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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Martinelli F. A survey on security for mobile devices. Common Surv Tutorials IEEE – 2013–56 p.
2. Bulgurcu B. Information security policy compliance, an empirical study of rational–based beliefs and informalion security awareness. – 2010 – P. 41–45.
3. Flowerday S. Smartphone informantion securety awareness: A victim of operational pressures. Computers & Security, Volume 42, May 2014. – P. 132–136.
4. Куканова Н. BYOD: в поисках компромиссов // Безопасность Деловой Информации. – 2014. – №7. – С. 38–41.
5. Allam S. An adaptation of the awardeness boundary model for smartphone computing. In: ISSA 2011. Johannesburg: IEEE; 2011. – С. 1–8.
6. Botha R. From desktop to mobile: examiner the securety expertience. Comput Secur 2009. – P. 67–69.
7. Михайлов Д. М., Жуков И. Ю. Защита мобильных телефонов от атак; Фойлис – Москва, 2011. – 192 с.
8. Якушин Петр. Безопасность мобильного предприятия// Открытые системы № 01, 2013. – С. 164–165.
9. Шетько Николай. Взлом сотовых сетей GSM: расставляем точки над «i»// ET CETERA – серия цифровых журналов, распространяемых по подписке № 32, 2013. – С. 76–78.
10. Безкоровайный Д. Безопасность мобильных устройств // Открытые системы. СУБД, М: Издательство «Открытые системы», 2011. – 26 с.
11. Бельтов А.Г. Вопросы безопасности мобильных устройств // Безопасность информационных технологий М.: Всероссийский научно–исследовательский институт проблем вычислительной техники и информатизации, 2012. – С. 5–7.

12. Белорусов Д.И. Wi–Fi – сети и угрозы информационной безопасности/ Д.И. Белорусов, М.С. Корешков // СПЕЦИАЛЬНАЯ ТЕХНИКА № 6, 2009; С. 2–6.

13. Коржов Валерий. Скорость и безопасность в LTE// «Сети/network world» №6, 2012. – С. 23–25.

14. Ванг Й. Проблемы безопасности смартфонов // Открытые системы. СУБД, М: Издательство «Открытые системы», 2013. – С. 23–31.

15. Генералов Д.Н. Идентификация скрытых каналов утечки информации при инсталляции инсайдера в мобильное устройство // Вестник поволжского государственного университета, 2009. – С. 25–29.

16. Михайлов Д.М. Защита мобильных телефонов от атак М.: Фойлис, 2011. – 192 с.

17. Орлов А.Н. Подвижные и опасные // Журнал «CIO: руководитель информационной службы» – №12, 2011. – С. 13–15.

18. Хаккарайнен А.П. Как защититься от мобильных угроз // Computerworld Россия – №24, 2007. – С. 32–34.

19. Куликов С.С. Метод риск–анализа информационно–телекоммуникационных систем при атаках на их ресурсы / С.С. Куликов, В.И. Белоножкин // Информация и безопасность, 2013. – Т. 16. – №1. – С. 143–144.

20. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска угроз безопасности сетей связи от экспертных данных при расчетах с использованием теории нечетких множеств // Вопросы кибербезопасности. 2014. – С. 61–67.

21. Бельфер Р.А., Морозов А.М. Информационная безопасность сети связи для соединения абонентов ТфОП/ISDN через SIP–T // Электросвязь. 2012. No 3. – С. 22–25.

22. Воронов А.А. Применение методологического анализа в исследовании безопасности / А.А. Воронов, И.Я. Львович // Информация и безопасность. – М.: 2011. – № 3. – С. 469–470.

23. Любченков А.В. Особенности взаимодействия владельцев информационных ресурсов при передаче конфиденциальной информации / А.В. Любченков, В.Г. Юрасов // Информация и безопасность, 2013. – Т. 16. – № 2. – С. 185–190.

24. Мак–Клар С. Секреты хакеров. Безопасность сетей – готовые решения, 2–е издание / С. Мак–Клар, Д. Скембрей, Д. Курц. – М.: Издательский дом «Вильямс», 2005. – С. 656–658.

25. Федотов Н. В. «Оценка и нейтрализация рисков в информационных системах»: Методическое пособие по курсу «Основы информационной безопасности» / Н.В. Федотов, В.А. Алешин; Под ред. Н.В. Медведева. – М.: Изд–во МГТУ им. Н.Э.Баумана, 2004. – С. 16–22.

26. Шевченко Е.Н. Математическое моделирование распределения риска при независимых случайных величинах вероятностей исходных событий и ущерба / Е.Н. Шевченко // Фундаментальные исследования, – 2011. – № 12. – С. 604–608.

27. Бутузов В.В. Риск–анализ в интервале времени: некоторые приложения / В.В. Бутузов, Л.Г. Попова // Информация и безопасность. – М.: 2013. – № 1. – С. 137–138.

28. Ермилов Е.В. Риск–анализ распределенных систем на основе параметров рисков их компонентов / Е.В. Ермилов, Е.А. Попов, М.М. Жуков, О.Н. Чопоров // Информация и безопасность. – М.: 2013. – № 1. – С. 123–126.

29. Жидко Е.А. Информационные риски как аргумент безопасного и устойчивого развития организаций / Е.А. Жидко, Л.Г. Попова // Информация и безопасность, 2010. – №4. – С. 543–552.

30. Карайчев Г.В. Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети. Известия высших учебных заведений / Г.В. Карайчев, В.А. Нестеренко // Естественные науки, 2008. – №1. – С.10–13.

31. Куликов С.С. Оценка общего риска информационно–телекоммуникационных систем при асинхронных воздействиях эффекта

«unicast flooding» / С.С. Куликов, И.Д. Петров, Н.Н. Толстых // Информация и безопасность, 2013. – Т. 16. – №2. – С. 249–250.

32. Кудрявцев А.М. Киберустойчивость информационно–телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи / СПб.: Бостон–спектр, 2015. – 150 с.

33. Остапенко А.Г. Жизнестойкость атакуемых распределенных систем: оценка рисков фатальных отказов компонентов: Монография / А.Г. Остапенко, Д.Г. Плотников, О.Ю. Макаров, Н.М. Тихомиров, В.Г. Юрасов; под ред. чл.–корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга», 2013. – С. 89–95.

34. Пастернак Ю.Г. К вопросу моделирования процесса реализации атак посредством компьютерных червей / Ю.Г. Пастернак, Н.Н. Корнеева, К.В. Дегтярева // Информация и безопасность, 2014. – Т. 17. – Вып. 2. – С. 330–331.

35. Радько Н.М. Противодействие вирусным атакам на сетевые структуры на основе риск–оценки / Н.М. Радько, Л.В. Паринова, Ю.Г. Пастернак, К.А. Разинкин, Н.М. Тихомиров // Информация и безопасность, 2013. – Т.16. – Ч. 4. – С. 502–503.

Приложение А

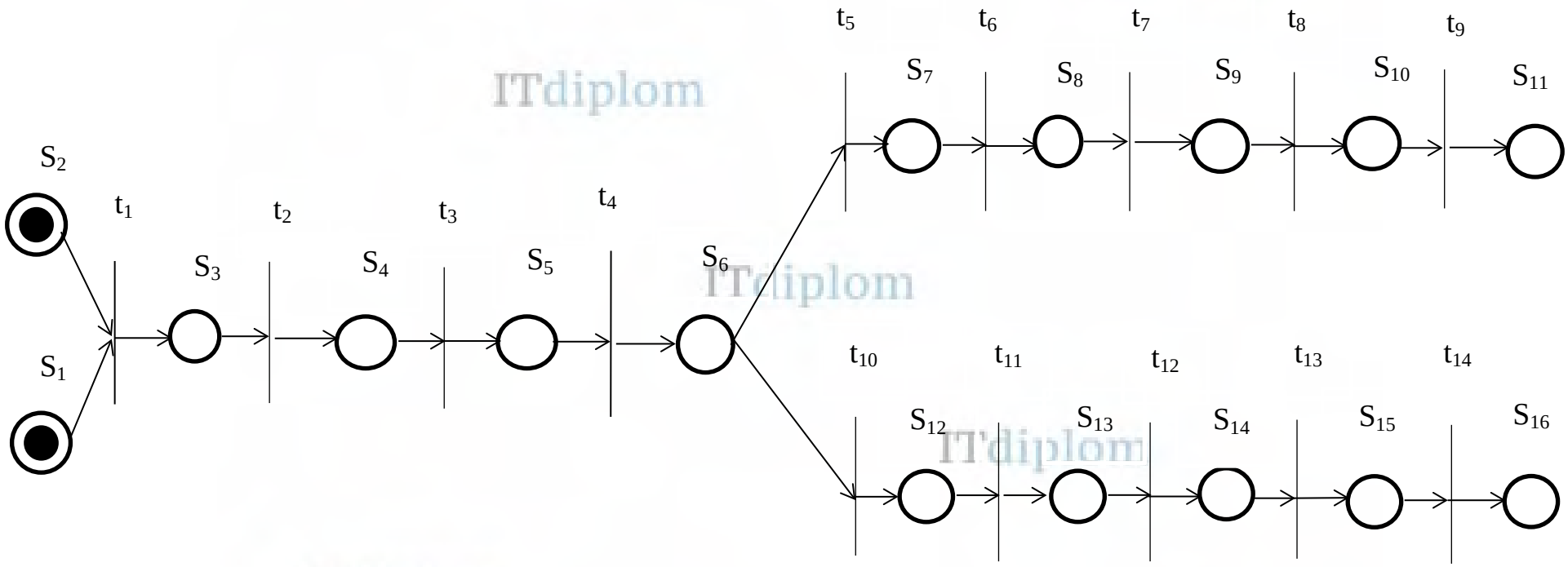

Рисунок 1 - Граф реализации удаленной атаки с использованием подменного IP-адреса мобильного устройства корпоративной информационной системы

Приложение Б

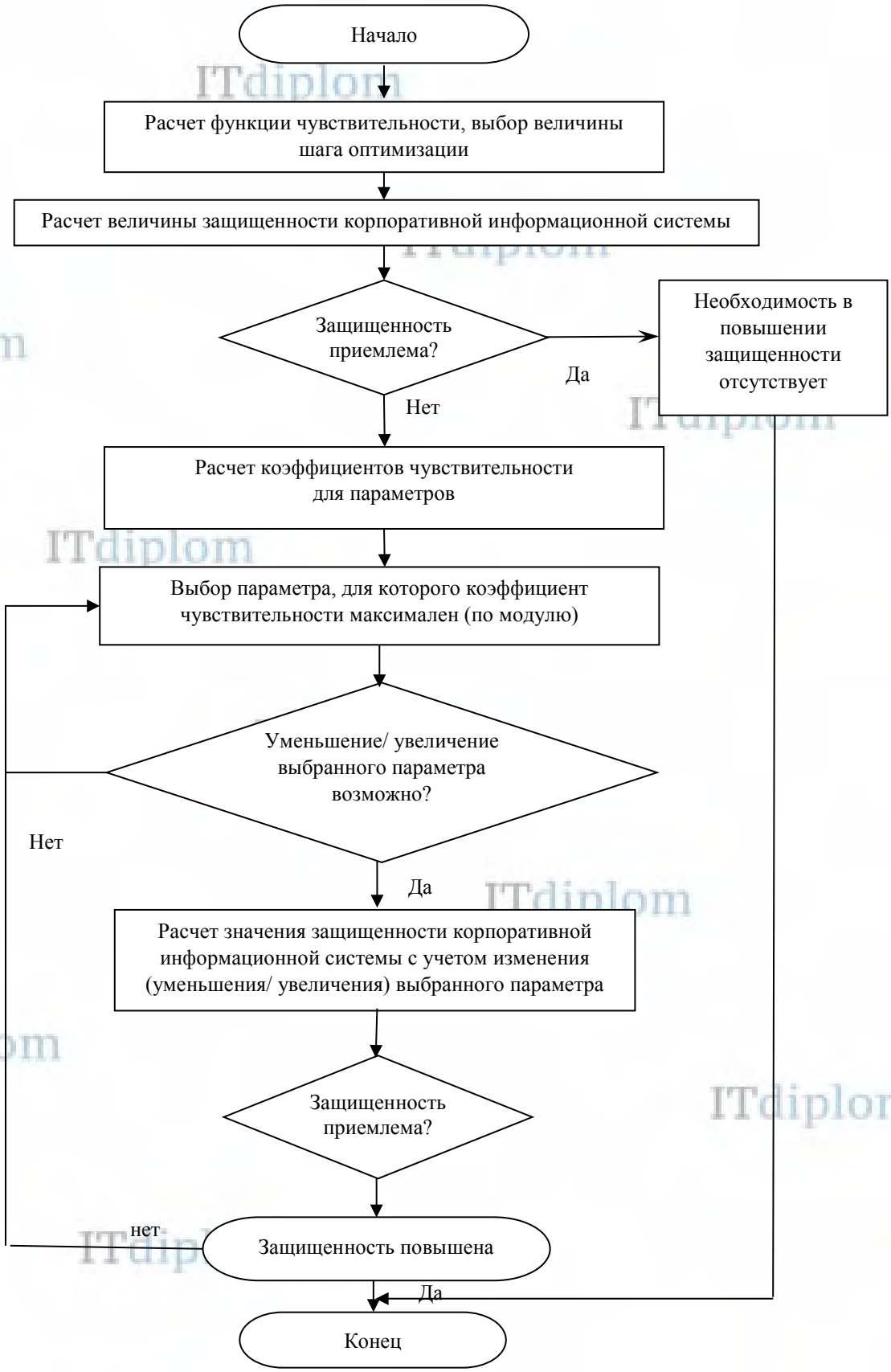

Рисунок 1 - Алгоритм управления защищенностью корпоративной информационной системы, имеющей в своем составе мобильные устройства