Методика управления ресурсами маскираторов информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения

Н.Ю. Лыков

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Аннотация: При применении маскираторов информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения (ИН РИ ИКС ВН) возникает необходимость обоснованного выбора их характеристик. Методика управления ресурсами маскираторов ИН РИ ИКС ВН относится к обеспечению безопасности ИН РИ ИКС ВН, и применяется для достижения требуемой нарицательной мощности маскиратора ИН, этого достигают обоснованием выбора количества ИН и скорости изменения *IP*-адресов при вариации средней скорости генерации корреспондентом информационных пакетов сообщений.
Ключевые слова: информационная технология, распределенная интегрированная инфокоммуникационная система, маскирование информационных направлений, угроза функционирования, информационный обмен.

Для защищенного информационного взаимодействия сегментов распределенных интегрированных инфокоммуникационных систем ведомственного назначения (РИ ИКС ВН) используются технологии *VPN*. Учитывая тот факт, что передаваемая в *VPN* информация надежно защищена с криптографической точки зрения, а взаимодействие осуществляется только с доверенными абонентами, наиболее эффективными являются воздействия, направленные на срыв процесса передачи данных. Нарушитель имеет возможность изучить и реконструировать функционально-логическую структуру (ФЛС) РИ ИКС ВН, а также интенсивность связей с высокой степенью подобия реальной РИ ИКС ВН. Обладая такой информацией, он способен осуществить подавление [1,2] критически важных узлов системы.

Большинство существующих методов и систем обнаружения *DoS*-атак позволяет эффективно распознавать и бороться с атаками сетевого и транспортного уровня, но они малоэффективны для обнаружения низкоинтенсивных *DoS*-атак, а также атак прикладного уровня,

направленных на конкретные сетевые сервисы и службы. Отличить трафик, генерируемый в ходе данных атак, от легального прикладного трафика достаточно сложно, что делает затруднительным применение сигнатурного метода обнаружения атак. Кроме того, низкоинтенсивные *DoS*-атаки [2] практически не приводят к образованию статистических аномалий. Таким образом, для обеспечения безопасного функционирования РИ ИКС ВН требуется реализация способа защиты от анализа и подавления, способного эффективно противодействовать как низкоинтенсивным, так и на сегодняшний день неизвестным типам атак.

Для решения этой задачи и противодействия возможным деструктивным воздействиям со стороны нарушителя было разработано программное обеспечение (ПО) – комплекс маскирования информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения (маскиратор) способное решать задачу обеспечения защищенного от исследования функционирования ИКС ВН путем:

ослабления или нейтрализации деструктивных воздействий на ИКС ВН со стороны нарушителя (в частности атак типа «отказ в обслуживании»);

поддержания нарушителя в полном или частичном неведении путем лишения его необходимой информации, или затруднения сбора и анализа информации;

формирования ложных стереотипов относительно информационных потоков ИКС ВН, составе элементов ИКС ВН, функционально-логической структуре ИКС ВН и алгоритмах ее функционирования.

Маскиратор производит расширение адресного пространства [3] и создает ложные информационные направления, за счет введения избыточности – изменения сетевого адреса (*IP*-адреса) выходного интерфейса на набор адресов из пула. Формируя *IP*-пакет на канале связи

маскираторы добавляют в поле заголовка *IP*-пакета адрес отправителя адрес своего исходящего интерфейса, а в поле адрес получателя адрес исходящего интерфейса соседа.

Методика управления ресурсами маскираторов ИН РИ ИКС ВН относится к области инфокоммуникаций, а именно к обеспечению безопасности информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения (ИН РИ ИКС ВН).

Назначение методики

При увеличении интенсивности конструктивного трафика, генерируемого корреспондентами, могут возникнуть две задачи:

увеличения частоты вариации *IP*-адресов корреспондентов для сохранения результативности маскирования и защиты от программного подавления (*DOS*/*DDOS*-атак);

увеличения количества (объема) маскирующего трафика для сохранения пропорциональности [4] конструктивного и маскирующего трафика, чем достигают правдоподобность маскирования.

Целью методики является достижение требуемой нарицательной мощности маскиратора ИН, чего достигают обоснованием выбора количества ИН и скорости изменения *IP*-адресов при вариации средней скорости генерации корреспондентом информационных пакетов сообщений.

Физическая (содержательная) постановка задачи

ИКС (сети связи общего пользования (ССОП), включающие транзитные узлы и линии связи), осуществляющие маршрутизацию и транзит трафика, и сетевые информационные объекты (корреспонденты), выполняющие задачу маскирования вариацией *IP*-адресов и маршрутизацией трафика от источника (то есть по предопределенному маршруту), имеют объективные ограничения в вычислительной мощности и пропускной

способности. Этот предел задают выделением некоего программно-аппаратного и (или) временного ресурса (то есть «вычислительной мощности») каждому ИН – конструктивному или маскирующему.

Необходимо выбрать скорость изменения *IP*-адресов имеющихся ИН, а также количество дополнительных ИН так, чтобы достигнуть требуемой нарицательной мощности маскиратора ИН, а суммарные затраты на увеличение ресурса (нарицательной мощности) маскиратора ИН были наименьшими возможными.

Очевидно, что в общем случае принципы синтеза средств защиты должны быть ориентированы на худший для защиты случай, т. е. обладать повышенной устойчивостью к нарушениям адекватности между априорной моделью и реальной ситуацией. Одно из важнейших направлений в реализации этого подхода – применение принципа минимакса.

Конкретные предельные значения нарицательной мощности маскиратора ИН зависят от производительности специализированных ЭВМ, на которых реализуют маскиратор ИН. Распределение дополнительных *IP*-адресов между маскираторами каждого ИН может быть непропорциональным, что также связано с возможной разницей нарицательной мощности между двумя СИО в рамках одного ИН.

Таки образом для каждого предполагаемого маскиратора ИН в каждой точке доступа к ИКС и каждого варианта нового (виртуального) ИН или увеличения производительности существующего конструктивного ИН необходимо решить ресурсную задачу, отвечающую на следующие вопросы:

на какую величину требуется увеличить частоту вариации *IP*-адресов корреспондентов;

сколько дополнительных ИН требуется организовать для защиты ИН между маскираторами (сетевыми информационными объектами).

Исходные данные

Пусть: x_j – нарицательная мощность j-го ИН ($j=\overline{1,N}$) маскиратора, $x_j = 1 \cdot P \cdot v_j$; B – суммарная (требуемая) нарицательная мощность всех N ИН маскиратора, $B = N \cdot P \cdot v$; D_j, d_j – соответственно наибольшая и наименьшая нарицательная мощность, которую может иметь j-е ИН маскиратора.

Φ_j (x_j) – итоговые расчетные затраты на j-м ИН маскиратора. По аналогии с [5] положим, что они равны сумме себестоимости *IP*-адресов $C_j(x_j)$ и произведения капиталовложений $K_j(x_j)$ на нормативную эффективность B: $C_j(x_j) + B \cdot K_j(x_j)$.

Задача состоит в том, чтобы найти план увеличения нарицательной мощности каждого ИН $x_1, x_2, \ldots, x_N$, обеспечивающий минимум общих затрат $\Phi_1(x_1) + + \Phi_2(x_2) + \ldots + \Phi_N(x_N)$ при условиях:

$$x_1 + x_2 + \ldots + x_N = B,$$

$$d_1 \le x_1 \le D_1, \ldots, d_N \le x_N \le D_N .$$

Условимся вместо оптимальных нарицательных мощностей x_1, x_2, … , x_N, искать оптимальные приросты мощностей X_1, X_2, … , X_N, по сравнению с наименьшими возможными мощностями ИН $X_j = x_j - d_j$, ($j=\overline{1,N}$), и обозначим

$$\varphi_j(X_j) = \Phi_j(x_j) - \Phi_j(d_j) = \Phi_j(X_j + d_j) - \Phi_j(d_j);$$

$$m_j = D_j - d_j;\ b = B - (d_1 + d_2 + \ldots + d_N);\ j = \overline{1,N},$$

где $\varphi_j(X_j)$ означает расчетные итоговые затраты на j-м ИН на создание дополнительной нарицательной мощности ИН X_j, считая от минимальной мощности d_j, а b – суммарный прирост мощностей на всех N ИН. Получаем следующую задачу математического программирования:

найти вектор (X_1, X_2, … , X_N), минимизирующий функцию $Z = \sum_{j=1}^{N} \varphi_j(X_j)$

при условиях $\sum_{j=1}^{N} X_j = b$, $0 \le X_j \le m_j$, $j = \overline{1, N}$.

Теоретической основой методики является теория оптимального управления и метод динамического программирования.

Показателем в разработанной методике является целевая функция $F(\xi) = \sum_{j=1}^{N} (C_j(x_j) + B \cdot K_j(x_j))$, а критерием – ее минимизация:

$$F(\xi) = \sum_{j=1}^{N} (C_j(x_j) + B \cdot K_j(x_j)) \to \min,$$

где $C_j(x_j)$ – себестоимость j-го *IP*-адреса; $K_j(x_j)$ – капиталовложения; B – нормативная эффективность.

Ограничения: D_j, d_j – верхняя и нижняя границы частоты вариации ДМП (*IP*-адресов) j-го ИН, $d_1 \le x_1 \le D_1, \ldots, d_N \le x_N \le D_N$; Φ_j (x_j) – итоговые расчетные затраты на j-м ИН маскиратора; поступающие от корреспондентов пакеты сообщений нормализованы, т. е. их длина $l = const$.

Для решения задачи воспользуемся методом динамического программирования, так как он наиболее подходит для исследования многошаговых процедур [5-9] вне зависимости от первоначального состояния (и решения). Выбор метода динамического программирования обосновывается как видом целевой функции, так и прагматической ценностью принципа оптимальности Беллмана.

Для достижения цели методики осуществляют следующую последовательность действий

Вводим параметр состояния и функцию состояния. Обозначим через $F_k(\xi)$ минимальные затраты на создание дополнительной нарицательной

мощности ξ только на первых k ИН, т. е. $F_k(\xi) = \min \sum_{j=1}^{k} \varphi(X_j)$, где минимум берется по переменным X_1, X_2, …, X_k, удовлетворяющим условиям $\sum_{j=1}^{k} X_j = \xi$, $0 \le X_j \le m_j$, $j = \overline{1,k}$.

Если на k-ом ИН предполагается создать дополнительную нарицательную мощность X_k, то на предыдущих (k – 1) ИН прирост мощности должен быть равен $\xi - X_k$. Как бы ни было выбрано значение X_k и какие бы затраты $\varphi_k(X_k)$ вследствие этого не возникли на k-ом ИН, необходимо использовать предыдущие (k – 1) ИН так, чтобы затраты на прирост нарицательной мощности $\xi - X_k$ на них были наименьшими возможными, т. е. чтобы они были равны $F_{k-1}(\xi - X_k)$.

Тогда затраты на первых k ИН на создание дополнительной нарицательной мощности ξ будут равны сумме $\varphi_k(X_k) + F_{k-1}(\xi - X_k)$, а минимальные затраты на первых k ИН получим, если выберем значение X_k между нулем и меньшим из значений ξ и m_k так, чтобы эта сумма приняла наименьшее возможное значение. Это приводит к рекуррентному соотношению $F_k(\xi) = \min_{X_k}(\varphi_k(X_k) + F_{k-1}(\xi - X_k))$, где X_k принимает значения $0 \le X_k \le \min(\xi, m_k)$ при $k = 2, 3, \ldots, N$. Если $k = 1$, то $F_1(\xi) = \varphi_1(\xi)$.

Теперь можно найти оптимальное решение – оптимальные приросты нарицательных мощностей и сами нарицательные мощности ИН. Здесь на k-ом шаге ищется минимум по X_k при фиксированном ξ, причем параметр ξ может принимать значения $0 \le \xi \le \min(b, \sum_{j=1}^{k} m_j)$.

Оценка эффективности методики управления ресурсами маскираторов ИН РИ ИКС ВН

Разработанная методика использует в качестве исходных данных детерминированные величины и ряд ограничений, необходимых для обеспечения возможности аналитических расчетов.

Оценить эффективность методики можно как экспериментально, так и с помощью модели. Рассмотрим вариант моделирования процесса функционирования маскиратора ИН без применения методики, с применением методики и при неоптимальном управлении ресурсами маскиратора, а полученные результаты сравним.

В связи с тем, что достоверные статистические сведения об изменении относительного объема информационного обмена корреспондента, в интересах которого функционирует сетевой информационный объект, при низкой средней и высокой интенсивности входящего трафика, ключевым образом зависят от ранга корреспондента, для примера расчета ограничимся учетом общей тенденции изменения трафика, и положим, что при переходе с низкой интенсивности входящего трафика на среднюю, относительный объем трафика увеличивается в пять раз, а затем снижается на 20%.

В качестве программной среды, в которой осуществляется реализация модели, выбрана система имитационного моделирования дискретных объектов *GPSS-PC*. Критерием выбора является то, что эта система специально создавалась в интересах разработки имитационных моделей, приспособлена для исследования систем массового обслуживания и имеет встроенные возможности параллельного выполнения нескольких процессов, без которого построение адекватной модели [10] не представляется возможным.

Результаты работы имитационной модели представлены в таблице 1.

Таблица № 1

Математические ожидания количества обслуженных маскиратором пакетов сообщений

Методы управления ресурсами маскиратора	Интенсивность	Суммарный поток, %	Поток 1, %	Поток 2, %	Поток 3, %
Без управления ресурсами маскиратора	Низкая	94,82	93,78	96,22	94,50
	Средняя	24,54	25,22	24,56	22,82
	Высокая	67,22	68,22	74,18	59,30
С применением методики	Низкая	97,26	97,50	96,88	97,44
	Средняя	95,24	93,68	95,84	96,82
	Высокая	96,36	95,22	96,74	97,10
При неоптимальном управлении ресурсами маскиратора					
$\lambda_1+\lambda_2$, λ_3	Низкая	95,28	94,56	93,88	97,40
	Средняя	70,24	68,22	69,30	96,82
	Высокая	82,20	74,16	75,44	96,98
$\lambda_1+\lambda_3$, λ_2	Низкая	94,18	92,52	96,80	93,24
	Средняя	66,24	64,48	95,84	67,66
	Высокая	78,62	68,26	97,18	70,42
$\lambda_2+\lambda_3$, λ_1	Низкая	94,40	97,20	92,78	93,24
	Средняя	61,42	93,68	62,22	63,88
	Высокая	76,68	94,14	66,62	69,28

На основании полученных результатов можно сделать вывод о том, что организация защиты с применением методики позволяет наиболее эффективно маскировать ИН за счет обслуживания и диспетчеризации каждого поступившего пакета сообщений.

Разработанная имитационная модель позволяет проверять адекватность математической модели управления ресурсами маскиратора ИН для верифицированного построения маскираторов с заданными параметрами и свойствами с учетом особенностей реализации аппаратной части и программной среды. Предусмотрены широкие возможности изменения логики функционирования одного процесса без корректировки остальных.

Литература

1. Давыдов А.Е., Максимов Р.В., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. М.: ОАО «Воентелеком», 2015. 520 с.

2. Куринных Д.Ю., Айдинян А.Р., Цветкова О.Л. Подход к кластеризации угроз информационной безопасности предприятий // Инженерный вестник Дона, 2018, №1 URL: ivdon.ru/magazine/archive/n1y2018/4803.

3. Искольный Б.Б., Максимов Р.В., Шарифуллин С.Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности, 2017, № 5 (24). С. 72-82. DOI: 10.21681/2311-3456-2017-5-72-82.

4. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation “Secure Information Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. pp. 83-87.

5. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding computer network proactive security tools unmasking features // Selected Papers of the VIII All-Russian Conference with International Participation “Secure In-formation Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. pp. 88-92.

6. Способ сравнительной оценки структур сетей связи: пат. 2626099 Рос. Федерация, МПК G06F / Максимов Р.В., Искольный Б.Б.., Лазарев А.А., Лыков Н.Ю., Хорев Г.А., Шарифуллин С.Р.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2016145568; заявл. 21.11.2016; опубл. 21.07.2017, Бюл. № 21. 19 с.

7. Способ маскирования структуры сети связи: пат. 2622842 Рос. Федерация, МПК G06F / Максимов Р.В., Голуб Б.В., Горячая А.В.,

Кожевников Д.А., Лыков Н.Ю., Тихонов С.С.; заявитель и патентообладатель Военная академия связи (RU). – № 2016119915; заявл. 23.05.2016; опубл. 20.06.2017, Бюл. № 17. 21 с.

8. Способ маскирования структуры сети связи: пат. 2656839 Рос. Федерация, МПК G06F / заявитель и патентообладатель Краснодарское высшее военное училище (RU). Дыбко Л.К., Иванов И.И., Лыков Н.Ю., Максимов Р.В., Проскуряков И.С., Хорев Г.А., Шарифуллин С.Р. – № 2017114782; заявл. 26.04.2017; опубл. 06.06.2018, Бюл. № 16. 27 с.

9. Способ маскирования структуры сети связи: пат. 2645292 Рос. Федерация, МПК H04L / Голуб Б.В., Краснов В.А., Лыков Н.Ю., Максимов Р.В.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2016124953; заявл. 21.06.2016; опубл. 19.02.2018, Бюл. № 5. 29 с.

10. Боргоякова Т.Г., Лозицкая Е.В. Системный анализ и математическое моделирование // Инженерный вестник Дона, 2018, №1 URL: ivdon.ru/magazine/archive/n1y2018/4763.

References

1. Davy`dov A.E., Maksimov R.V., Saviczkij O.K. Zashhita i bezopasnost` vedomstvenny`x integrirovanny`x infokommunikacionny`x sistem [The protection and security of departmental integrated information communication systems]. M.: OAO «Voentelekom», 2015. 520 p.

2. Kurinnykh D.Yu., Aydinyan A.R., Tsvetkova O.L. Inženernyj vestnik Dona (Rus), 2018, №1. URL: ivdon.ru/ru/magazine/archive/n1y2018/4803.

3. Iskol`ny`j B.B., Maksimov R.V., Sharifullin S.R. Voprosy` kiberbezopasnosti. 2017. № 5 (24). pp. 72-82. DOI: 10.21681/2311-3456-2017-5-72-82.

4. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems Selected Papers of the VIII All-Russian Conference with International Participation “Secure Information Technologies”

(BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. pp. 83-87.

5. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding computer network proactive security tools unmasking features Selected Papers of the VIII All-Russian Conference with International Participation “Secure In-formation Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. pp. 88-92.

6. Sposob sravnitel`noj ocenki struktur setej svyazi [Method of comparative evaluation of communication network structures]: pat. 2626099 Ros. Federaciya, MPK G06F Maksimov R.V., Iskol`ny`j B.B.., Lazarev A.A., Ly`kov N.Yu., Xorev G.A., Sharifullin S.R.; zayavitel` i patentoobladatel` Krasnodarskoe vy`sshee voennoe uchilishhe (RU). № 2016145568; zayavl. 21.11.2016; opubl. 21.07.2017, Byul. № 21. 19 p.

7. Sposob maskirovaniya struktury` seti svyazi [A method of masking a structure of a communication network]: pat. 2622842 Ros. Federaciya, MPK G06F Maksimov R.V., Golub B.V., Goryachaya A.V., Kozhevnikov D.A., Ly`kov N.Yu., Tixonov S.S.; zayavitel` i patentoobladatel` Voennaya akademiya svyazi (RU). № 2016119915; zayavl. 23.05.2016; opubl. 20.06.2017, Byul. № 17. 21 p.

8. Sposob maskirovaniya struktury` seti svyazi [A method of masking a structure of a communication network]: pat. 2656839 Ros. Federaciya, MPK G06F zayavitel` i patentoobladatel` Krasnodarskoe vy`sshee voennoe uchilishhe (RU). Dy`bko L.K., Ivanov I.I., Ly`kov N.Yu., Maksimov R.V., Proskuryakov I.S., Xorev G.A., Sharifullin S.R. № 2017114782; zayavl. 26.04.2017; opubl. 06.06.2018, Byul. № 16. 27 p.

9. Sposob maskirovaniya struktury` seti svyazi [A method of masking a structure of a communication network]: pat. 2645292 Ros. Federaciya, MPK H04L Golub B.V., Krasnov V.A., Ly`kov N.Yu., Maksimov R.V.; zayavitel` i

patentoobladatel` Krasnodarskoe vy`sshee voennoe uchilishhe (RU). № 2016124953; zayavl. 21.06.2016; opubl. 19.02.2018, Byul. № 5. 29 p.

10. Borgoyakova T.G., Lozitskaya E.V. Inženernyj vestnik Dona (Rus), 2018, №1. URL: ivdon.ru/magazine/archive/n1y2018/4763.