Инженерный вестник Дона, №8 (2023)
ivdon.ru/ru/magazine/archive/n8y2023/8621

Выбор стратегий обеспечения информационной безопасности объекта защиты в условиях неопределенности и противодействия

О.С. Акупиян[1], *А.Г. Коршунов*[2], *В.А. Ломазов*[1,3], *Д.П. Кравченко*[1]

[1]*Белгородский государственный аграрный университет им. В.Я. Горина,*
[2]*Белгородский университет кооперации, экономики и права*
[3]*Белгородский государственный национальный исследовательский университет,*

Аннотация: Работа посвящена проблематике поддержки принятия решений в сфере информационной безопасности. Целью работы является построение (в рамках теоретико-игрового подхода) итерационной процедуры определения смешанной игровой стратегии обеспечения информационной безопасности при неопределенности состояния объекта защиты и противодействии злоумышленника. Использование методологического аппарата имитационного моделирования (наряду с применением метода фиктивного разыгрывания Брауна-Робинсон) обусловлено возможным непуассоновским типом потоков событий, приводящих к изменению состояния объекта защиты, а также сложностью решения стохастических игр с тремя участниками. Применение разработанной процедуры позволяет повысить научную обоснованность управленческих решений по выбору стратегий защиты стохастически-динамических (меняющих свое состояние случайным образом) объектов.
Ключевые слова: информационная безопасность, неопределенность, противодействие, теоретико-игровой подход, имитационное моделирование.

Введение

В настоящее время задача совершенствования методологического аппарата поддержки принятия управленческих решений, направленных на обеспечение защиты информации, приобретает все большее значение, что связано как с ростом угроз информационной безопасности, так и с повышением роли информационного обеспечения при проектировании и реализации сложных организационно-технологических процессов и производств [1].

Одним из эффективных подходов, позволяющих повысить научную обоснованность управленческих решений в сфере информационной безопасности, является использование современных моделей и методов теории стохастических игр, основанных на применении моделей и методов имитационного моделирования [2,3].

Это определило цель настоящей работы, состоящую в построении (в рамках теоретико-игрового подхода) итерационной процедуры определения смешанной игровой стратегии обеспечения информационной безопасности при стохастической неопределенности состояния объекта защиты (ОЗ) и противодействии злоумышленника. При этом отличие рассматриваемой постановки задачи от игры трех лиц [4] состоит в том, что при альтернативности интересов двух основных игроков (злоумышленника и защитника), выбирающих свои стратегии, третий игрок (объект защиты, природа) может с некоторой вероятностью находиться в некотором состоянии.

Материалы и методы

1. Формализация описания объекта защиты, злоумышленника и защитника

Рассмотрим типовую задачу, возникающую при эксплуатации системы информационной безопасности ОЗ.

Будем полагать, что функционирование ОЗ может осуществляться в трех основных режимах:

- S_1 (режим штатного функционирования);
- S_2 (режим проведения регламентных работ);
- S_3 (нерабочий режим).

При этом, в рамках более детального рассмотрения, режимы S_1 и S_2 могут быть разбиты на подрежимы. Переход от одного режима к другому производится под влиянием некоторых потоков распоряжений, связанных с функционированием ОЗ, понимаемых, как последовательности однородных событий, следующих одно за другим через случайные интервалы времени с плотностью вероятности перехода (интенсивностью потока) λ_{ij} ($i,j = 1,2,3$). Графически это может быть представлено в виде размеченного графа состояний (рис.1)

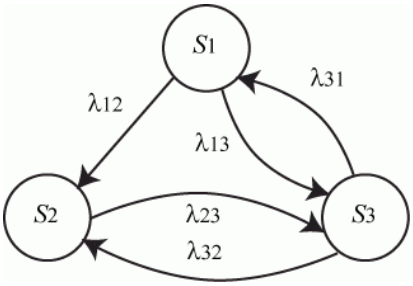

Рис. 1. – Граф состояний объекта защиты

В достаточно широко распространенном частном случае, когда все потоки являются пуассоновскими, процесс будет марковским [5]. Тогда вероятности состояний (режимов функционирования) объекта защиты в момент времени t: $p_i\ (t)$ ($i = 1,2,3$) могут быть определены путём решения системы дифференциальных уравнений Колмогорова, имеющих вид:

$$\frac{dP_i(t)}{dt} = \sum_{j=1}^{3} \lambda_{ji} p_j(t) - p_i(t) \sum_{j=1}^{3} \lambda_{ij}$$

Предельные значения вероятностей состояний объекта (при $\frac{dp_i(t)}{dt} = 0$) могут быть найдены путем решения системы алгебраических уравнений:

$$\sum_{j=1}^{3} \lambda_{ji} p_j(t) - p_i(t) \sum_{j=1}^{3} \lambda_{ij} = 0$$

Однако в случае непуассоновских потоков событий использование соотношений (2) невозможно и остается воспользоваться подходом имитационного моделирования, состоящим в проведении вычислительных экспериментов и статистической обработке их результатов.

Пусть противодействие злоумышленника нормальному функционированию ОЗ угрозой *Threat* из конечной совокупности $THREAT = \{Threat_1, Threat_2, \ldots, Threat_N\}$, различающихся типом *Type*, интенсивностью *Intens* и величиной возможного максимального ущерба *Dam*:

$$Threat = < Type, Intens, Dam >$$

В качестве ответной реакции защитника возможно использование с некоторой относительной частотой стратегий *Strat* из домена $STRAT = \{ Strat_1, Strat_2, \ldots, Strat_K \}$.

Задача состоит в определении рациональных частот стратегий из *STRAT*, которые может быть рекомендованы для противодействия угрозам, входящим в *THREAT*, с учетом нахождения ОЗ в одном из возможных состояний

В дальнейшем для простоты ограничимся рассмотрением только трех возможных стратегий:

- *Maintaining* (сохранение существующей системы информационной безопасности);

- *Modification* (модификация системы информационной безопасности);

- *Reengineering* (замена системы информационной безопасности),

т.е.:

$$Strat \in STRAT = \{Maintaining, Modification, Reengineering\}$$

Отметим, что в рамках повышения детализации рассмотрения первые две стратегии могут быть разбиты на подстратегии.

2. Теоретико-игровая модель выбора стратегии противодействия угрозам при неопределенности состояния объекта защиты

Применение теоретико-игрового подхода для поддержки принятия управленческих решений предполагает необходимость предварительного построения трехмерной матрицы игры *A*, компонентами которой являются значения выигрыша/ущерба a_{knj}, ($k=1,2,\ldots, K$; $n=1,2,\ldots, N$; $j=1,2,\ldots, J$), возникающего при использовании стратегии $Strat_k$ при реализации угрозы $Threat_n$ в то время как ОЗ находится в состоянии S_j . В дальнейшем будем полагать значения a_{knj} известными (полученными в результате

реальных/имитационных экспериментов или экспертного оценивания). В соответствии с общей методологией теории стохастических $\frac{dP_i(t)}{dt} =$ игр искомая цена игры W^* понимается как средний максимальный гарантированный выигрыш (минимальный гарантированный ущерб), получаемый злоумышленником (защитником) при многократном повторении игры с учетом того, что ОЗ может случайным образом менять свое состояние. При этом рациональные смешанные угрозы злоумышленника *Threat** и стратегии $Strat^*$ защитника представляют собой вектора относительных частот применения ими своих чистых угроз/стратегий $Threat_i$ и $Strat_i$, при которых достигается цена игры:

$$Threat^* = (Th_1^*, Th_2^*, \ldots, Th_N^*), \quad \sum_{n=1}^{N} Th_n^* = 1, \quad Th_n^* \geq 0, \quad n = 1,2,\ldots,N$$

$$Strat^* = (St_1^*, St_2^*, \ldots, St_K^*), \quad \sum_{k=1}^{K} St_k^* = 1, \quad St_k^* \geq 0, \quad k = 1,2,\ldots,K$$

$$W^* = \sum_{n=1}^{N}\sum_{k=1}^{K}\sum_{j=1}^{J} Th_n^* St_k^* p_j a_{nkj}$$

Рассматриваемая игра является альтернативной для злоумышленника и защитника (такого вида игры исследовались, например, в [6]), но в то же время (что является принципиальным отличием) имеет черты игры с природой [7], поскольку состояние ОЗ (природы) можно считать решением, принимаемом игроком, который не заинтересован в исходе игры. Сведение рассматриваемой игры к парной альтернативной (матричной) игре переходом к математическим ожиданиям выигрышей/ущербов с последующим решением соответствующей пары двойственных задач линейного программирования является не вполне оправданным, поскольку вероятности состояний ОЗ могут быть неизвестны и (в общем случае) может отсутствовать простая процедура их вычисления. При этом и при решении

классических матричных игр зачастую целесообразно использовать итерационные процедуры, имитирующие многократное повторение игры [8].

Результаты

Основным результатом проведенных исследований является разработанная итерационная процедура выбора стратегии обеспечения информационной безопасности ОЗ (блок-схема приведена на рис.2), основанная на имитационном моделировании потока распоряжений по изменению состояния объекта защиты и применяемом для решения матричных (парных альтернативных игр) подхода фиктивного разыгрывания Брауна-Робинсон. В случае матричных игр сходимость метода Брауна-Робинсон доказана [8]. В рассматриваемом случае применение этого подхода носит эвристический характер, а сходимость предложенной процедуры была проверена вычислительными экспериментами.

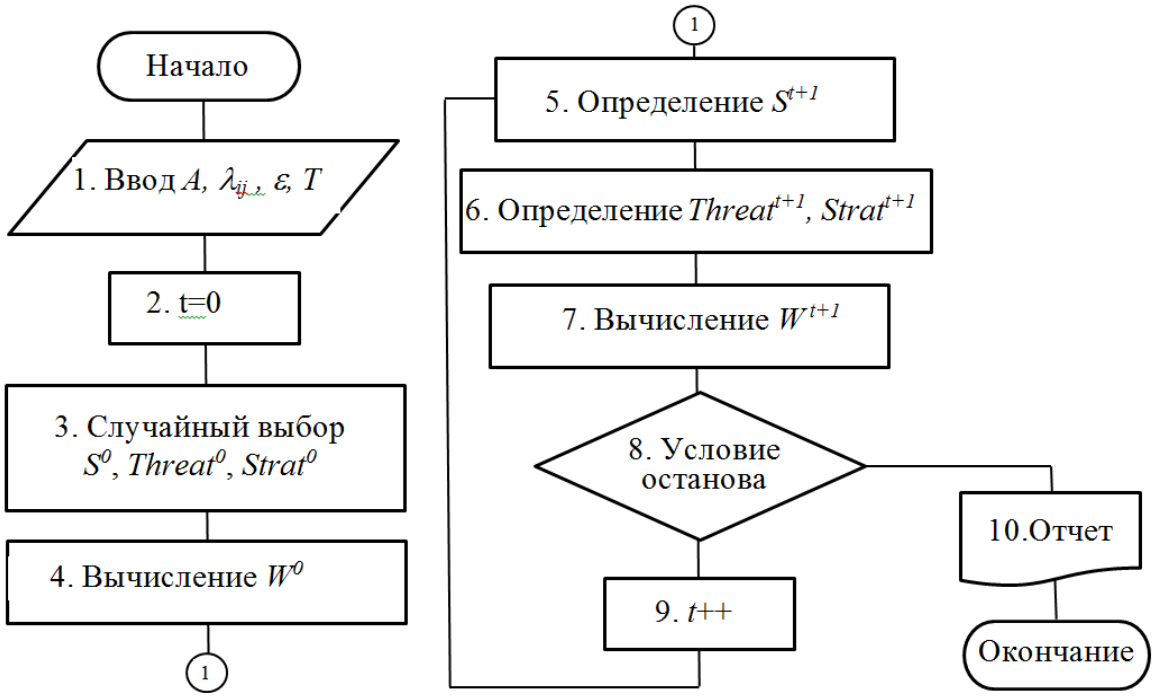

Рис. 2. – Схема процедуры поддержки принятия решений по выбору стратегий

Поясним основные этапы процедуры:

На начальных этапах процедуры (этапы 1-4) осуществляется ввод трехмерной матрицы игры A и интенсивностей потоков распоряжений по изменению состояний ОЗ λ_{ij} $(i,j = 1,2,3)$; задается точность определения цены игры $\varepsilon > 0$ и максимальное число итераций T; устанавливается начальное нулевое значение счетчика итераций (повторений игры) $t=0$ случайным образом выбирается начальное состояние ОЗ S^0, начальная смешанная угроза злоумышленника $Threat^0$, начальная смешанная стратегия защитника $Strat^0$ и вычисляется начальный выигрыш/ущерб W^0 при этом выборе.

На этапе имитационного моделирования (этап 5) генерируется очередное распоряжение и определяется новое состояние ОЗ: S^{t+1}.

На шестом этапе процедуры строится наилучшая (для злоумышленника) угроза при смешанной стратегии защитника $Strat^t$ делается пересчет относительных частот для получения $Threat^{t+1}$, а затем наилучшая (для защитника) стратегия при смешанной угрозе злоумышленника $Threat^{t+1}$ и делается пересчет относительных частот для получения $Strat^{t+1}$.

На седьмом этапе находится выигрыш/ущерб при использовании построенных смешанных стратегий W^{t+1}.

На восьмом этапе осуществляется проверка условия останова процедуры, который осуществляется при достижении:

- либо требуемой точности $abs(W^{t+1} - W^t) < \varepsilon$,
- либо максимального числа итераций $t=T$.

В случае выполнения условия формируется отчет (этап 10), содержащий приближенные значения цены игры, рациональной смешанной угрозы и рациональной смешанной стратегии, а также число выполненных итераций, после чего прекращается работа процедуры. В противном случае,

производится увеличение значения счетчика (этап 9) и выполняется новая итерация (переход на этап 4).

Заключение

Разработанная на основе теоретико-игрового подхода и методологии имитационного моделирования итерационная процедура позволяет построить рациональную смешанную игровую стратегию обеспечения информационной безопасности при неопределенности состояния объекта защиты и противодействии злоумышленника. Применение разработанной процедуры позволяет повысить научную обоснованность решений при управлении защитой стохастически-динамических (меняющих свое состояние случайным образом) объектов. Продолжение исследований может быть связано с построением комплекса мероприятий, направленных на реализацию выбранных решений, для чего могут быть использованы, например, эволюционные процедуры синтеза динамических систем [9,10].

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. Simulation Models & Games XVIII-XI centuries. Interactive Learning Book for Reading / Ed. Kavtaradze D., Leigh E. URL: referencepapers.info/index.html.

3. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем. Омск: Изд-во ОмГУ, 2013. 160 с.

4. Гробер Т.А., Колотиенко М.А. Имитационное моделирование задачи о дуэли трёх лиц // Инженерный вестник Дона. 2017. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4640.

5. Кельберт М. Я., Сухов Ю. М. Марковские цепи как отправная точка теории случайных процессов и их приложения: В 2 ч. Ч. 1. М.: МЦНМО. 2021. 396 с.

6. Лаврентьев А.В., Зязин В.П. О применении методов теории игр для решения задач компьютерной безопасности // Безопасность информационных технологий. 2013. Т. 20, № 3. С. 19-24.

7. Фролова Т.В. Теория игр: игры с природой // Известия Института систем управления СГЭУ. 2020. № 1(21). С. 217-221.

8. Воробьев А.А., Данеев А.В. Стратегическая рефлексия в матричных играх // Известия Самарского научного центра Российской академии наук. 2017. Т. 19, № 6. С. 146-155.

9. Петросов Д. А., Ломазов В.А., Басавин Д.А. Эволюционный синтез систем на основе заданной элементной базы компонентов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2015. № 7(204). С. 116-124.

10. Petrosov D.A., Lomazov V.A., Dobrunova A.I., Matorin S.I., Lomazova V.I. Evolutionary synthesis of large discrete systems with dynamic structure // Biosciences Biotechnology Research Asia. 2015. Vol. 12. No 3. pp. 2971-2981.

References

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

2. Simulation Models & Games XVIII-XI centuries. Interactive Learning Book for Reading / Ed. D. Kavtaradze, E. Leigh. URL: referencepapers.info/index.html.

3. Gucz A.K., Vaxnij T.V. Teoriya igr i zashhita komp`yuterny`x system [Game theory and protection of computer systems]. Omsk: Izd-vo OmGU, 2013. 160 p.

4. Grober T.A., Kolotienko M.A. Inzhenernyj vestnik Dona. 2017. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4640.

5. Kel`bert M. Ya., Suxov Yu. M. Markovskie cepi kak otpravnaya tochka teorii sluchajny`x processov i ix prilozheniya [Markov chains as a starting point for the theory of random processes and their applications]: V 2 ch. Ch. 1. M.: MCzNMO. 2021. 396 p.

6. Lavrent`ev A.V., Zyazin V.P. Bezopasnost` informacionny`x texnologij. 2013. T. 20, № 3. Pp. 19-24.

7. Frolova T.V. Izvestiya Instituta sistem upravleniya SGE`U. 2020. №1 (21). Pp. 217-221.

8. Vorob`ev A.A., Daneev A.V. Izvestiya Samarskogo nauchnogo centra Rossijskoj akademii nauk. 2017. T. 19, № 6. Pp. 146-155.

9. Petrosov D. A., Lomazov V.A., Basavin D.A. Nauchny`e vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: E`konomika. Informatika. 2015. № 7(204). Pp. 116-124.

10. Petrosov D.A., Lomazov V.A., Dobrunova A.I., Matorin S.I., Lomazova V.I. Biosciences Biotechnology Research Asia. 2015. Vol. 12. No 3. Pp. 2971-2981.