Поиск новых технических решений по маскированию структуры информационных систем на основе реконфигурирования их сетевых параметров

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, проведен анализ известных технических решений, направленных на сокрытие структуры и алгоритмов функционирования информационных систем за счет реконфигурирования сетевых параметров ее узлов и эмуляции ложных компонентов. Предложены варианты технических решений, позволяющих устранить выявленные у аналогов недостатки и повысить результативность защиты.*

Ключевые слова: *Информационная система, угрозы безопасности информации, реконфигурация сетевых параметров, ложные компоненты.*

Введение

Концепция развития процессов информационного взаимодействия между объектами и субъектами доступа предусматривает повсеместное использование высокоскоростных технологий передачи данных, повышения оперативности обмена информации между их участниками, что обусловливает необходимость объединения их в единую плоскость взаимодействия [1]. Пространством для взаимодействия различных участников информационного обмена, в том числе и нелегитимных, является сеть связи общего пользования (ССОП), чему послужило историческое развитие структур построения ССОП [2]. Однако, в этом пространстве, открытом для массового потребителя, в данном контексте – нарушителя (в том числе с высоким потенциалом, представляющего интересы иностранных государств), возникает ряд угроз информационной безопасности:

– обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

– определения типов объектов защиты;

– определения топологии вычислительной сети;
– получения предварительной информации об объекте защиты.

Противодействие угрозам безопасности информации в ведомственных информационных системах (ИС) построено на реализации мер и рекомендаций регуляторов (например, Приказы ФСТЭК России №№ 21, 27, 135, 239 и др.) [3]. Однако, применяемые на данный момент технические решения не в полной мере позволяют реализовать меры безопасности, направленные на обеспечение:

– планирования и принятия мер по предотвращению повторного возникновения инцидентов;
– навязывания нарушителю ложного представления об истинных информационных технологиях и/или структурно-функциональных характеристиках ИС;
– защиты информации в случае возникновения отказов (сбоев) в системе защиты информации ИС;
– сокрытия архитектуры и конфигурации ИС;
– управления изменениями конфигурации ИС.

В данной работе рассматриваются теоретические методы и практические реализации противодействия вышеуказанным угрозам безопасности информации локальным сегментам ИС, реализованных на основе построения ССОП.

1. Функционирование локальных сегментов информационных систем

Под локальным сегментом ИС понимается структурно обособленная ИС, объединенная с локальными сегментами каналами связи различной протяженности с использованием коммуникационных технологий (оборудования) через ССОП, с целью предоставления пользователям ИС информационных ресурсов (программ и сервисов). Доступ к информационным ресурсам ИС, в том числе удаленный, реализован с применением протоколов сетевого взаимодействия.

Использование коммуникационного оборудования (коммутаторы, маршрутизаторы) и неконтролируемых системой защиты инфраструктурных элементов, предоставляет возможности для сетевой разведки (СР) по изучению и реконструкции топологии и сетевых параметров атакуемой ИС, что является неотъемлемым этапом в подготовке к реализации компьютерных атак [4].

Таким образом, целью принятия превентивных мер защиты ИС для усложнения проведения компьютерных атак являются сокрытие данных о структуре ИС, используемых устройствах, программного обеспечения и его версиях, возможных уязвимостях и применяемых средствах защиты.

2. Реконфигурирование сетевых параметров информационных систем

Суть защиты ИС путем динамического изменения сетевых параметров узлов ИС заключается в периодическом или случайном изменении сетевых настроек абонентов системы (используемого адресного пространства и номеров портов абонентов) [5]. Техническая реализация данного подхода заключается в применении DHCP-сервера с расширенными настройками, под управлением которого производится реконфигурирование сетевых параметров узлам ИС, а синхронизация участников информационного обмена обеспечивается внесением изменений в настройки DNS-сервера.

Для снижения вероятности компрометации сетевых параметров ИС и исключения возможности идентификации средствами СР алгоритмов реконфигурации сетевых параметров узлов ИС, разработаны способы проактивной защиты вычислительных сетей на основе динамического управления адресным пространством [6].

Однако, нерелевантная периодичность смены сетевых параметров узлов ИС может привести к отказу в обслуживании легитимных абонентов ИС при избыточной смене, или к преодолению системы защиты средствами СР при недостаточной периодичности превентивной смены сетевых параметров. К тому же, сетевые адреса, высвобождаемые после реконфигурации сетевых параметров узлам ИС, создают предпосылки к компрометации элементов средств защиты.

3. Применение ложных компонентов информационных систем

Применение ложных компонентов ИС направлено на введение в заблуждение нарушителя относительно топологии и применяемых информационных технологиях ИС путем эмуляции и конфигурирования виртуальной сети. Также, использование ложных компонентов ИС позволяет создавать сетевые «приманки», эмулирующие ложные уязвимости, что позволяет своевременно регистрировать и анализировать факты воздействия средств СР в целях противодействия компьютерным атакам.

Применение данной технологии приводит значительному увеличению ресурсов, затрачиваемых злоумышленником на изучение объекта компьютерной атаки при относительно незначительном увеличении ресурсов обороняющейся стороны [7, 8].

К недостаткам применения ложных компонентов ИС следует отнести статичность сетевых параметров эмулируемых ложных узлов, что со временем может привести к их компрометации [9].

Заключение

Проведенный анализ рассмотренных технологий противодействия СР позволяет оценить специфику их функционирования сформулировать основные направления и пути решения по их совершенствованию.

Выявленные недостатки рассмотренных теоретических методов и практических реализаций противодействия угрозам безопасности информации позволяют сделать вывод о целесообразности совместного использования реконфигурирования сетевых параметров и ложных компонентов ИС.

Применение методов реконфигурирования сетевых параметров к эмулируемым ложным компонентам позволит уменьшить вероятность их компрометации. При этом, переназначение высвобождаемые после реконфигурации ИС сетевые параметры целесообразно перераспределять между ложными компонентами, что исключит нахождение в информационном пространстве, предоставляемом СР, явно незадействованных в информационном обмене узлов ИС. Моделирование процесса функционирования локального сегмента ИС с эмуляцией ложных компонентов и реконфигурированием сетевых параметров ее компонентов в условиях воздействия СР позволит определить релевантные временные интервалы смены сетевых параметров.

Предложенные варианты технических решений позволят устранить выявленные недостатки рассмотренных технологий противодействия СР и повысить результативность защиты ИС.

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. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н. Е. Жуковского : Сборник научных статей VIII Международной научно-практической конференции «Научные чтения имени профессора Н.Е. Жуковского», Краснодар, 20-21 декабря 2017 года / КВВАУЛ им. Героя Советского Союза А. К. Серова. – Краснодар : Общество с ограниченной ответственностью «Издательский Дом – Юг», 2018. – С. 47-52.

4. Соколовский, С. П. Модель конфликта в информационной сфере / С. П. Соколовский, С. Р. Шарифуллин, Е. С. Маленков // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-ой годовщине полета Ю. А. Гагарина в космос : Сборник научных статей, Краснодар, 12-13 апреля 2018 года / КВВАУЛ им. А. К. Серова. – Краснодар: Общество с ограниченной ответственностью «Издательский Дом – Юг», 2018. – С. 299-304.

5. Соколовский, С. П. Моделирование способа обфускации идентификаторов сетевых устройств в интересах минимизации компрометирующих признаков средств проактивной защиты вычислительных сетей / С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2018. – № 3. – С. 239-248.

6. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения : Материалы XXIII Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева. В 2-х частях, Красноярск, 11-15 ноября 2019 года / Под общей редакцией Ю. Ю. Логинова. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», 2019. – С. 447-448.

7. Патент № 2649789 C1 Российская Федерация, МПК H04L 12/801, H04L 29/06, H04L 9/32. Способ защиты вычислительных сетей : № 2017125677 : заявл. 17.07.2017 : опубл. 04.04.2018 / Р. В. Максимов, Д. Н. Орехов, И. С. Проскуряков, С. П. Соколовский ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко» Министерства обороны Российской Федерации.

8. Патент № 2696330 C1 Российская Федерация, МПК G06F 21/50, G06F 21/60, H04L 9/00. Способ защиты вычислительных сетей : № 2018128075 : заявл. 31.07.2018 : опубл. 01.08.2019 / В. В. Барабанов, С. П. Соколовский, Р. В. Максимов [и др.] ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко» Министерство обороны Российской Федерации.

9. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов, С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Технические и технологические системы : Материалы девятой Международной научной конференции «ТТС-17», Краснодар, 22-24 ноября 2017 года / Кубанский государственный технологический университет, Краснодарское высшее военное авиационное училище летчиков имени А. К. Серова; под общей редакцией Б. Х. Гайтова. – Краснодар: Общество с ограниченной ответственностью «Издательский Дом – Юг», 2017. – С. 117-121.