОМПЛЕКСА ПО ФОРМИРОВАНИЮ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ 62
3.1 Оценка динамики защищенности информационной системы медицинского учреждения в условиях реализации атак подмены IP-адреса 62
3.2 Оценка влияния предложенных методов защиты и выработка рекомендаций по повышению защищенности информационной системы медицинского учреждения 69
3.3 Управление функцией защищенности информационной системы медицинского учреждения в условиях реализации атак подмены IP-адреса 75
3.4 Основные выводы по главе 81
ЗАКЛЮЧЕНИЕ 83
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 85
ПРИЛОЖЕНИЕ А 89
ПРИЛОЖЕНИЕ Б 92
ПРИЛОЖЕНИЕ В 93

ПРИЛОЖЕНИЕ Б

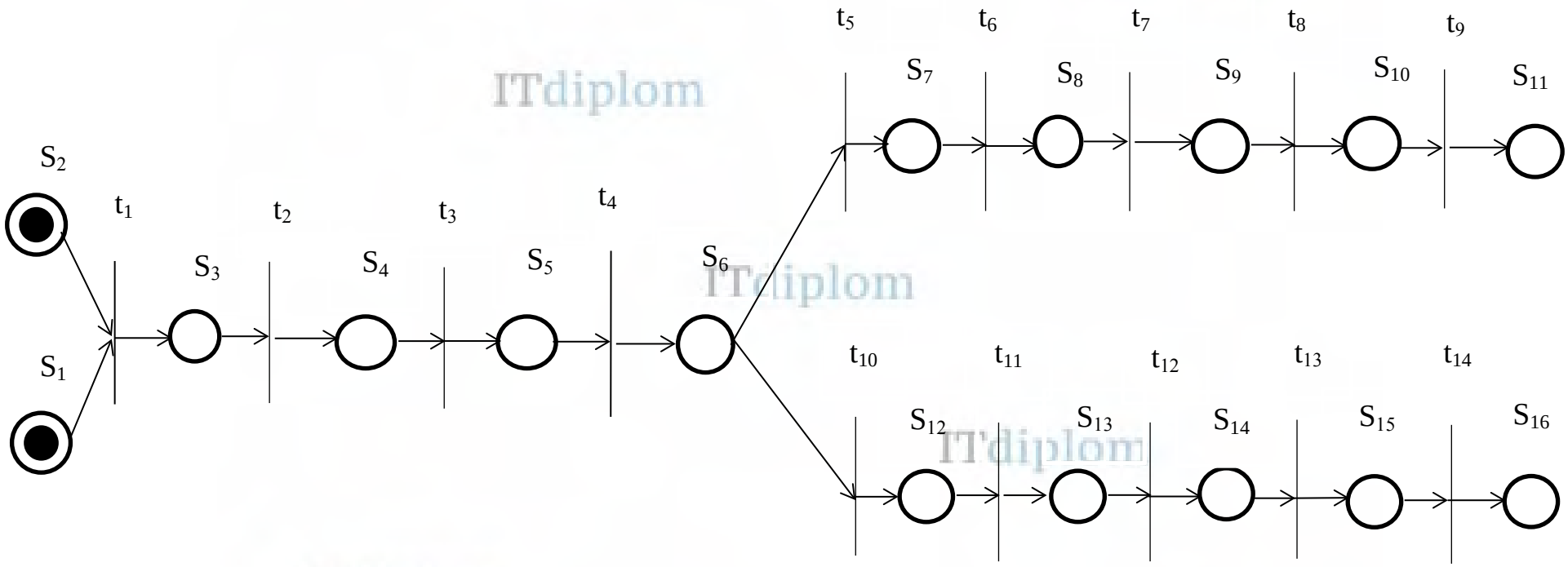

Рисунок 1 - Граф реализации атаки подмены IP-адреса компонента информационной системы медицинского учреждения

ПРИЛОЖЕНИЕ В

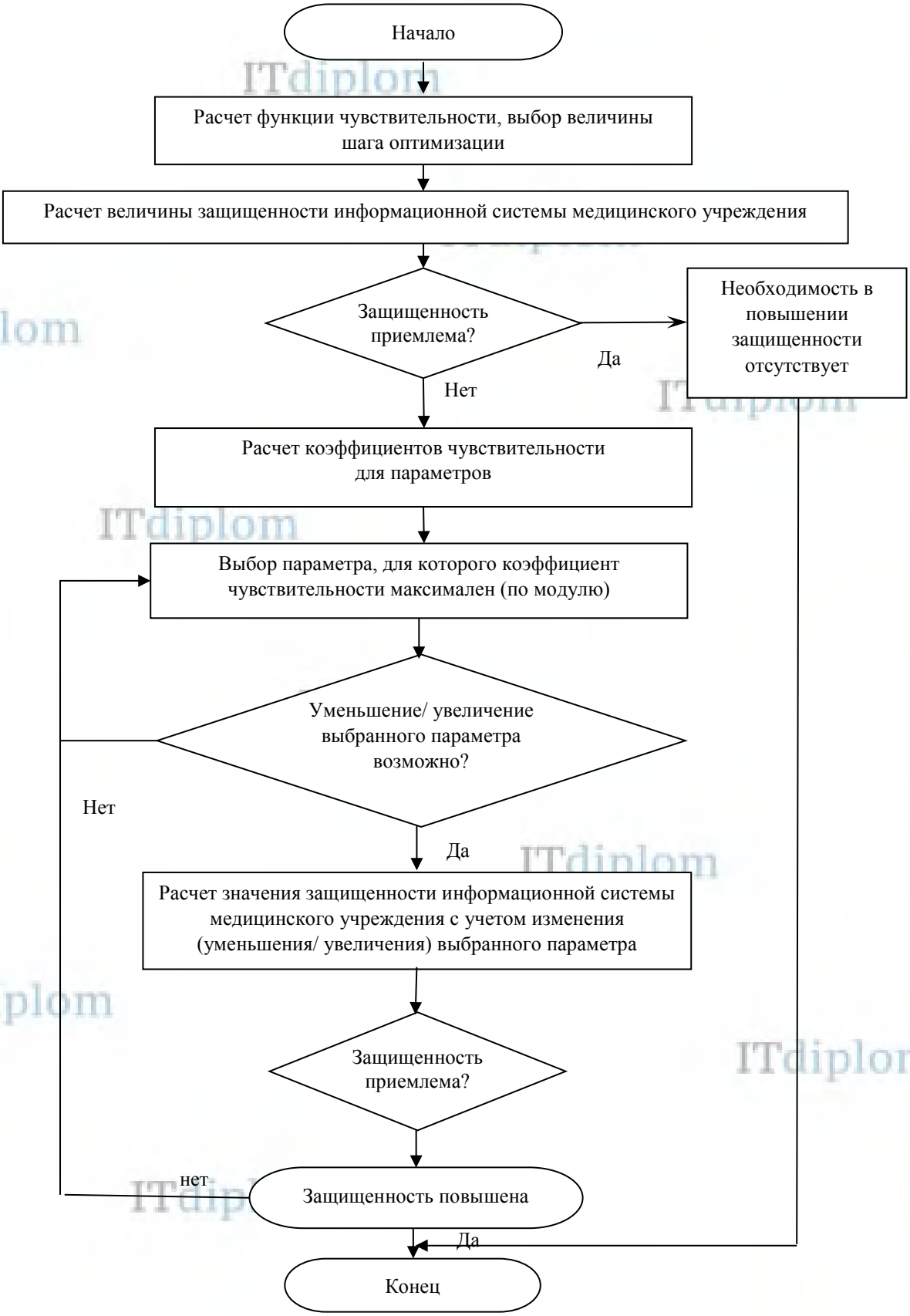

Рисунок 1 - Алгоритм управления защищенностью информационной системы медицинского учреждения