Методика изменения структур информационной системы в условиях воздействия сетевой разведки

М. А. Каплин, email: MacKaplin@yandex.ru [1]

[1] Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко

Аннотация. *В данной статье рассматривается актуальность защиты информационных систем от компьютерных атак, носящих разведывательный характер, представлена постановка задачи на оптимизацию показателей эффективности изменения структур информационной системы в условиях воздействия сетевой разведки и его методика.*

Ключевые слова: *Информационная система, сетевая разведка, ложные компоненты.*

Введение

Повсеместная информатизация в различных сферах деятельности ведомств и организаций, обусловленная повышением эффективности в достижении поставленных целей, существенно повышает роль применяемых информационных технологий. Объединение различных информационных ресурсов на инфраструктуре сетей связи общего пользования (ССОП) существенно оптимизирует процессы информационного взаимодействия между их участниками, но, в свою очередь, увеличивает количество деструктивных воздействий на все составляющие информационных систем [1].

Так как взаимодействие между сегментами информационных систем (ИС) осуществляется через ССОП, передача информационных потоков между ними повышает возможности сетевой разведки (СР) по вскрытию состава, структуры и алгоритмов функционирования ИС [2, 3]. В ведомственных ИС обеспечение безопасности осуществляется в соответствии с требованиями регуляторов. При этом, применение традиционных средств защиты, основанных на реализации запрещающих регламентов, вынуждают злоумышленника находить новые способы преодоления системы защиты [4]. Создание (эмуляция) ложных компонентов ИС, предоставляемых в качестве целей для злоумышленника при осуществлении им компьютерных атак, позволяет проводить регистрацию и анализ действий злоумышленника в целях

последующего противодействия компьютерным атакам. Однако статичность сетевых параметров ложных компонентов (ЛК) ИС со временем может привести к их компрометации.

Разработанные технологии динамического управления сетевыми параметрами абонентов клиент-серверных вычислительных сетей (КС ВС) [5-10] позволяют управлять изменениями конфигурации ИС. Однако, нерелевантная периодичность смены сетевых параметров абонентам КС ВС может привести к их вскрытию злоумышленником в случае не обнаружения фактов воздействия СР средствами системы обнаружения атак (СОА), либо к отказу в обслуживании абонентов ИС, вызванной слишком частой сменой сетевых параметров.

1. Постановка задачи

ИС представляет собой совокупность данных, технического и программного обеспечения, персонала, а также коммуникационного оборудования, соединенного физическими линиями связи. Взаимодействие между субъектами ИС осуществляется на основе клиент-серверной архитектуры построения вычислительных сетей. В процессе конфигурирования сетевых параметров ИС DHCP-сервер формирует и направляет каждому сетевому устройству сообщения с новыми сетевыми параметрами. При этом, новые сетевые параметры задаются эмулированным ЛК ИС. Процесс смены СФХ клиентам ИС обеспечивается протоколом DHCP (Dynamic Host Configuration Protocol). По истечении времени аренды сетевых параметров или с поступлением заявок от СОА о фактах воздействия средств СР, производится реконфигурация сетевых параметров ИС.

Суть процесса изменения структур ИС в условиях воздействия СР сводится к оценке достаточности применяемых мер сетевой защиты от воздействий СР на этапе исследования ею состава и структуры ИС, в процессе многошаговой смены сетевых параметров абонентам ИС и эмулируемым ЛК на каждом этапе смены СФХ, как представлено на рис. 1. В зависимости от наличия или отсутствия фактов идентификации средствами СОА попыток исследования логической структуры ИС средствами СР, определяется время аренды сетевых параметров участникам информационного обмена и эмулируемым ЛК, рассчитанное на этапе масштабирования КС ВС, на основе которой реализована ИС.

Время аренды сетевых параметров рассчитывается таким образом, чтобы не позволить СР идентифицировать топологию и типологию реальной структуры ИС, тем самым нивелируя полученные в ходе сканирования СР результаты. Применение технологий сетевого маскирования, в том числе и к ЛК введет дополнительную обфускацию относительно структуры ИС.

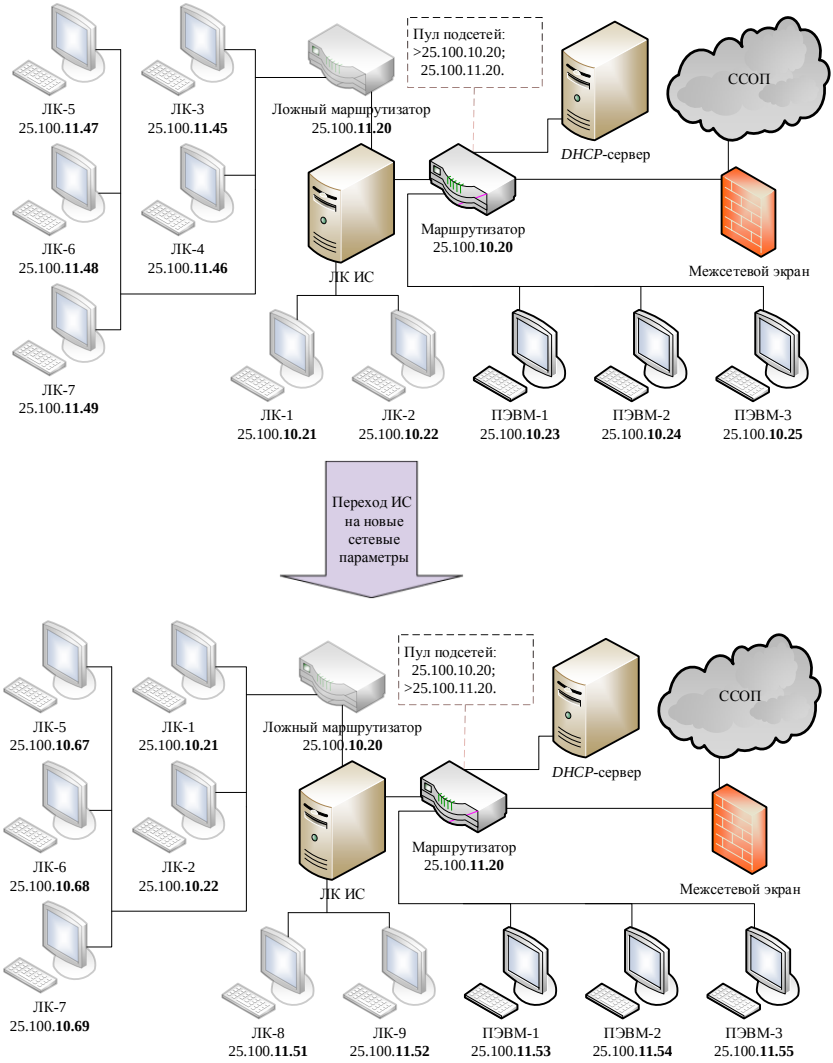

Рис. 1. Схема процесса изменения структур ИС

Показателем эффективности изменения структур ИС в условиях воздействия СР является максимизация вероятности бескомпроматного функционирования ИС в условиях воздействия СР $P_D^C(t) \to \min$.

2. Методика изменения структур информационной системы в условиях воздействия сетевой разведки

Назначением разработанной методики является релевантное изменение как истинной структуры сетевых устройств, так и структуры ЛК ИС, обеспечивающая повышение результативности защиты за счет изменения значений IP-адресов клиентов в зависимости от условий функционирования КС ВС и действий СР, в рамках задаваемого пула IP-адресов сети.

Теоретической основой методики являются теории систем управления, вероятности, массового обслуживания, исследования операций.

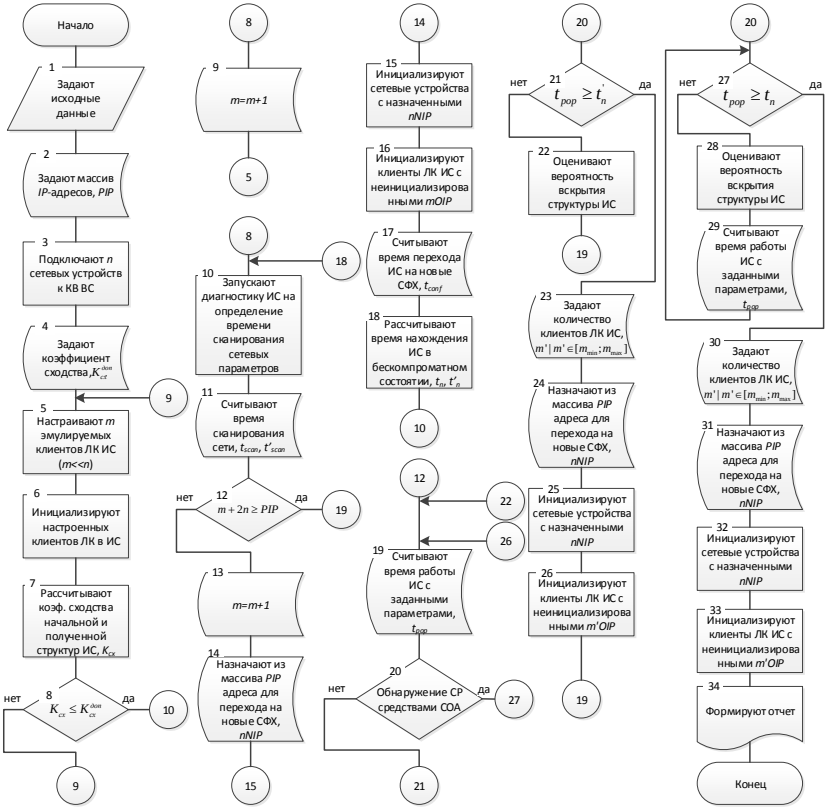

Рис. 2. Блок-схема последовательности действий, реализующих методику изменения структур ИС в условиях воздействия СР

Блок-схема методики изменения структур ИС в условиях воздействия СР, представленная на рис. 2, включает следующие этапы:

1. Задают основные исходные данные, обозначение и описание которых приведены в табл.

Таблица

Обозначение и описание основных исходных данных

Переменная	Описание
K_{cx}^{don}	Коэффициент минимально допустимого сходства двух структур ИС (первоначальной и после смены сетевых параметров), задаваемый декларативно
PIP	Пул (множество) IP-адресов, определяемый для последующего их распределения (перераспределения) клиентам ИС DHCP-сервером
NIP	Множество IP-адресов, распределяемых клиентам ИС в процессе смены сетевых параметров
OIP	Сменяемые IP-адреса, оставляемые в КС ВС в качестве ЛК
K_{cx}	Коэффициент сходства двух структур ИС
t_n	Время нахождения ИС в бескомпроматном состоянии
t'_n	Время нахождения ИС в бескомпроматном состоянии при сканировании сети с отсрочкой тайминга
t_{conf}	Время, за которое ИС переходит на новые СФХ
t_{scan}	Время сканирования СР полученной в процессе перевода на новые СФХ ИС, определяемое в процессе диагностики сети
t'_{scan}	Время сканирования СР полученной в процессе перевода на новые СФХ ИС с отсрочкой тайминга, определяемое в процессе диагностики сети
t_{pop}	Время функционирования ИС с действующими сетевыми параметрами

2. Задают массив IP-адресов, предназначенных для распределения (перераспределения) сетевым устройствам и ЛК ИС DHCP-сервером.

3. Подключают n сетевых устройств к КС ВС.

4. Задают коэффициент сходства K_{cx}^{don}.

5. Настраивают m эмулируемых клиентов ЛК ИС, причем $m << n$.

6. Инициализируют настроенных клиентов ЛК в ИС.

7. Рассчитывают коэффициент сходства начальной и полученной структур ИС (первоначальной и после смены сетевых параметров) $K_{сх}$.

8. Сравнивают коэффициент сходства двух структур ИС (первоначальной и после смены сетевых параметров) $K_{сх}$ с минимально допустимым коэффициентом сходства $K_{сх}^{доп}$.

9. Если коэффициент сходства двух структур ИС (первоначальной и после смены сетевых параметров) $K_{сх}$ превышает минимально допустимый коэффициент сходства $K_{сх}^{доп}$, увеличивают количество эмулируемых клиентов ЛК ИС на 1 и повторяют процедуру эмуляции минимально допустимого количества ЛК и их инициализации в ИС (блоки 5-8).

10. В противном случае запускают диагностику ИС на определение времени сканирования сетевых параметров.

11. Считывают время сканирования t_{scan} и время сканирования с отсрочкой тайминга t'_{scan}.

12. Сравнивают сумму эмулированных ЛК и удвоенное количество подключенных сетевых устройств с пулом (множеством) IP-адресов, определенных для последующего их перераспределения клиентам ИС DHCP-сервером PIP.

13. Если сумма эмулированных ЛК и удвоенное количество подключенных сетевых устройств меньше количества IP-адресов, определенных для последующего их перераспределения клиентам ИС DHCP-сервером PIP, увеличивают количество эмулируемых клиентов ЛК ИС на 1.

14. Назначают из пула IP-адресов, определенных для последующего их перераспределения клиентам ИС DHCP-сервером PIP сетевые адреса для перехода на новые СФХ $nNIP$.

15. Инициализируют сетевые устройства с назначенными $nNIP$.

16. Инициализируют ЛК ИС с неинициализированными $mOIP$, высвобожденные после назначения новых сетевых адресов сетевым устройствам.

17. Считывают время перехода на новые СФХ t_{conf}.

18. Рассчитывают время нахождения ИС в бескомпроматном состоянии t_n и t'_n, и повторяют процедуру поэтапного наращивания

структуры ИС путем подключения ЛК ИС и расчета времени сканирования для каждого этапа наращивания (блоки 10-18).

19. В противном случае считывают время работы ИС с заданными сетевыми параметрами t_{pop} (от англ. – *processing on the parameters*).

20. Считывают информацию о фактах обнаружения СР средствами СОА.

21. В случае отсутствия обнаружения СР средствами СОА сравнивают время t_{pop} со временем нахождения в бескомпроматном состоянии при сканировании сети с отсрочкой тайминга t'_n.

22. В случае, если $t_{pop} < t'_n$, проводят оценку вероятности вскрытия структуры ИС средствами СР, применяя модель верификации результативности маскирования структуры информационных систем [11], после чего повторяют процедуры проверки времени работы ИС с заданными параметрами и проверки наличия фактов обнаружения СР средствами СОА (блоки 19-22).

23. В случае превышения времени работы ИС с заданными сетевыми параметрами t_{pop} времени нахождения в бескомпроматном состоянии при сканировании сети с отсрочкой тайминга t'_n, задают количество ЛК ИС m' в интервале от минимального до максимального количества ЛК ИС, назначавшихся при проведении процедуры поэтапного наращивания структуры ИС путем подключения ЛК ИС и расчета времени сканирования для каждого этапа наращивания $m' \in [m_{\min}; m_{\max}]$.

24. Назначают из массива PIP адреса для перехода на новые СФХ $nNIP$.

25. Инициализируют сетевые устройства с назначенными $nNIP$.

26. Инициализируют ЛК ИС с неинициализированными $m'OIP$, после чего повторяют процедуру периодической смены СФХ абонентам и ЛК ИС с учетом полученных результатов сканирования и рандомизацией количества подключаемых ЛК ИС (блоки 19-26).

27. В случае наличия фактов обнаружения СР средствами СОА сравнивают время t_{pop} со временем нахождения в бескомпроматном состоянии t_n.

28. В случае, если $t_{pop} < t_n$, проводят оценку вероятности вскрытия структуры ИС средствами СР.

29. Считывают время работы ИС с заданными параметрами t_{pop}, после чего повторяют процедуру сравнения t_{pop} с t_n и оценки вероятности вскрытия структуры ИС средствами СР (блоки 27-29).

30. В противном случае задают количество ЛК ИС m' в интервале от минимального до максимального количества ЛК ИС, назначавшихся при проведении процедуры поэтапного наращивания структуры ИС путем подключения ЛК ИС и расчета времени сканирования для каждого этапа наращивания $m' \in [m_{\min}; m_{\max}]$.

31. Назначают из массива PIP адреса для перехода на новые СФХ $nNIP$.

32. Инициализируют сетевые устройства с назначенными $nNIP$.

33. Инициализируют ЛК ИС с неинициализированными $m'OIP$.

34. Формируют отчет.

Заключение

Разработанная методика позволяет повысить результативность защиты структуры ИС за счет изменения логической структуры сетевых устройств и эмулируемых ЛК через интервалы времени, изменяемые адаптивно в зависимости от условий функционирования и действий средств СР. Превентивная смена сетевых параметров ЛК и сетевых устройств через рассчитываемые временные интервалы девальвирует результаты, добытые средствами СР.

Список литературы

1. Максимов, Р. В. Этюды технологии маскирования функционально-логической структуры информационных систем / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 11-12 октября 2017 года. – Санкт-Петербург : Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2017. – С. 147-154.

2. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические

ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 166-173.

3. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2009. – № 1(72). – С. 181-187.

4. Максимов, Р. В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 11-12 октября 2017 года. – Санкт-Петербург : Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2017. – С. 138-147.

5. Патент № 2219577 C1 Российская Федерация, МПК G06F 17/40. Устройство поиска информации : № 2002111059/09 : заявл. 24.04.2002 : опубл. 20.12.2003 / Е. С. Ксенз, В. А. Липатников, Р. В. Максимов [и др.] ; заявитель Военный университет связи.

6. Патент № 2331158 C1 Российская Федерация, МПК H04L 12/28. Способ выбора безопасного маршрута в сети связи (варианты) : № 2007103774/09 : заявл. 31.01.2007 : опубл. 10.08.2008 / Д. А. Кожевников, Р. В. Максимов, А. В. Павловский, Д. Ю. Юрьев ; заявитель Военная академия связи.

7. Максимов, Р. В. Модель случайных помех интегрированным системам ведомственной связи / Р. В. Максимов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 151-155.

8. Патент № 2408928 C1 Российская Федерация, МПК G06F 21/20, H04L 12/28. Способ сравнительной оценки структур информационно-вычислительной сети : № 2009129726/08 : заявл. 03.08.2009 : опубл. 10.01.2011 / П. А. Берест, К. Г. Богачев, Р. В. Максимов [и др.] ; заявитель Государственное образовательное учреждение высшего профессионального образования «Военная академия связи имени С. М. Буденного» Министерства обороны Российской Федерации.

9. Патент № 2306599 C1 Российская Федерация, МПК G06F 21/00. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети : № 2006114272/09 : заявл. 26.04.2006 : опубл. 20.09.2007 / А. А. Андриенко, Д. А. Кожевников, Р. В. Максимов [и др.] ; заявитель Военная академия связи.

10. Патент № 2355024 C2 Российская Федерация, МПК G06F 15/00, G06F 17/00. Способ мониторинга безопасности автоматизированных систем : № 2007105319/09 : заявл. 12.02.2007 : опубл. 10.05.2009 / А. С. Евстигнеев, К. М. Зорин, Р. В. Максимов [и др.] ; заявитель Военная академия связи имени С. М. Буденного.

11. Каплин, М. А. Модель верификации результативности маскирования структуры информационных систем / М. А. Каплин – Текст : непосредственный // Информатика: проблемы, методы, технология : сборник статей XXI международной научно-технической конференции. – Воронеж, 2021. – С. 737-746.