СТАТЬИ XXXIII ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫСШЕЙ ШКОЛЕ»

БИТ

A.D. Afanasyev, A.A. Tikhomirov, A.I. Trufanov

Network Paradigm of Information Security

Keywords: information security, networks, topology.

An issue of topological analysis has been claimed as a key one while creating robust and secure network systems. Some examples of complex network applications in information security domain have been cited.

А.Д. Афанасьев, АА. Тихомиров, А.И. Труфанов

СЕТЕВАЯ ПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Один из основателей отечественной школы информационной безопасности В.А. Герасименко, 20 лет назад определяя задачи защиты информации в тогдашних средствах вычислительной техники и связи и сопутствующих методов обработки данных, указывал на растущий масштаб использования этих средств и методов [1]. Развиваемые современной цивилизацией социальные, экономические и технологические системы отличаются глобальностью не только в смысле территориальной распределенности, глубины и широты охвата процессов обработки информации, но множественности участников (акторов), задействованных в этих процессах. Известные определения понятия информационной безопасности (ИБ) предполагают (см., например, [2]), что современные системы – сложные и многоакторные конструкции, выполняющие свои функции в сложном окружении при наличии широкого спектра угроз и множественности их носителей. В таких системах важны не только элементные, функциональные, но и структурные (топологические) факторы. При этом речь, безусловно, ведется как о безопасности компьютерных сетей, так и социальных, индустриальных и других.

Оказывается, зачастую природа сети отходит на второй план при определении стартовых позиций для построения надежных и безопасных сетевых систем: ключевыми объявляются задачи их топологической уязвимости. Новая эра исследования сетей связана с публикацией А.-Л. Барабаши и Р. Альберт [3], которая положила начало использованию эффективных методов комплексных сетей с понятным языком и большей содержательной нагрузкой, нежели формальная теории графов, что воодушевляет не только ученых, но и практиков. При рассмотрении топологических проблем безопасно-

сти выделяют такие их аспекты, как: а) структурная стойкость и уязвимость, обусловленная сбоями и атаками на комплексные сети [4]; б) каскадные эффекты [5]; с) сетевая перегрузка [6]; д) сетевое распространение угроз [7]. Необходимо отметить, что многие секторы предметной области ИБ удачно интерпретируются в формате развитых сетевых моделей. Известно, что все мероприятия в ИБ направлены на предотвращение или сокращение потенциального ущерба, инициируемого различного рода атаками на информационные системы и обусловленное их последствиями. Прямой ущерб связан с нарушением работоспособности ИКТ-системы, выведением из строя отдельных групп ее элементов, что приводит к невозможности доставки пакетов данных в сети и требует затрат на восстановление. Топологические исследования указывают на необходимость разумного распределения финансовых ресурсов на защиту элементов сети исходя из их значимости (центральности) [8]. Кроме того, анализ топологии позволяет спланировать оптимальную схему восстановительных работ. Косвенно еще больший ущерб от атак на элементы информационной сети может быть связан с отказами во взаимосвязанной технологической сети, ремонт которой бывает весьма дорогостоящим. Так, каскадные сбои взаимосвязанных сетей изучались в [9]. Стволовые сети [10] позволяют измерить и визуализировать свойства конфиденциальности, целостности и доступности в информационной системе. На стволовых сетевых моделях достаточно эффективно прослеживаются возможные каналы утечки и демонстрируются требования в модели управления доступом Bell-Lapadula. Агрегатные сети дают возможность моделирования глобальных информационных процессов, учитывая национальные и региональные особенности [11]. Стратегии операций над узлами и связями имитируют реализуемые в реальных условиях угрозы – случайные и преднамеренные, а также их комбинации [8].

В качестве примера прикладных разработок в рассматриваемой области можно привести НИОКР «Безопасность комплексных сетей», выполненную сотрудниками Университета шт. Аризона по контракту с Исследовательской лабораторией ВВС США, база ВВС Райт-Паттерсон, шт. Огайо. Основная цель этого трехлетнего проекта [12] заключалась в проведении многостороннего исследования комплексных сетей с позиции безопасности и защиты информации с использованием междисциплинарного подхода. В рамках исследования рассматривались следующие тематики: каскадные аварии в комплексных сетях, вызванные атаками, и соответствующие стратегии управления; безопасность комплексных кластерных и градиентных сетей; колебательные процессы, инициированные атаками; безопасность и надежность беспроводных сенсорных сетей; динамика масштабируемых сетей; процессы распространения в комплексных сетях и ряд других.

Можно предполагать, что сетевые подходы с развитием онтологий, моделей, инструментов расчета и визуализации и практик применения окажутся основополагающими в противодействии масштабным многоплановым информационным угрозам РФ: государству, обществу, гражданам. Использование этих перспективных подходов, в комплексе с традиционными, представляется эффективным механизмом в борьбе с распространением враждебных идеологий, экстремизма, плагиата в научно-исследовательской деятельности. Для развития этого механизма потребуются сетевое описание реальных социально экономических, природных, информационных и технологических систем в их взаимосвязи, синтетические модели и исследование на них ключевых сетевых явлений и процессов.

СПИСОК ЛИТЕРАТУРЫ:

1. Герасименко В.А. Защита информации в автоматизированных системах обработки информации М.: Энергоатомиздат. 1994 .
2. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А. Введение в информационную безопасность: Учебное пособие для вузов. 2014.
3. BarabásiA.-L., AlbertR. Emergence of scalingin random networks // Science. 1999. V.286. P. 509–512.
4. Albert R., Jeong H., Barabási A.-L. Attack and error tolerance of complex networks//Nature. 2000. V.406. P. 378–482.
5. Motter A. E., Lai Y.-C. Cascade-based attacks on complex networks// Phys. Rev. 2002. E, V.66(6).P. 065102 (R).
6. Sreenivasan S., Cohen R., Lopez E., Toroczkai Z., Stanley H.E. Structural bottlenecks for communication in networks. //Phys. Rev. E. 2007. V. 75(3). P.036105 (R).
7. Moreno Y., Pastor-Satorras R., Vespignani A. Epidemic outbreaks in complex heterogeneous networks// Euro. Phys. JournalB .2002. V. 26(4). P. 521–529.
8. 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.
9. Buldyrev S.V., Parshani R, Paul G., Stanley H.E., Havlin S. Catastrophic cascade of failures in interdependent networks // Nature. 2010. V. 464 (7291). P. 1025–1028.
10. Тихомиров А.А, Труфанов А.И. Сверхсложные сети: новые модели интерпретации социально-экономических и биосоциальных процессов // Труды Института государства и права РАН. 2011. № 6. С. 162–170.
11. Tikhomirov A., Afanasyev A., Kinash N., Trufanov A., Berestneva O., Rossodivita A., Gnatyuk S., Umerov R. Network Society: Aggregate Topological Models. Communications in Computer and Information Science. 2014. V. 487. P. 415–421.
12. Lai Y.-C.Security of complex networks.FA9550-07-1-0045. 18-02-2010. Arizona State University, Tempe, AZ. AFRL-OSR-VA-TR-2012-0082. 15 p.

REFERENCES:

1. Gerasimenko V.A. Zashchita informacii v avtomatizirovannyh sistemah obrabotki informacii M.: Energoatomizdat. 1994.
2. Malyuk A.A., Gorbatov V.S., Korolev V.I., Fomichev V.M., Durakovskij A.P., Kondrat'eva T.A. Vvedenie v informacionnuyu bezopasnost': Uchebnoe posobie dlya vuzov. 2014.
3. Barabási A.-L., Albert R. Emergence of scaling in random networks // Science. 1999. V.286. P. 509–512.
4. Albert R., Jeong H., Barabási A.-L. Attack and error tolerance of complex networks//Nature. 2000. V.406. P. 378–482.
5. Motter A. E., Lai Y.-C. Cascade-based attacks on complex networks // Phys. Rev. 2002. E, V. 66(6). P. 065102 (R).
6. Sreenivasan S., Cohen R., Lopez E., Toroczkai Z., Stanley H.E. Structural bottlenecks for communication in networks // Phys. Rev. E. 2007. V. 75(3). P.036105 (R).
7. Moreno Y., Pastor-Satorras R., Vespignani A. Epidemic outbreaks in complex heterogeneous networks// Euro. Phys. Journal B.2002. V. 26(4). P. 521–529.
8. Galindo F., Dmitrienko N.V., Caruzo A.,Rossodivita A., Tikhomirov A.A., Trufanov A.I., Shubnikov E.V. Modelirovanie slozhnyh atak na kompleksnye seti // Bezopasnost' informacionnyh tekhnologij. 2010. № 3. P. 115–121.
9. Buldyrev S.V., Parshani R, Paul G., Stanley H.E., Havlin S. Catastrophic cascade of failures in interdependent networks // Nature. 2010. V.464 (7291). P. 1025–1028.
10. Tikhomirov A.A, Trufanov A.I. Sverhslozhnye seti: novye modeli interpretacii social'no-ehkonomicheskih i biosocial'nyh processov // Trudy Instituta gosudarstva i prava RAN. 2011. № 6. P. 162–170.
11. Tikhomirov A., Afanasyev A., Kinash N., Trufanov A., Berestneva O., Rossodivita A., Gnatyuk S., Umerov R. Network Society: Aggregate Topological Models. Communications in Computer and Information Science. 2014. V. 487. P. 415–421.
12. Lai Y.-C. Security of complex networks.FA9550-07-1-0045. 18-02-2010. Arizona State University, Tempe, AZ. AFRL-OSR-VA-TR-2012-0082. 15 p.