СПИСОК ЛИТЕРАТУРЫ:

1. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций: Учебное пособие. М.: МИФИ, 2008. — 180 с.
2. ГОСТ Р МЭК 61508-4-2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения».
3. *Rubino G., Tuffin B.* Rare Event Simulation Using Monte Carlo Methods. John Willey & Sons Ltd., 2009. — 271 p.
4. *Durairaj G., Koren I. and Krishna C.M.* Importance Sampling to Evaluate Real-Time System Reliability: A Case Study // Simulation. Vol. 76. № 3. March 2001. P. 172–183.

А. А. Тихомиров, А. И. Труфанов, В. Н. Дмитриенко, А. Россодивита, Е. В. Шубников

КЛАССИФИКАЦИЯ АТАК В ИМИТАЦИОННЫХ ИССЛЕДОВАНИЯХ УЯЗВИМОСТИ КОМПЛЕКСНЫХ СЕТЕЙ

Большинство социальных, биологических и технологических сетей демонстрируют свои существенные нетривиальные топологические особенности, со связями между их элементами, которые невозможно определить однозначно как регулярные или случайные. Такие особенности включают в себя тяжелые хвосты распределений связующего, высокие значения коэффициента кластеризации, ассортативность и диссортативность узлов, общинные и иерархические структуры. Подобные сети называют комплексными сетями (КС) [1–3].

Устойчивость сетевой архитектуры является одной из важнейших проблем построения любых систем. Оценке стойкости комплексных сетей при воздействии дестабилизирующих угроз в рамках имитационных исследований посвящен значительный объем научных публикаций, в том числе [4–15]. Моделирование (генерация) атаки в КС заключается, как правило, в удалении элементов сети в соответствии с заранее заявленными алгоритмами угроз и уязвимостей и последующем анализе изменений сети. Выбор угроз и уязвимостей во многих работах определяется информированностью и предпочтениями авторов, причем зачастую слабо аргументирован или не аргументирован вовсе. При этом характерно, что область комплексных сетей является междисциплинарной площадкой, где базовые позиции занимают физики, математики и специалисты ИТ. Таковые обычно либо не принимают во внимание, либо принимают лишь на уровне интуиции известное определение теории информационной безопасности, утверждающее, что атака — это пара «источник угрозы — уязвимость», реализующая угрозу и приводящая к ущербу. С учетом данного определения в настоящей работе предлагается краткий обзор основных атакующих действий, значимых при моделировании деградации сетей, имеющих комплексную структуру, и следующая классификация атак.

1. Защищенность элемента сети. Как правило, исследователи изначально рассматривали незащищенные, полностью уязвимые элементы, а угрозы в таком случае тождественны атакам [4]. Учет защиты элементов сети наблюдается в работах нынешнего десятилетия [5–6].

2. Атакуемый элемент. Таким элементом может быть как узел, так и связь. Основной мишенью с первых работ по имитации атак на КС является узел [7]. Связь как мишень используется реже [8].

3. Принадлежность к антропогенному источнику угроз. Большинство обзоров КС классифицирует угрозы по единственному признаку и делит на две группы: случайные и преднамеренные (зачастую соответствующие реализации называют «сбоями» и непосредственно «атаками» [9]) .

4. Выбор мишени для антропогенных угроз. При выборе узла (или связи) оценивают его значимость для сети: центральность — степенную, близости, мостовую, собственного значения, организационную (Degree centrality, Closeness centrality, Betweenness, Eigenvalue centrality, Hubs and Authorities) [10]. При этом может учитываться неполнота знаний о сети и ее узлах [11].

5. Очередность угрозы. Имитация угроз реализуется как цепь одновременных событий (параллельные угрозы) или как цепь последовательных. В последнем случае каждая новая атака учитывает повреждения, нанесенные предшествующими атаками [12].

6. Область действия угроз. Обычно такой областью является вся сеть, но для ряда глобальных сетей, таких как Интернет, зачастую разумнее моделировать локальную атаку на отдельный кластер, информация о котором для атакующего в той или иной мере доступна [13].

7. Агрегированность угроз и их порядок. Угрозы могут представлять композиции из различных составляющих п. 1—6. Например, сумма из угроз случайных, действующих на связи, и преднамеренных, нацеленных на узлы с различной центральностью:

а) степенной, с выведением из строя элементов одновременно;

б) мостовой, с уничтожением защищенных узлов последовательно в заданном кластере (см., например: [5]).

8. Мера ущерба. Изменения таких показателей, как диаметр сети, средняя степень узлов, средний коэффициент кластеризации, относительный размер максимального кластера и др., а также вектор таких показателей [14].

9. Мера атаки. Таковой может быть как число атакованных узлов, так и стоимостное выражение атакующих действий [15].

В целом, предлагаемая система классификации атак может быть полезна при анализе стойкости модельных и реальных комплексных сетей.

СПИСОК ЛИТЕРАТУРЫ:

1. *Barabási A.-L., Albert R., Jeong H.* Mean-field theory for scale-free random networks // Physica A. Vol.272. 1999. P. 173—187.
2. *Watts, Duncan J.; Strogatz, Steven H.* Collective dynamics of "small-world" networks // Nature 393 (6684). 1998. P. 440—442.
3. *Евин И. А.* Введение в теорию сложных сетей // Компьютерные исследования и моделирование. 2010. Т. 2. № 2. С. 121—141.
4. *Zhao L., Park K., Lai Y.-C., Ye N.* Tolerance of scale-free networks against attack-induced cascades // Physical Review. Vol. E 72. 2005. URL: http://enpub.fulton.asu.edu/ye/Published_Journal_Papers/Ye_58.pdf.
5. *Галиндо Ф., Дмитриенко Н. В., Карузо А., Россодивита А., Тихомиров А. А., Труфанов А. И., Шубников Е. В.* Моделирование сложных атак на комплексные сети // Безопасность информационных технологий. 2010. № 3. С. 115—121. URL: http://www.pvti.ru/data/file/bit/bit_3_2010_23.pdf.
6. *Xiao S., Xiao G.* On imperfect node protection in complex communication networks // J. Phys. A: Math. Theor. Vol. 44 . 2011. N 5. URL:http://iopscience.iop.org/1751-8121/44/5/055101/pdf/1751-8121_44_5_055101.pdf.
7. *Albert R., Jeong H., Barabasi A.-L.* Error and attack tolerance of complex networks // Nature. 2000. Vol. 406. P. 378—382.
8. *Gong B., Liu J., Huang L., Yang K., Yang L.* Geographical constraints to range-based attacks on links in complex networks // New J. Phys. Vol. 10. 2008. http://iopscience.iop.org/1367-2630/10/1/013030/pdf/1367-2630_10_1_013030.pdf.
9. *Liu Z., Lai Y.-C., Ye N.* Statistical properties and attack tolerance of growing networks with algebraic preferential attachment // Physical Review. Vol. E 66. 2002. N 3. URL: http://enpub.fulton.asu.edu/ye/Published_Journal_Papers/Ye_37.pdf.
10. *Dodds P.* Measures of centrality // Complex Networks. Course 303A. Spring, 2009. Department of Mathematics & Statistics. University of Vermont. URL: http://www.uvm.edu/~pdodds/teaching/courses/2009-01UVM-303/docs/2009-01UVM-303-centrality-handout.pdf.
11. *Xiao S., Xiao G., Cheng T.* Tolerance of local information-based intentional attacks in complex networks // J. Phys. A: Math. Theor. Vol. 43. 2010. N 33. URL:http://m.iopscience.iop.org/1751-8121/43/33/335101/pdf/1751-8121_ 43_33_335101.pdf.
12. *Holme P., Kim B. J., Yoon C. N., Han S. K.* Attack vulnerability of complex networks // Phys Rev E Stat Nonlin Soft Matter Phys. Vol. 65. 2002. N 5. Pt 2. URL: http://arxiv.org/ftp/cond-mat/papers/0202/0202410.pdf
13. *Xiao S., Xiao G.* On Intentional Attacks and Protections in Complex Communication Networks. 2006. URL: http:// arxiv.org/ftp/cs/papers/0609/0609077.pdf.

14. *Najgebauer A., Antkiewicz R., Chmielewski M., Kasprzyk R.* The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution // Journal of Telecommunications and Information Technologies. 2008. N 2. P. 14—20.
15. *Nazarova I. A.* Models and Methods for Solving the Problem of Network Vulnerability // Journal of Computer and Systems Sciences International. 2006. Vol. 45. № 4. P. 567—578.

А. А. Хейн, Б. А. Щукин

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ С ВЕБ-СЕРВИСОМ

В последнее время становится популярной покомпонентная сборка приложений на базе сервис-ориентированной архитектуры (SOA, Service-Oriented Architecture). Каждый такой компонент представляет собой сервис, являющийся модулем системы SOA. Использование данного подхода к программированию ИТ-инфраструктуры позволяет крупному предприятию получить преимущества при дальнейшем развитии.

Для эффективного контроля безопасности SOA-приложений должен быть установлен уровень требований к информационной безопасности (ИБ) составляющих сервисов, в частности веб-сервисов. ИБ — это состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних угроз, а также способность ИТ выполнять предписанные действия без нанесения ущерба субъектам информационных отношений. Так как SOA-приложения становятся все более популярны в бизнес-сообществе, консорциум W3C (World Wide Web Consortium) и OASIS (Organization for the Advancement of Structured Information Standards) прилагают значительные усилия для обеспечения гарантированного уровня их безопасности. Уровень требований устанавливается с помощью сертификатов (стандартов) безопасности. W3C и OASIS рекомендуют стандарты X.509, SPKI, XKMS, SSL/TLS, а также протоколы P3P и SAML в целях повышения информационной безопасности SOA-приложений.

Язык разметки подтверждения безопасности (SAML, Security Assertion Markup Language) (см. [1]) — основанный на языке XML стандарт, разработанный OASIS для обмена данными об аутентификации и авторизации между защищенными доменами, в рамках которых исполняются веб-сервисы. Стандарт SAML не зависит от платформы и состоит из утверждений, протоколов, привязок и профилей. Утверждения — это описания (высказывания) службы идентификации (identity authority) о конечном пользователе. Существуют три вида утверждений: авторизации, аутентификации и атрибута. Каждое в отдельности представляет собой набор общих элементов: предмет, условие и аутентификационное высказывание — и содержит информацию о типе сделанного запроса. Если запрашивается авторизация доступа к приложению, то утверждение SAML сообщает, разрешен ли пользователю вход в систему, и показывает набор его прав доступа. Если запрашивается аутентификация для сетевого ресурса или приложения, утверждение SAML указывает метод аутентификации, а также ее дату и время. В свою очередь, утверждения атрибута позволяют авторизовать пользователей для доступа к определенной информации на основании их статуса. В стандарте SAML хорошо то, что сервер управления идентификацией инкапсулирует, т. е. скрывает, реальные процессы авторизации и аутентификации, что позволяет сочетать решения безопасности от разных производителей. Одна из важных проблем, которую пытается решить SAML, — обеспечение сквозной аутентификации (технология единого входа, Single Sign On) при работе через браузер. Эта технология предполагает использование специального программного