Количественная оценка рекомпозиционной системы защиты информации

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

Уфимский университет науки и технологий, Уфа

Аннотация: Данная работа посвящена количественной оценке системы защиты информации. Авторы предлагают построить систему, объединяющую компоненты со свойствами динамичности и эффективности защиты. Предложена система защиты информации, включающая два типа антивирусных компонентов, три системы предотвращения утечек данных и четыре системы обнаружения и предотвращения вторжений. Для наглядности в статье приведена теоретико-графическая интерпретация системы защиты информации. Каждый возможный путь в системе представляет собой ее состояние. Показано, что добавление новых компонентов или подсистем приводит к увеличению всех возможных состояний системы, усложняя анализ со стороны злоумышленника. В рамках данного многокомпонентного подхода каждый элемент системы взаимодействует с другими, что способствует достижению оптимального уровня эффективности в обеспечении защиты информации. Кроме того, предложенный подход характеризуется масштабируемостью, что обеспечивает беспрепятственное интегрирование как отдельных компонентов, так и подсистем в целом.
Ключевые слова: рекомпозиция, система защиты информации, состояние системы, DLP-система, IPS/IDS-система.

В настоящее время мир вступил в эпоху цифровизации, где основная часть информации обрабатывается в информационных системах с применением компьютеров [1]. Компьютерные технологии используются как для проведения атак со стороны злоумышленников на системы обработки информации и системы защиты информационных систем, так и для снижения времени реакции защиты на эти атаки до минимального уровня [2]. Человек неспособен обеспечить правильную и своевременную реакцию на такие атаки, поэтому требуется автоматизация данных процессов [3]. Разработка алгоритмов поведенческих реакций на атаки и создание эффективного, масштабируемого и экономически выгодного подхода к построению систем защиты в информационных системах является актуальной и неотложной задачей [4, 5].

По нашему мнению, требуется изменить подход к построению и функционированию систем защиты информации [6, 7]. Не менее важна

система управления системой защиты информации, например, в [8] предложена динамическая модель управления информационной безопасностью. Анализ показал, что одним из недостатков существующих подходов является их статичность, возможность изучения (подверженность разведке), предсказуемость ответных действий со стороны защиты и слабая масштабируемость.

В работе [9] предложена концептуальная модель рекомпозиционного подхода в защите информации. В работах [10] авторами описан рекомпозиционный подход к построению и функционированию систем защиты информации для автоматизированных систем. Данная работа продолжает исследования авторов. В работе [11] представлена теория функциональной надежности информационных систем как составная часть общей теории надежности, но несколько в другой области.

Атака на систему защиты информации со стороны злоумышленника представляет собой последовательность этапов. Различные модели атаки могут выделять различное количество этапов, однако все они включают этап разведки, который заключается в изучении системы защиты информации. Очевидно, что после проведения тщательной разведки взлом системы защиты становится лишь вопросом времени. Следовательно, усложнение выполнения данного этапа является необходимым.

Любая система защиты информации в информационной системе представляет собой совокупность подсистем защиты информации. При использовании рекомпозиционного подхода каждая подсистема состоит из нескольких самостоятельных вариантов подсистемы, или компонентов. В каждый момент времени активен только один из вариантов подсистемы (компонентов). Важно не только взаимодействие между подсистемами, но и возможные варианты переключения компонентов внутри подсистемы. Переключение компонентов в рамках подсистемы усложняет проведение

этапа разведки. С нашей точки зрения количественная оценка характеристик рассматриваемой модели является первоочередной задачей при анализе эффективности рекомпозиционного подхода для реализации системы защиты информации в информационной системе.

Далее, для ясности понимания, предлагаемый подход будет сопровождаться конкретным примером.

Рассмотрим систему защиты информации, состоящую из двух типов антивирусных компонент (p=2), трех систем предотвращения утечек данных (DLP) (q=3) и четырех систем обнаружения и предотвращения вторжений (IPS/IDS) (r=4), при условии, что количество компонент хотя бы одного типа более одного ($p \cdot q \cdot r > 1$).

Заметим, что каждый из компонентов сам по себе не обязательно является сложным, дорогим и эффективным. Предлагается из них построить систему следующего уровня, у которой будут новые свойства, не присущие ни одной из них по отдельности. Важным свойством будущей системы должно быть отсутствие статичности. Это можно сделать, например, разработкой алгоритма переключения между имеющимися вариантами сборки, в результате система станет динамической. Оно же позволит существенно уменьшить подверженность системы защиты информации изучению (разведке). Таким образом, суть рекомпозиционного подхода заключается в многократной перестройке системы [10].

Систему защиты информации можно интерпретировать в виде полного трехдольного графа (Рис.1). Вершинами графа являются два самостоятельных типа антивирусных систем − X_1, X_2, три самостоятельных типа DLP систем − Y_1, Y_2, Y_3, четыре самостоятельных типа IPS/IDS систем − Z_1, Z_2, Z_3, Z_4. Ребра соединяют вершины различных структур − антивирусной, DLP, IPS/IDS компонентов.

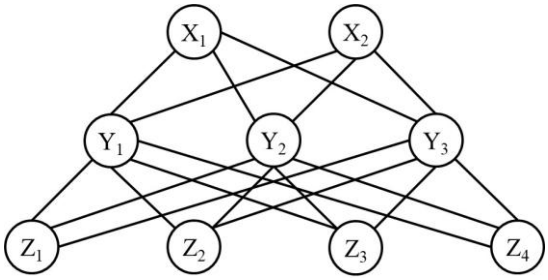

Рис.1. − Теоретико-графическая интерпретация системы защиты информации

Для расчета количества всевозможных путей, соединяющих вершины различных структур трехдольного графа, можно использовать комбинаторный подход. Количество комбинаций, которые могут быть образованы путями, соединяющими различные типы вершин (антивирусная, DLP и IPS/IDS компоненты) равно $N=p \cdot q \cdot r$. В рассматриваемом примере $N=24$.

Каждый возможный путь в рассматриваемой системе представляет собой состояние системы (S_{ijk}, $i=1…p$, $j=1…q$, $k=1…r$), включающее антивирус, DLP и IPS/IDS [12]. В рассматриваемом примере система может находиться в двадцати четырех состояниях. Эти пути отражают все возможные комбинации использования различных состояний.

Эти состояния можно наглядно представить в виде пространственного графа, где каждая вершина соответствует конкретному состоянию, а ребра представляют переходы между этими состояниями (Рис.2). Для более понятной визуальной наглядности пространственного графа на рисунке 2 оставлены лишь некоторые ребра, соединяющие вершины, не изображены все возможные переходы между состояниями. Это улучшит читаемость графического представления. Очевидно, что количество всех возможных переключений из одного состояния в другое равно $N \cdot (N-1)$.

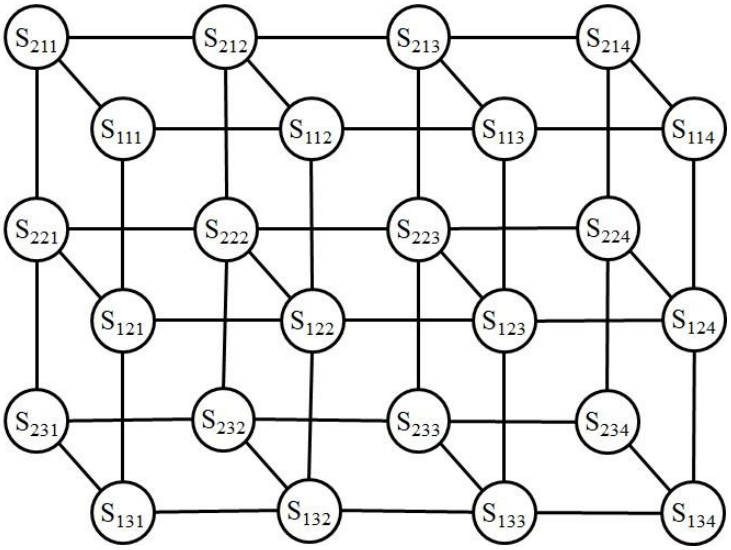

Рис.2. − Теоретико-графическая интерпретация состояний системы защиты информации

На первый взгляд, система сильно избыточна и поэтому экономически не оправдана. Но, есть несколько моментов, которые стоит учесть.

Во-первых, на небольшом количестве (p+q+r) недорогих компонентов построили достаточно большое количество (N=p·q·r) вариантов сборки работающих систем защиты информации, причем по ходу приобрели новое свойство динамичности, которое по-другому вряд ли удастся получить. Даже если их использовать в классическом стационарном варианте, то это уже многократно оправдывает вложения.

Во-вторых, если добавить m новых компонентов (в один из блоков), то на выходе получим гораздо больше. Элементарный подсчет показывает, что при этом дополнительно приобретается m·q·r новых вариантов сборки для нашей системы: N_1=(p+m)·q·r= p·q·r+m·q·r= N+ m·q·r.

Для примера, пусть m=3. Тогда количество всех вариантов равно N_1=(2+3)·3·4= N+ 2·3·3= N+18. Если же эти новые компоненты добавить в разные блоки, например, по одному на каждый блок, то N_2=(p+1)·(q+1)·(r+1)=N+p·q+ p·r+q·r+p+q+r+l. В нашем примере N_2=N+36.

Таким образом, увеличение количества компонентов хотя бы в одной подсистеме структуры защиты информации будет сопровождаться резким увеличением количества всех возможных состояний системы. Кроме того, добавление еще одной подсистемы (блока), например системы доверенной загрузки, приводит к добавлению еще одного слоя состояний (граф будет четырехмерным). Другими словами, добавление новых элементов (компонентов, подсистем и т.д.) приводит к комбинаторному росту возможных конфигураций, что в свою очередь увеличит количество состояний системы защиты информации, и, как следствие, переходов (переключений из одного состояния в другое). Такие изменения значительно усложняют анализ (разведку) системы защиты информации со стороны злоумышленника. Этот вопрос уже относится к качественной оценке предложенной рекомпозиционной системы и будет подробно описан в последующих работах авторов.

Предложенная рекомпозиционная модель представляет собой системный подход к обеспечению безопасности, в котором каждый компонент взаимодействует с другими для достижения максимальной эффективности защиты информационных ресурсов организации. Взаимосвязь между антивирусными системами, DLP системами и IPS/IDS системами создает синергию, обеспечивая эффективную систему защиты информации от современных киберугроз. Более того, предложенная модель обладает свойством масштабируемости, т.е. система имеет возможность бесконфликтного встраивания как компонентов, так и подсистем.

Литература

1. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

2. Каплин М.А., Соколовский С.П., Горбачев А.А. Модель конфигурирования структурно-функциональных характеристик информационных систем ведомственного назначения // Инженерный вестник Дона, 2023, №9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8678.

3. Cho J., Sharma D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense // IEEE Commun. Surv. Tutor. - 2020. - №22. - P. 709-745.

4. Гуревич И.Б., Левин В.И. Надежность телекоммуникационных систем: моделирование и анализ. - Санкт-Петербург: БХВ-Петербург, 2018. - 121 с.

5. Карпов А.П., Махмудов А.А., Шагуфтинский А.Г. Методы повышения надежности телекоммуникационных систем. - Москва: Издательство Телеком, 2015. - 245 с.

6. Шагапов И.А. Подход повышения эффективности защиты информации // Естественные и технические науки. - 2021. - №12 (163). - С. 324-326.

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

8. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Исмагилова А.С. Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия // Инженерный вестник Дона, 2023, №11. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802.

9. Salov I.V., Shagapov I.A., Ismagilova A.S. Conceptual Model of the Efficiency of Information Security System // Imitation Market Modeling in Digital Economy: Game Theoretic Approaches: Conference proceedings. - Moscow: Springer Nature Switzerland, 2022. - P. 221-227.

10. Шагапов И.А., Исмагилова А.С., Салов И.В. Рекомпозиционный подход в защите информации // Международный форум KAZAN DIGITAL

WEEK – 2021: Сборник материалов. - Казань: ГБУ «НЦБЖД», 2021. - С. 275-282.

11. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. - Ульяновск: Печатный двор, 2012. - 296 с.

12. Gupta N., Jindal V, Bedi P. A Survey on Intrusion Detection and Prevention Systems // SN Computer Science. - 2023. - №4 (5). - P. 439.

References

1. Ibragimova Z.M., Batchaeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

2. Kaplin M.A., Sokolovskij S.P., Gorbachev A.A. Inzhenernyj vestnik Dona, 2023, №9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8678.

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

4. Gurevich I.B., Levin V.I. Nadezhnost' telekommunikacionnyh sistem: modelirovanie i analiz [Reliability of Telecommunication Systems: Modeling and Analysis]. Sankt-Peterburg: BHV-Peterburg, 2018. 121 p.

5. Karpov A.P., Mahmudov A.A., Shaguftinskij A.G. Metody povyshenija nadezhnosti telekommunikacionnyh system [Methods for increasing the reliability of telecommunication systems]. Moskva: Izdatel'stvo Telekom, 2015. 245 p.

6. Shagapov I.A. Estestvennye i tehnicheskie nauki. 2021. №12 (163). pp. 324-326.

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

8. Valeev S.S., Kondrat'eva N.V., Guzairov M.B., Ismagilova A.S. Inzhenernyj vestnik Dona, 2023, №11. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802.

9. Salov I.V., Shagapov I.A., Ismagilova A.S. Imitation Market Modeling in Digital Economy: Game Theoretic Approaches: Conference proceedings. Moscow: Springer Nature Switzerland, 2022. pp. 221-227.

10. Shagapov I.A., Ismagilova A.S., Salov I.V. Mezhdunarodnyj forum KAZAN DIGITAL WEEK 2021: Sbornik materialov. Kazan': GBU «NCBZhD», 2021. pp. 275-282.

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

12. Gupta N., Jindal V, Bedi P. A SN Computer Science. 2023. №4 (5). P. 439.

Дата поступления: 22.06.2024

Дата публикации: 3.08.2024