Инженерный вестник Дона, №4 (2022)
ivdon.ru/ru/magazine/archive/n4y2022/7613

Графоаналитическая модель процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Д.М. Крюков

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко

Аннотация: Важнейшей задачей теории и практики обеспечения информационной безопасности является анализ процесса функционирования подсистемы реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак системы защиты информации автоматизированных систем специального назначения в условиях воздействия компьютерных атак злоумышленника на защищаемый информационный ресурс, сервис или сеть, что предполагает моделирование процесса реагирования. Обобщенная модель процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты представлена в виде направленного графа, где вершины соответствуют состояниям подсистемы, а дуги – переходам из состояния в состояние. Описание функционирования подсистемы в пространстве состояний позволяет моделировать процесс реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, оценивая обобщенные показатели времени нахождения подсистемы в различных состояниях и оперативно управлять процессом реагирования путем изменения управляемых параметров модели. Модель учитывает множества видов компьютерных атак и множества стратегий управления средствами защиты информации в процессе ликвидации последствий компьютерных атак, является теоретической основой для разработки методического аппарата анализа, оценки и определения приоритета обработки компьютерных инцидентов, а также исследования вопросов динамического управления подсистемой реагирования на компьютерные инциденты с целью повышения оперативности ее функционирования. Использование предложенной модели позволяет применять как эмпирические значения времени реализации подпроцессов реагирования и противодействия, полученные в результате измерений или моделирования, так и теоретическую базу для моделирования противодействия средств защиты информации компьютерным атакам различных видов.
Ключевые слова: автоматизированная система специального назначения в защищенном исполнении, моделирование, система защиты информации, средства защиты информации, компьютерный инцидент, компьютерная атака, состояние ссистемы.

Система защиты информации автоматизированных информационных систем специального назначения в защищенном исполнении (далее – АС СН) представляет сложную организационно-техническую систему, состоящую из множества разнотипных средств защиты информации и персонала структурных подразделений по информационной безопасности, эксплуатирующих эти средства.

Анализ состава, структуры и задач, решаемых системой защиты информации, а также возможных целей злоумышленника в ходе осуществления компьютерных атак на информационные ресурсы (далее – ИР) АС СН, позволяет сделать вывод о том, что он будет стремиться снизить потребительские характеристики АС СН и нанести ущерб конфиденциальности, целостности и доступности ИР, обрабатываемых такими системами [1-3]. В данных условиях модель функционирования подсистемы ликвидации последствий компьютерных атак системы защиты информации АС СН может быть представлена в виде графоаналитической модели [4,5].

Обобщенная модель процесса реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак на ИР АС СН представлена на рисунке 1 в виде направленного графа и формально описывается выражением (1):

$$G_1 = G_1(S_i; D_1), \tag{1}$$

где: конечное множество вершин графа $S = \{S_i^{\langle B \rangle}\}$, $i = \langle 0,1,2,3,4,5,6,7,8,9 \rangle$, $B = \{N, O, R, CA, A, L\}$, соответствуют состояниям процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты системой защиты информации АИС СН, семантическое описание которых приведено в таблице № 1, и конечное множество дуг графа D_1 – являющихся переходами между состояниями процесса, формализуемых выражением 1.2.

$$\begin{aligned} D_1 = \{&(S_0^{\langle N \rangle}, S_1^{\langle O \rangle}); (S_0^{\langle N \rangle}, S_2^{\langle O \rangle}); (S_0^{\langle N \rangle}, S_3^{\langle O \rangle}); (S_1^{\langle O \rangle}, S_4^{\langle R \rangle}); (S_1^{\langle O \rangle}, S_5^{\langle R \rangle}); \\ &(S_1^{\langle O \rangle}, S_6^{\langle R \rangle}); (S_2^{\langle O \rangle}, S_4^{\langle R \rangle}); (S_2^{\langle O \rangle}, S_5^{\langle R \rangle}); (S_2^{\langle O \rangle}, S_6^{\langle R \rangle}); (S_3^{\langle O \rangle}, S_4^{\langle R \rangle}); (S_3^{\langle O \rangle}, S_5^{\langle R \rangle}); \\ &(S_3^{\langle O \rangle}, S_6^{\langle R \rangle}); (S_4^{\langle R \rangle}, S_0^{\langle N \rangle}); (S_5^{\langle R \rangle}, S_0^{\langle N \rangle}); (S_6^{\langle R \rangle}, S_0^{\langle N \rangle}); (S_4^{\langle R \rangle}, S_7^{CA}); (S_5^{\langle R \rangle}, S_7^{CA}); \\ &(S_6^{\langle R \rangle}, S_7^{CA}); (S_7^{\langle CA \rangle}, S_8^{\langle A \rangle}); (S_8^{\langle A \rangle}, S_9^{\langle L \rangle}); (S_9^{\langle L \rangle}, S_4^{\langle R \rangle}); (S_9^{\langle L \rangle}, S_5^{\langle R \rangle}); (S_9^{\langle L \rangle}, S_6^{\langle R \rangle})\}. \end{aligned} \tag{1.2}$$

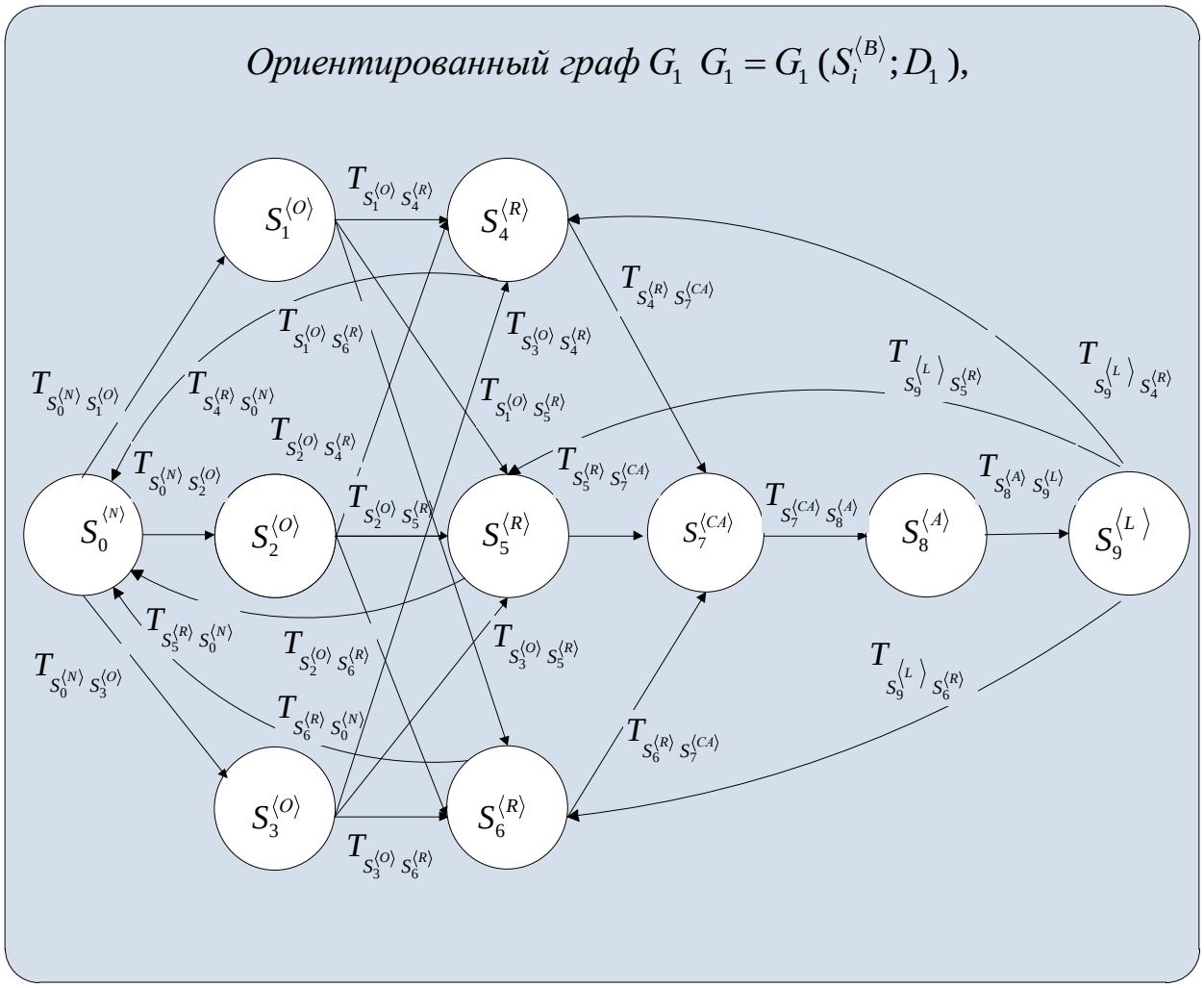

Рис. 1 Модель процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Для каждой дуги определена весовая характеристика – T_i соответствующая времени, за которое осуществляется переход подсистемы реагирования и ликвидации последствий из состояния $S_i^{\langle B\rangle}$ в состояние $S_j^{\langle B\rangle}$ [6].

В начальный момент времени подсистема реагирования и ликвидации последствий находится в нулевом состоянии $S_0^{\langle N\rangle}$. Переходы из состояния в

состояние осуществляются в дискретные моменты времени при осуществлении противником компьютерной атаки [7,8].

Таблица № 1

Семантическое описание состояний

Состояние	Семантическое содержание
$S_0^{\langle N \rangle}$	Начальное состояние
$S_1^{\langle O \rangle}$	Состояние обнаружения компьютерных атак, направленных на нарушение конфиденциальности
$S_2^{\langle O \rangle}$	Состояние обнаружения компьютерных атак, направленных на нарушение целостности
$S_3^{\langle O \rangle}$	Состояние обнаружения компьютерных атак, направленных на нарушение доступности
$S_4^{\langle R \rangle}$	Состояние реагирования средств защиты информации на компьютерные атаки, направленные на нарушение конфиденциальности
$S_5^{\langle R \rangle}$	Состояние реагирования средств защиты информации на компьютерные атаки, направленные на нарушение целостности
$S_6^{\langle R \rangle}$	Состояние реагирования средств защиты информации на компьютерные атаки, направленные на нарушение доступности
$S_7^{\langle CA \rangle}$	Состояние обнаружения компьютерного инцидента
$S_8^{\langle A \rangle}$	Состояние оценки, анализа и определения степени критичности компьютерного инцидента
$S_9^{\langle L \rangle}$	Состояние управления процессом реагирования и ликвидации

Так система из состояния $S_0^{\langle N \rangle}$ перейдет за время $T_{S_0^{\langle N \rangle} S_i^{\langle O \rangle}}$ в состояние $S_i^{\langle O \rangle}$ обнаружения $i-m$ средством защиты информации компьютерной атаки $i-го$ класса. За время $T_{S_i^{\langle O \rangle} S_i^{\langle R \rangle}}$ подсистема перейдет в состояние реагирования $i-го$ средства защиты информации на обнаруженный компьютерный инцидент. По результатам реагирования, подсистема может перейти в начальное состояние $S_0^{\langle N \rangle}$ в случае отражения средствами защиты информации компьютерной атаки, либо перейдет за время $T_{S_i^{\langle R \rangle} S_7^{CA}}$ состояние

компьютерного инцидента $S_7^{\langle CA \rangle}$. Переход из состояния $S_7^{\langle CA \rangle}$ в состояние анализа, оценки и определения критичности компьютерного инцидента должностным лицом группы реагирования на компьютерные инциденты $S_8^{\langle A \rangle}$ характеризуется временем $T_{S_8^{\langle CA \rangle} S_9^{\langle A \rangle}}$, переход из состояния $S_8^{\langle A \rangle}$ характеризуется временем $T_{S_8^{\langle A \rangle} S_9^{\langle L \rangle}}$, затрачиваемым должностным лицом группы реагирования на компьютерные инциденты на анализ, оценку и определение степени критичности компьютерного инцидента, переход из состояния $S_9^{\langle L \rangle}$ в состояния $S_i^{\langle R \rangle}$ реагирования средств защиты информации и ликвидации последствий компьютерных атак, характеризуемые временем $T_{S^{\langle L \rangle} S_i^{\langle R \rangle}}$ затрачиваемым должностным лицом группы реагирования на компьютерные инциденты на формирование, выбор оптимальной стратегии ликвидации последствий компьютерных атак и управления ею, в зависимости от критичности компьютерного инцидента, состояния подсистемы реагирования на компьютерные инциденты [2,8]. Переходы из состояний $S_i^{\langle O \rangle}$ характеризуются весовыми характеристиками соответствующих дуг этих переходов $T_{S_i^{\langle O \rangle} S_i^{\langle R \rangle}}$ в состояния $S_i^{\langle R \rangle}$ и учитывают реализуемые противником комплексные компьютерные атаки, направленные на нарушение конфиденциальности и/или целостности и/или доступности. Далее система переходит из состояния $S_9^{\langle L \rangle}$ за время $T_{S^{\langle L \rangle} S_i^{\langle R \rangle}}$ в состояние $S_i^{\langle R \rangle}$ что означает выработку стратегии и ее реализацию соответствующими средствами.

Рассмотри структурные элементы графа G_1, представленного на рисунке 2:

состояние $S^{T_1} = \left\{ S_1^{\langle O \rangle}, S_2^{\langle O \rangle}, S_3^{\langle O \rangle} \right\}$ формирует устойчивую во времени структуру, зависящую от процессов обнаружения компьютерных атак, где $T_1 = const$;

Каждая дуга обозначает переход системы из состояния в состояние:

состояние $S^{T_2} = \left\{ S_8^{\langle A \rangle}, S_9^{\langle L \rangle} \right\}$ формирует блок состояний, влияющих на изменение временного параметра обработки компьютерного инцидента и ликвидации последствий компьютерных атак;

состояние $S^{T_3} = \left\{ S_4^{\langle R \rangle}, S_5^{\langle R \rangle}, S_6^{\langle R \rangle}, S_0^{\langle N \rangle} \right\}$ формирует блок состояний, являющихся финальными для процесса реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, и время их достижения, напрямую зависит от временных параметров в блоке S^{T_2};

блок $S^{T_0} = S_7^{\langle CA \rangle}$ является истоковым состоянием системы, инициализирующим все последующие блоки состояний в условиях реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак.

Рассмотрим ориентированный граф G_2, представленный на рисунке 2, описываемый выражением (1.3), где $S^{T_0} = S^{\langle CA \rangle}$, а дуги – D_2 формализованно описаны выражением (1.4):

$$G_2 = G_1 (S^{T_0}, S_8^{\langle A \rangle}, S_9^{\langle L \rangle}; D_2), \tag{1.3}$$

$$D_2 = \left\{ (S^{T_0}, S_8^{\langle A \rangle}); (S_8^{\langle A \rangle}, S_9^{\langle L \rangle}); (S_9^{\langle L \rangle}, S^{T_3}) \right\}, \tag{1.4}$$

где весовые характеристики перехода подсистемы из состояния в состояние (1.5-1.7):

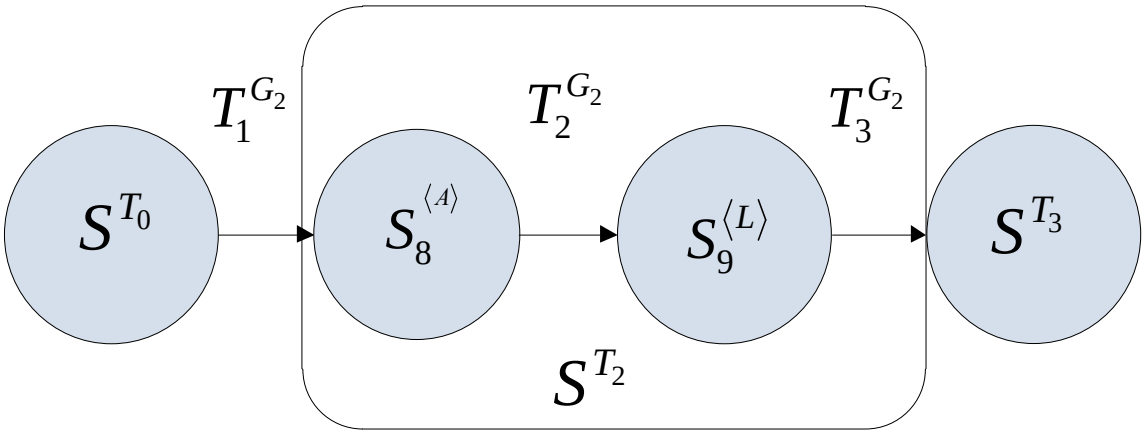

Рис. 2 Ориентированный граф G_2

$$T_1^{G_2} = T(S^{T_0}, S_8^{\langle A\rangle}), \tag{1.5}$$

$$T_2^{G_2} = T(S_8^{\langle A\rangle}, S_9^{\langle L\rangle}), \tag{1.6}$$

$$T_3^{G_2} = T(S_9^{\langle L\rangle}, S^{T_3}). \tag{1.7}$$

Граф G_2 описывает блоковую структуру модели процесса функционирования подсистемы ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты с акцентом на состояния, которые непосредственно формируют изменение времени работы всей подсистемы [9,10].

Таким образом, видна линейная зависимость, выраженная временем пребывания подсистемы в состояниях, формирующих процесс реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак (1.8):

$$T^{S_{ЛПКА}^{РЕЗ}} = T^{S^{T_2}} + T^{S^{T_3}}, \tag{1.8}$$

где управляемыми параметрами модели будут веса дуг $(S_8^{\langle A\rangle}, S_9^{\langle L\rangle}), (S_9^{\langle L\rangle}, S_4^{\langle R\rangle}); (S_9^{\langle L\rangle}, S_5^{\langle R\rangle}); (S_9^{\langle L\rangle}, S_6^{\langle R\rangle})$ – время перехода T_i из

состояния S^{T_2}, напрямую влияющих на переход в состояние S^{T_3}, являющееся финальным.

Вывод: разработанная модель функционирования подсистемы реагирования на компьютерные инциденты в пространстве состояний позволяет моделировать процесс реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, оценивая обобщенные показатели времени нахождения подсистемы в различных состояниях и оперативно управлять процессом реагирования путем изменения управляемых параметров модели. Модель учитывает множества классов компьютерных атак и множества стратегий ликвидации последствий компьютерных атак, является теоретической основой для разработки методического аппарата анализа, оценки и определения приоритета обработки компьютерных инцидентов, а также исследования вопросов динамического управления подсистемой реагирования на компьютерные инциденты с целью повышения оперативности ее функционирования.

Литература

1. Королев И.Д., Петрова О.В., Овчаренко И.О. Моделирование системы защиты многоканальных автоматизированных комплексов // Вестник Российского нового университета, 2019. № 1. С. 3-10.

2. Крюков Д.М., Петрова О.В., Королев И.Д., Колесников В.Л. Способ оценки защищенности автоматизированной информационной системы специального назначения от DDoS-атак на основе теоретико-эмпирического подхода // Инженерный вестник Дона, 2021. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779.

3. Королев И.Д., Петрова О.В., Овчаренко И.О., Леонов Д.В., Модель системы защиты многоканальных автоматизированных комплексов от DDoS–атак с учетом освобождения по мере обработки каналов //

Инженерный вестник Дона, 2019, № 7. URL: ivdon.ru/ru/magazine/archive/N7y2019/6080.

4. Овчинникова Е.С. Графовые модели динамики реализации сетевых атак в автоматизированных системах ОВД // Вестник Дагестанского государственного технического университета. Технические науки. 2021. Том 48, № 1, С. 119-129.

5. Рогозин Е.А., Попов А.Д., Мещерякова Т.В. Проблемы и пути их решения при проектировании систем защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД // Информационные технологии, связь и защита информации МВД России. 2017. Ч. 1. С. 115-118.

6. Березина Л.Ю. Графы и их применение. Учебное пособие / Березина Л.Ю. М: Просвещение, 1979. 143 с.

7. Kresimir S., Hrvoje O., Marin G. The information systems' security level assessment model based on an ontology and evidential reasoning approach // Computers & Security. 2015. P. 100-112.

8. Lan Y., Liu S., Lin L., Ma Y. Effectiveness Evaluation on Cyberspace Security Defense System // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. P. 576-579.

9. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. СПб: Наукоемкие технологии, 2017. 120 с.

10. Lu L., Safavi-Naini R., Hagenbuchner M., Susilo W., Horton J., Yong S.L., Tsoi A.C. Ranking attack graphs with graph neural networks // Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics. LNCS, 2009. pp. 345–359.

References

1. Korolev I.D., Petrova O.V., Ovcharenko I.O. Vestnik Rossiyskogo novogo universiteta. 2019. № 1. pp. 3-10.

2. Kryukov D.M., Petrova O.V., Korolev I.D., Kolesnikov V.L. Inzhenernyj vestnik Dona. 2020. № 7. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779.

3. Korolev I.D., Petrova O.V., Ovcharenko I.O., Leonov D.V. Inzhenernyj vestnik Dona. 2019. № 7. URL: ivdon.ru/ru/magazine/archive/N7y2019/6080.

4. Ovchinnikova E.S. Vestnik Dagestanskogo texnicheskogo universiteta. Tehnicheskie nauki. 2021. T. 48, № 1, pp. 119-129.

5. Rogozin E.A., Popov A.D., Mescheryakova T.V. Informacionnie tehnologii, svyaz i zaschita informacii MVD Rossii. 2017. T. 1. pp. 115-118.

6. Berezina L.U. Grafi i ih primnenie [Graphs and their application]. Uchebnoe posobie. M. Prosveshenie, 1979. pp. 22-30.

7. Kresimir S., Hrvoje O., Marin G. Computers & Security. 2015. pp. 100-112.

8. Lan Y., Liu S., Lin L., Ma Y. Effectiveness Evaluation on Cyberspace Security Defense System. International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. pp. 576-579.

9. Drobotun E.B. Teoreticheskie osnovi postroeniya sistem zaschiti ot kompyuternih atak dlya avtomatizirovannih sistem upravleniya [Theoretical foundations of building protection systems against computer attacks for automated control systems]. SPb.: Naukoemkie tehnologii, 2017. pp. 34-37.

10. Lu L., Safavi-Naini R., Hagenbuchner M., Susilo W., Horton J., Yong S.L., Tsoi A.C. Ranking attack graphs with graph neural networks. Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics. LNCS, 2009. pp. 345–359.