

АННОТАЦИЯ

Ключевые слова: мобильные устройства, корпоративные информационные системы, методы защиты информации, атаки с использованием подменного IP-адреса, риск-модель, защищенность системы, алгоритм повышения защищённости.

Объектом исследования являются компоненты корпоративных информационных систем, имеющих в составе мобильные устройства, в отношении которых реализуются атаки с использованием подменного IP-адреса.

Цель настоящей работы заключается в разработке рекомендаций по повышению защищенности корпоративных информационных систем, имеющих в составе мобильные устройства.

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

В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

1. Разработанная описательная модель корпоративной информационной системы отличается от известных тем, что включает анализ угроз, связанных с работой включенных в состав мобильных устройств и учитывает принципы построения современных систем.

2. Разработанная модель ущерба реализации атак с использованием подменного IP-адреса отличается от известных тем, что в ней отражены особенности корпоративной информационной системы, имеющей в составе мобильные устройства, что позволяет более детально исследовать действия нарушителя.

3. Разработанный алгоритм управления функцией защищенности корпоративной информационной системы, имеющей в составе мобильные

устройства, отличается от известных тем, что отражает степень влияния предложенных методов защиты информации.

Практическая ценность работы заключается в том, что:

1. Анализ угроз, воздействующих на корпоративные информационные системы, имеющие в составе мобильные устройства, позволяет выявить наиболее опасные их виды и дает возможность владельцам систем уделить особое внимание защите от атак с использованием подменного IP-адреса.

2. Построенная модель ущерба реализации сетевых атак на компоненты корпоративной информационной системы, имеющей в составе мобильные устройства, включает возможность дополнения необходимым набором параметров нарушителя и системы. Такая модель позволяет владельцу системы оценить ущерб от реализации атак с использованием подменного IP-адреса для конкретного нарушителя, реализуя переход от универсальной к более точной модели.

3. Разработанные методические рекомендации могут быть внедрены в корпоративные и государственные организации с целью повышения защищенности в отношении противодействия атак с использованием подменного IP-адреса при переходе на использование в сети мобильных устройств.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ.....	7
ВВЕДЕНИЕ.....	8
1 Исследование безопасности информационных систем, компонентами которых являются мобильные устройства.....	14
1.1 Изучение особенностей и проблем использования мобильных устройств в составе корпоративных информационных систем.....	14
1.2 Анализ уязвимостей и угроз безопасности информационных систем, имеющих в составе мобильные устройства.....	23
1.3 Требования безопасности, предъявляемые к корпоративным информационным системам.....	31
1.4 Постановка задач исследования.....	34
2 Риск-моделирование атаки с использованием подменного IP-адреса на мобильные устройства корпоративной информационной системы.....	36
2.1 Действия нарушителя и последствия реализации атаки с использованием подменного IP-адреса на мобильные устройства корпоративной информационной системы.....	36
2.2 ... Разработка математической модели реализации атаки с использованием подменного IP-адреса на мобильные устройства корпоративной информационной системы.....	40
2.3 ... Оценка функции ущерба реализации атаки IP-спуфинг, направленной на получение корпоративной информации и вывод из строя технологического оборудования.....	46
2.4 .. Оценка функции ущерба реализации атак с использованием подменного IP-адреса, направленной на замедление работы корпоративной информационной системы.....	54
2.5 Обоснование выбора аналитического выражения функций риска и защищенности корпоративной информационной системы.....	63
2.6 Основные выводы по главе.....	68

3 Разработка методов защиты информации и управление защищенностью корпоративной информационной системы в условиях реализации атак с использованием подменного IP-адреса.....	70
3.1 Оценка динамики защищенности корпоративной информационной системы в условиях реализации атак с использованием подменного IP-адреса.....	70
3.2 Оценка влияния предложенных методов защиты и выработка рекомендаций по повышению защищенности корпоративной информационной системы	78
3.3 Управление функцией защищенности корпоративной информационной системы в условиях реализации атак с использованием подменного IP-адреса.....	85
3.4 Основные выводы по главе	91
ЗАКЛЮЧЕНИЕ	93
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	95
Приложение А	99

Приложение А

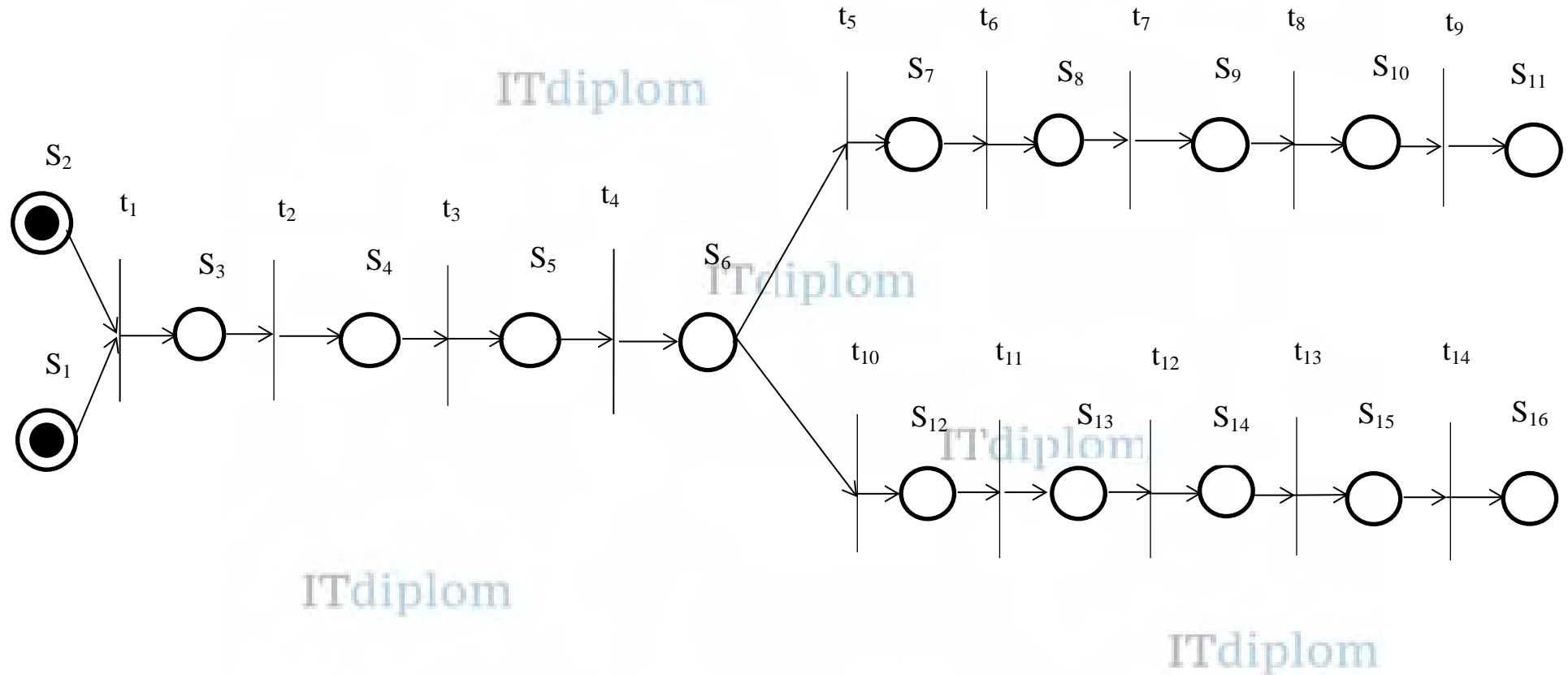


Рисунок 1 - Граф реализации удаленной атаки с использованием подменного IP-адреса мобильного устройства корпоративной информационной системы

Приложение Б

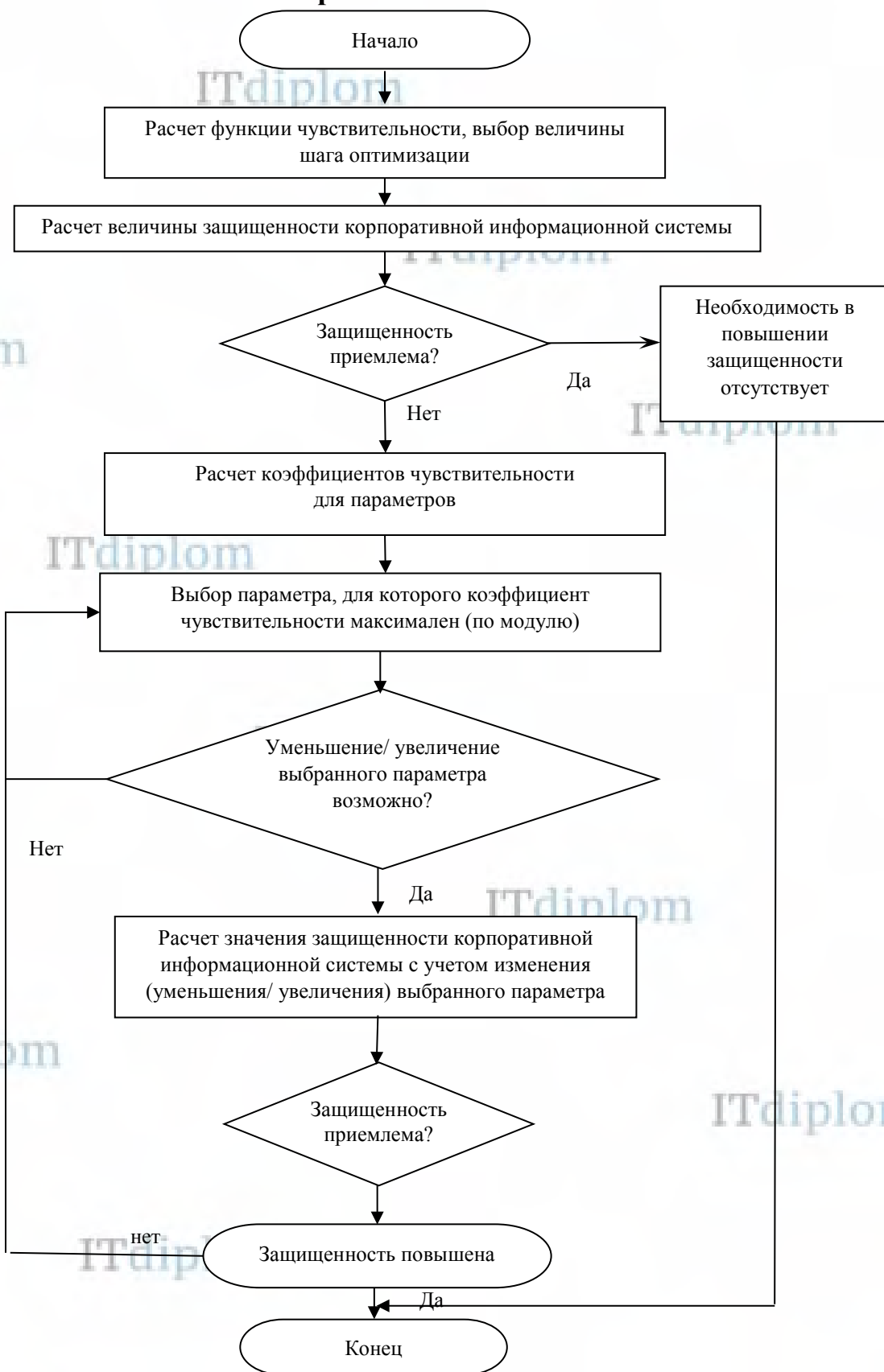


Рисунок 1 - Алгоритм управления защищенностью корпоративной информационной системы, имеющей в своем составе мобильные устройства