Инженерный вестник Дона, №9 (2024)
ivdon.ru/ru/magazine/archive/n9y2024/9463

Теоретико-графовая интерпретация системы защиты информации

А.С. Исмагилова, И.А. Шагапов, И.В. Салов

Уфимский университет науки и технологий, Уфа

Аннотация: Предложена интегрированная система защиты информации, сочетающая динамичность и эффективность, представлена количественная оценка данной системы. Исследование направлено на идентификацию всех потенциальных маршрутов переключений максимальной длины между уникальными состояниями, принимая во внимание потенциальные трудности, которые могут возникнуть при реализации рекомпозиционной системы защиты информации. Основным инструментом для анализа и моделирования различных переходных конфигураций в исследуемой системе предложен аппарат теории графов. В рамках предложенного подхода каждая подсистема включает несколько независимых вариантов или компонентов, причем в любой момент времени функционирует только один из этих вариантов. Важным аспектом является как взаимодействие между подсистемами, так и возможности переключения компонентов внутри одной подсистемы. Для наглядного понимания предложенного подхода приведен пример, который иллюстрирует основные принципы и механизмы работы разработанной системы.

Ключевые слова: система защиты информации, граф состояний, DLP-система, IPS/IDS-система.

Компьютерные технологии применяются не только в контексте осуществления атак со стороны злоумышленников на системы обработки информации, но и для оптимизации времени реакции защитных механизмов на эти атаки, стремясь снизить его до минимально возможного уровня [1]. Человек не всегда способен обеспечить своевременную реакцию на возникающие киберугрозы [2]. В этой связи, разработка алгоритмов, способствующих формированию поведенческих реакций на атаки, а также создание эффективного, масштабируемого и экономически целесообразного подхода к построению систем защиты в рамках информационных систем представляют собой актуальные и неотложные задачи [3-5]. Совершенствование этих систем требует не только теоретических разработок, но и практической реализации решений, направленных на адекватное реагирование на современные вызовы в условиях постоянно эволюционирующих угроз [6].

В [7] предложена система, объединяющая компоненты со свойствами динамичности и эффективности защиты, приведена количественная оценка системы защиты информации. Показано, что добавление новых компонентов или подсистем приводит к увеличению всех возможных состояний системы, усложняя анализ со стороны злоумышленника.

Целью настоящей работы является выявление всех возможных маршрутов переключений максимальной длины между уникальными состояниями, принимая во внимание потенциальные сложности, которые могут возникнуть при реализации рекомпозиционной системы защиты информации. В качестве основного метода для решения поставленной задачи используется аппарат теории графов, который предоставляет необходимые теоретические и практические инструменты для анализа и моделирования различных конфигураций переходов в рассматриваемой системе.

Ясно, что любая система информационной безопасности в рамках информационной системы представляет собой совокупность различных подсистем защиты данных. При применении рекомпозиционного подхода каждая подсистема включает несколько независимых вариантов или компонентов. В любой момент времени функционирует только один из данных вариантов подсистемы. В данном случае значение имеет не только взаимодействие между подсистемами, но и возможные варианты переключения компонентов внутри одной подсистемы.

Для понимания предложенного подхода будет представлено иллюстрирование его применения. Пример позволит наглядно продемонстрировать основные принципы и механизмы работы предложенного авторами подхода.

Рассмотрим систему защиты информации, основанную на использовании одного антивирусного компонента (p=1), двух систем предотвращения утечек данных (DLP) (q=2) и трех систем обнаружения и

предотвращения вторжений (IPS/IDS) (r=3), количество компонент хотя бы одного типа более одного (p·q·r>1).

Модель системы защиты информации можно представить в виде полного трехдольного графа (Рис.1). Вершинами графа являются антивирус − X_1, два самостоятельных типа DLP − Y_1, Y_2, три самостоятельных типа IPS/IDS − Z_1, Z_2, Z_3. Ребра соединяют вершины различных структур − антивирус, DLP, IPS/IDS компонентов.

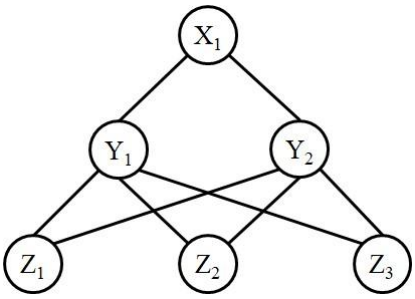

Рис.1. − Граф системы защиты информации

Согласно комбинаторному подходу, количество всех возможных путей, соединяющих различные типы вершин (антивирус, DLP и IPS/IDS компоненты) равно N=p·q·r=6. Каждый путь, соединяющий различные типы вершин, есть состояние системы − S_i, i=1…N. Таким образом, в рассматриваемом примере система может находиться в шести состояниях.

Эти состояния можно наглядно представить в виде полного графа, где каждая вершина S_i (i=1…6) соответствует состоянию системы, а ребра u_j (j=1…15) представляют переходы (переключения) между этими состояниями (Рис.2). Количество ребер в графе равно N·(N-1)/2, где N – количество вершин в графе. Переключения из одного состояния в другое, и наоборот являются различными, поэтому количество всех возможных переключений в рассматриваемом примере N·(N-1) =30.

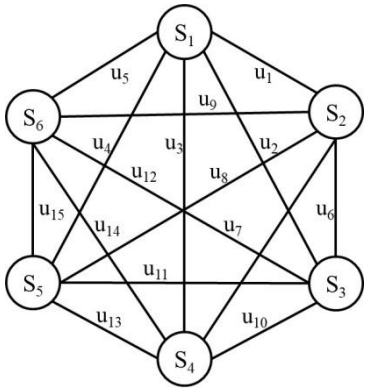

Рис.2. − Граф состояний

Можно рассчитать все возможные маршруты графа состояний, содержащие заданное количество ребер k=1…N. Для этого достаточно возвести матрицу смежности вершин в k-ю степень. Тогда элемент матрицы αpq указывает на количество маршрутов длины k из вершины S_p в вершину S_q (p, q=1…N) [8].

В рассматриваемом примере матрица смежности вершин имеет вид:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Результат возведения в квадрат:

$$\begin{pmatrix} 5 & 4 & 4 & 4 & 4 & 4 \\ 4 & 5 & 4 & 4 & 4 & 4 \\ 4 & 4 & 5 & 4 & 4 & 4 \\ 4 & 4 & 4 & 5 & 4 & 4 \\ 4 & 4 & 4 & 4 & 5 & 4 \\ 4 & 4 & 4 & 4 & 4 & 5 \end{pmatrix}$$

Элемент α_{12}, к примеру, равен 4. Это значит, что существуют четыре маршрута длиной в два ребра из вершины S_1 в S_2. Действительно, u_2u_6, u_3u_7, u_4u_8, u_5u_9. И т.д.

Аналогично, возводя матрицу смежности вершин в шестую степень,

$$\begin{pmatrix} 2605 & 2604 & 2604 & 2604 & 2604 & 2604 \\ 2604 & 2605 & 2604 & 2604 & 2604 & 2604 \\ 2604 & 2604 & 2605 & 2604 & 2604 & 2604 \\ 2604 & 2604 & 2604 & 2605 & 2604 & 2604 \\ 2604 & 2604 & 2604 & 2604 & 2605 & 2604 \\ 2604 & 2604 & 2604 & 2604 & 2604 & 2605 \end{pmatrix}$$

можно видеть что, например, существует 2604 маршрута длиной в шесть ребер из вершины S_1 в S_2.

Таким образом, даже для графов (полных) с небольшим количеством вершин заранее сложно предсказать маршруты переключений из одного состояния в другое состояние без применения методов анализа графов.

Если воспользоваться модифицированной матрицей смежности, в ячейки которой записаны названия ребер, то можно получить не только количество маршрутов, но и сами маршруты. Действительно, имея матрицу смежности:

$$\begin{pmatrix} 0 & u_1 & u_2 & u_3 & u_4 & u_5 \\ u_1 & 0 & u_6 & u_7 & u_8 & u_9 \\ u_2 & u_6 & 0 & u_{10} & u_{11} & u_{12} \\ u_3 & u_7 & u_{10} & 0 & u_{13} & u_{14} \\ u_4 & u_8 & u_{11} & u_{13} & 0 & u_{15} \\ u_5 & u_9 & u_{12} & u_{14} & u_{15} & 0 \end{pmatrix}$$

и возводя ее в квадрат, можно видеть, что элементами матрицы первой строки, к примеру, являются: $u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2$, $u_2u_6 + u_3u_7 + u_4u_8 + u_5u_9$, $u_1u_6 + u_3u_{10} + u_4u_{11} + u_5u_{12}$, $u_1u_7 + u_2u_{10} + u_4u_{13} + u_5u_{14}$, $u_1u_8 + u_2u_{11} + u_3u_{13} + u_5u_1$, $u_1u_9 + u_2u_{12} + u_3u_{14} + u_4u_{15}$. Таким образом, маршруты длины два из вершины

S_1 в S_2 (Рис.3): u_2u_6, u_3u_7, u_4u_8, u_5u_9; из S_1 в S_3: u_1u_6, u_3u_{10}, u_4u_{11}, u_5u_{12}; из S_1 в S_4: u_1u_7, u_2u_{10}, u_4u_{13}, u_5u_{14}; из S_1 в S_5: u_1u_8, u_2u_{11}, u_3u_{13}, u_5u_{15}; из S_1 в S_6: u_1u_9, u_2u_{12}, u_3u_{14}, u_4u_{15}.

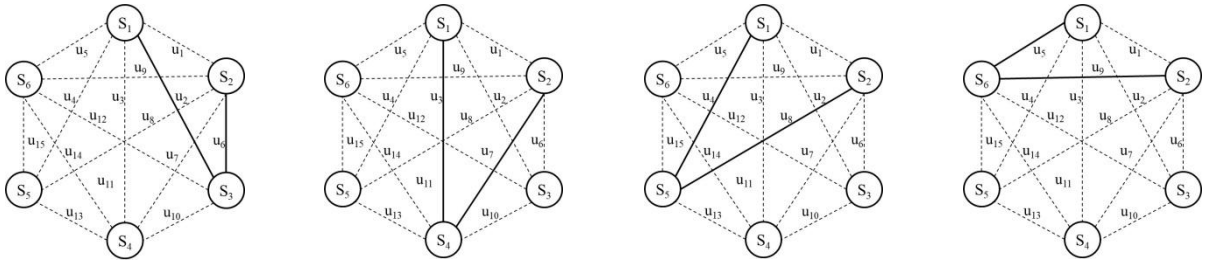

Рис.3. − Все возможные маршруты длины два из вершины S_1 в S_2

Аналогично, возводя модифицированную матрицу смежности вершин в k-ю степень, можно выписать все маршруты длины k=1…N.

С точки зрения защиты информации в контексте графа состояний, определенные ребра, представляющие собой переключения, могут оказаться «нежелательными» и, следовательно, не должны существовать. Примером таких нежелательных переключений является использование различных подходов к расстановке меток конфиденциальности в рамках различных методов мандатного доступа для разграничения доступа. В данном случае может возникнуть ситуация, когда одни и те же поля могут использоваться для разных целей, что приведет к неоптимальному управлению доступом и потенциальным уязвимостям.

Еще одним примером нежелательных переключений может служить возможный конфликт между различными антивирусными продуктами, который может проявляться в невозможности их одновременной работы в условиях переходных процессов. Эти конфликты могут приводить к снижению эффективности защиты информации и созданию дополнительных рисков для системы. Исходя из этого, важным становится оптимальный выбор средств защиты информации (компонентов) [9, 10].

В связи с этим матрица смежности графа состояний будет характеризоваться меньшей однородностью по сравнению с выше представленными. Это обусловлено тем, что наличие «нежелательных» ребер нарушает целостность и согласованность структуры графа, что, в свою очередь, может негативно сказаться на эффективности механизмов защиты информации.

Например, если матрица смежности вершин имеет вид:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

то, возводя ее в шестую степень, получим:

$$\begin{pmatrix} 477 & 545 & 680 & 545 & 615 & 615 \\ 545 & 756 & 875 & 756 & 740 & 740 \\ 680 & 875 & 1047 & 875 & 905 & 905 \\ 545 & 756 & 875 & 756 & 740 & 740 \\ 615 & 740 & 905 & 740 & 804 & 803 \\ 615 & 740 & 905 & 740 & 803 & 804 \end{pmatrix}$$

т.е. из вершины S_1 в S_2, к примеру, существуют 545 маршрутов длиной в шесть ребер и т.д.

В заключение отметим, что имея несколько несложных недорогих подсистем защиты информации, содержащих различные компоненты защиты, возможно построение системы следующего уровня, которая объединяет их свойства и обладает новыми характеристиками. Это позволяет создать более эффективную систему защиты, не требующую отдельных сложных компонентов. Переключение системы между состояниями значительно снижает уязвимость системы перед разведывательными

действиями злоумышленников. Таким образом, интеграция различных компонентов и переключения между состояниями способствуют повышению безопасности информационных систем.

Литература

1. Козлова О.А., Хеззекова К.Т. Интеграция европейских стран в области региональной безопасности на примере НОРДЕФКО // Национальная безопасность / Nota Bene. – 2023. – № 2. – С. 20-35.
2. Cho J., Sharma D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense // IEEE Commun. Surv. Tutor. - 2020. - №22. - pp. 709-745.
3. Бычков С.С., Попов А.М. Методы повышения надежности информационных систем // Решетневские чтения. – 2014. – Т. 2. – С. 28-29.
4. Бандурова Е.Е., Омельченко Т.А. Механизмы обеспечения надежности объектов информационных систем // НБИ технологии. – 2021. – Т. 15, № 4. – С. 5-12.
5. Кочеров Ю.Н., Тихонов Э.Е., Самойленко Д.В. Увеличение надежности схем порогового разделения данных // Инженерный вестник Дона, 2020. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2020/6612.
6. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. – Ульяновск: Печатный двор, 2012. – 296 с.
7. Исмагилова А.С., Шагапов И.А., Салов И.В. Количественная оценка рекомпозиционной системы защиты информации // Инженерный вестник Дона, 2024, №8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9436.
8. Оре О. Теория графов. – М.: Наука, 1980. – 336 с.

9. Прокушев Я.Е., Малий Ю.В. Концептуальная модель выбора средств программно-аппаратной защиты // Computational Nanotechnology. – 2020. – №7 (1). – С. 63-71.

10. Camara A. The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense System // Вопросы безопасности – 2024. – №1. URL: nbpublish.com/library_read_article.php&id=69882.

References

1. Kozlova O.A., Hezzekova K.T. Nacional'naja bezopasnost'. Nota Bene. 2023. № 2. P. 20-35.

2. Cho J., Sharma D.P. IEEE Commun. Surv. Tutor, 2020. №22. pp. 709-745.

3. Bychkov S.S., Popov A.M. Reshetnevskie chtenija, 2014. T. 2. pp. 28-29.

4. Bandurova E.E., Omel'chenko T.A. NBI tehnologii, 2021. T. 15, № 4. pp. 5-12.

5. Kocherov Ju.N., Tihonov Je.E., Samojlenko D.V. Inzhenernyj vestnik Dona, 2020. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2020/6612.

6. Shubinskij I.B. Funkcional'naja nadezhnost' informacionnyh sistem. Metody analiza [Functional reliability of information systems. Analysis methods]. Ul'janovsk: Pechatnyj dvor, 2012. 296 p.

7. Ismagilova A.S., Shagapov I.A., Salov I.V. Inzhenernyj vestnik Dona, 2024, №8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9436.

8. Ore O. Teorija grafov [Graph Theory]. M.: Nauka, 1980. 336 p.

9. Prokushev Ja.E., Malij Ju.V. Computational Nanotechnology. 2020. №7 (1). pp. 63-71.

10. Camara A. Voprosy bezopasnosti, 2024. №1. URL: nbpublish.com/library_read_article.php&id=69882.

Дата поступления: 3.07.2024

Дата публикации: 10.08.2024