Технико-экономическое обоснование выбора оптимальных средств обнаружения атак (вторжений) для нужд центров мониторинга Российской Федерации

М.П. Табункова[1], Л.Л. Оганесян[2]

[1]Краснодарское высшее военное училище, Краснодар
[2]Кубанский государственный технологический университет

Аннотация: Предметом исследования являются технические и экономические характеристики средств обнаружения атак, влияющие на эффективность их применения для системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты критической информационной инфраструктуры Российской Федерации. Представлен анализ подходов к выбору наилучших решений, результат которого лег в основу предлагаемого решения. В статье содержится исследование подходов к решению задачи технико-экономического обоснования выбора, формализованы постановка задачи и математическая модель решения задачи выбора оптимального средства обнаружения атак для реализации соответствующих задач. При этом применяемые методы исследований включают системный анализ, моделирование и методы экспертного оценивания. Цель разработки методики – повышение уровня обоснованности принятия решения о выборе наилучшего из предложенных средств обнаружения атак.
Ключевые слова: средства обнаружения атак, средства обнаружения вторжений, технико-экономическое обоснование, конкурентный анализ, средства защиты информации, система поддержки принятия решений, СОА, система защиты информации, оптимизация, целочисленное линейное программирование.

Введение.

Для формирования выводов о состоянии исследований на предмет проведения конкурентного анализа средств обнаружения атак (вторжений) (далее – СОА) определим ретроспективность исследования – не старше 10 лет, при этом должны быть исследованы труды отечественных и зарубежных авторов.

В тезисах доклада [1] проведена технико-экономическая оценка рыночного потенциала, выполнен обзор программных средств, предназначенных для решения задач выявления сетевых атак, защиты от них в информационно-телекоммуникационных системах с высоким объемом трафика. В указанном труде автором не представлена модель проведения технико-экономического обоснования, представлены только его результаты,

что не позволяет сделать вывод о наборе соответствующих параметров данной модели.

В статье [2] предлагается применение качественного состава характеристик СОА. За основу взяты наборы тестов, с помощью которых оценивается реализация. В качестве таких характеристик выступает набор тестов для оценки реализации критических функций СОА. В статье не приведен механизм выбора наилучшего (единственного) варианта средства, что не решает задачу, сформулированную в теме статьи.

В докладе [3] представлены результаты сравнительного анализа современных программных средств защиты информации от сетевых атак. При этом не учтены функциональные возможности новых средств, появляющихся на внутреннем рынке Российской Федерации СОА.

В материалах статьи [4] рассмотрены вопросы анализа возможностей и особенностей применения программных средств защиты информации от сетевых атак. Заявлено, что целью исследования является повышение обоснованности принятия решений при выборе СОА в интересах обеспечения защиты от деструктивных воздействий на информацию, которая храниться, обрабатывается и передается по каналам сети передачи данных или системы, однако аппарата решения данной задачи в статье не приведено.

Алгоритм программы для ЭВМ [5] решает задачу выбора наиболее подходящего из имеющихся модельного аппарата для обнаружения видов атак с заданными показателями качества обнаружения. Реализована возможность настройки системы под определенные виды атак и условий функционирования целевой инфраструктуры. Обоснование модели решения не представлено, что не позволяет сделать вывод о ее обоснованности.

В статье [6] представлен сравнительный анализ существующих методик и стандартов оценки возможностей систем аудита информационной безопасности. В рассмотренных методиках не учтены требования

регуляторов к СОА, что не позволяет использовать данные материалы для решения задачи выбора оптимального средства с учетом санкционированных требований к организации систем защиты информации для объектов критической информационной инфраструктуры.

В статье [7] обосновываются критерии эффективности СОА. Предлагается смешанная модель выбора признаков, которая потенциально сочетает в себе сильные стороны как фильтра, так и процедуры выбора. В статье описывается подтверждение предлагаемого решения, которое позволяет эффективно подбирать оптимальный набор функций СОА, но не позволяет выявить наиболее оптимальное средство при нескольких альтернативах. Кроме того, при формировании гибридной модели не учтены требования регуляторов к СОА, что предопределяет необходимость доработки данной модели в случае ее применения для решения задачи выбора оптимального средства для объекта критической информационной инфраструктуры.

Исследование [8] сосредоточено на разработке нового алгоритма выбора признаков для сценариев обнаружения вторжений. Формирование механизма увязывания данного алгоритма с решением задачи выбора оптимального СОА выходит за рамки исследования и, соответственно не способствует решению поставленной задачи.

Целью работ [9-11] авторами заявляется оптимизация процесса выбора признаков таким образом, чтобы повысить точность классификатора, что лишь опосредовано может быть использовано при проектировании модели выбора оптимального СОА при проведении конкурентного анализа.

Если у рассматриваемой задачи есть много решений, то естественно выбирать то из них, которое квалифицируется как лучшее, или, как описывается в ряде источников – оптимальное [12, 13]. Из этого следует, что

выбор наилучшего из предложенных СОА сводится к классической задаче оптимизации.

Экспериментально-методическая часть.

Дано: S система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы объекта критической информационной инфраструктуры Российской Федерации; X – множество входных параметров; Y – множество выходных параметров; $y_1,\ldots,y_n$ – оптимизируемые выходные параметры, определяющие эффективность СОА; Z – множество внутренних параметров системы; E – множество параметров среды в условиях информационно-технического воздействия.

Содержательная (вербальная) постановка задачи: разработать методику M обеспечения максимизации выходных параметров $y_1,\ldots,y_n\left(\forall y_i \geq y_i^{mp}, y_i \in Y, i=1..n\right)$, где $y_1^{mp},\ldots,y_n^{mp}$ – значения требуемых показателей качества в диапазоне значений входных параметров X, за счет варьирования значений технических и экономических характеристик Z, при ограничениях на значения параметров среды $E \in E_{доп}$.

Математическая (формальная) постановка задачи.

Исходные данные:

$I = \{i_1,\ldots,i_k\}$ – множество предлагаемых вариантов СОА;

$M = \{m_1,\ldots,m_n\}$ – множество требований к СОА, отраженных в разделах II и III Приказа Федеральной службы безопасности Российской Федерации «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» от 6 мая 2019 года № 196:

$$m_{ij} \in \{0;1\}, i = \overline{1,k},\ j = \overline{1,n}$$

$$m_{ij} = \begin{cases} 1, \\ 0, \end{cases}$$

1 – если *j*-ое требование реализовано в *i*-ом СОА;

0 – если *j*-ое требование не реализовано в *i*-ом СОА;

$P = \{p_1, \ldots, p_h\}$ – множество требований к СОА, отраженных в Методическом документе ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня узла второго класса защиты» (ИТ.СОВ.У2.ПЗ) и в Методическом документе ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня сети второго класса защиты» (ИТ.СОВ.С2.ПЗ):

$$p_{ij} \in \{0;1\}, i = \overline{1,k}, j = \overline{1,h}$$

$$p_{ij} = \begin{cases} 1, \\ 0, \end{cases}$$

1 – если *j*-ое требование реализовано в *i*-ом СОА;

0 – если *j*-ое требование не реализовано в *i*-ом СОА;

$O_i, i = \overline{1,k}$ – коэффициент обнаружения *i*-ым СОА компьютерных атак, имеющих высокую критичность:

$$O_i = \frac{\sum\limits_{y_i \in p} O_{yi}}{\sum\limits_{i=1}^{z} O_y},$$

где p – компьютерные атаки, имеющие высокую критичность и обнаруженные *i*-ым СОА, O_y – компьютерные атаки, имеющие высокую критичность и поданные на вход для тестирования исследуемых СОА;

$l_i, i = \overline{1,k}$ – стабильность работы средства:

$$l_{ij} = \begin{cases} 1, \\ 0, \end{cases}$$

1 – если *i*-ым СОА реализована возможность просмотра логов;

0 – если *i*-ым СОА возможность просмотра логов не реализована;

$c_i, i = \overline{1,k}$ – стоимость i-го СОА;

$t_i, i = \overline{1,k}$ – сроки внедрения i-го СОА в S.

Решение:

Введем булеву переменную $x_i \in \{0;1\}, i = \overline{1,k}$, такую что:

$$x_i = \begin{cases} 1, \\ 0, \end{cases}$$

1 – если i-ое СОА есть в решении;

0 – если i-го СОА нет в решении.

Тогда $X = (x_1, \ldots, x_k)$ – решение в виде вектора булевых переменных, где значение 1 соответствует тому СОА, которое лучше всех удовлетворяет заданным критериям оптимальности.

Используя исходные данные, сформулируем целевую функцию (1) и систему ограничений (2) для поиска решения задачи оптимизации:

$$\sum_{j=1}^{n}\sum_{i=1}^{k} x_i m_{ij} \to \max \tag{1}$$

$$\begin{cases} \max\limits_{j=\overline{1,n}} \sum\limits_{i=1}^{k} x_i m_{ij} \le 1 \\ \max\limits_{j=\overline{1,h}} \sum\limits_{i=1}^{k} x_i p_{ij} \le 1 \\ \sum\limits_{i=1}^{k} c_i x_i \le c \ , c = const \\ \sum\limits_{i=1}^{k} t_i x_i \le t \ , t = const \\ \sum\limits_{i=1}^{k} x_i \le 1 \\ \max\limits_{i=\overline{1,k}} \sum\limits_{i=1}^{k} x_i O_i \le 1 \\ \max\limits_{i=\overline{1,k}} \sum\limits_{i=1}^{k} x_i l_i \le 1 \end{cases} \tag{2}$$

Значения констант устанавливаются экспертным методом и представляют собой предельно допустимые значения стоимости СОА (c_i) и сроках ожидания внедрения i-го СОА (t_i).

Решение задачи – нахождение всех неизвестных компонент вектора – X и выбор того СОА из множества $I = \{i_1, \ldots, i_k\}$, для которого соответствующая компонента вектора x_i равна 1.

Результаты и их обсуждение.

Данная оптимизационная задача сводится к известной задаче целочисленного линейного программирования, и может быть решена различными методами, такими как сечения Гомори, разветвления и другими.

Существуют три основных метода решения задач целочисленной оптимизации: методы отсечения, комбинаторные методы и приближенные методы [14].

Решение задачи методами отсечения осуществляется с учетом каждого нового ограничения, и если ответ при очередной итерации не является целочисленным, то вводится новое ограничение.

Комбинаторные методы позволяют достичь решения с наименьшим количеством ошибок, в отличие от методов отсечения, и достаточно просты, но их применение ограничено решением задач малой размерности.

Затраты времени на реализацию комбинаторных метолов по сравнению с методами отсечения более высоки, при этом их алгоритм функционирования характеризуется более сложной логики и меньшей вероятностью получения ожидаемого и логически предсказуемого результата.

Отмеченная особенность комбинаторных методов и методов отсечения заключается в высокой сложности вычисляемых процедур, что актуализирует необходимость использования приближенных методов. Широкое применение данной группы методов наблюдается при решении

прикладных задач, которые имеют большую размерность и специфические ограничения. Именно в таком виде задач оперативное получение приближенного ответа является приемлемым и достаточным. Кроме этого, достоинством приближенных методов является то, что они предусматривают решение задач с использованием неточных исходных данных.

Недостатком приближенных методов является то, что в случае некорректного ответа при поиске решения, метод не позволяет определить причину такого исхода и внести соответствующие корректировки. Кроме того, невозможно определить, насколько близко к оптимальному полученное этим методом решение.

Учитывая результаты анализа методов решения, их достоинств и недостатков, наиболее обоснованным будет использование метода ветвей и границ для решения оптимизационной задачи. Выбор данного метода связан с возможностью оперативного завершения алгоритма в тот момент, когда получено хотя бы одно допустимое целочисленное решение, даже при том, что оно может быть не оптимальным. Кроме того, при решении линейной задачи указанным методом может быть получено значение, выражающее то, насколько далеко полученное решение от оптимального. Методы ветвей и границ позволяют получить несколько оптимальных решений.

В основе метода ветвей и границ лежит идея последовательного разделения множества допустимых решений на соответствующие подмножества. На каждом шаге реализации метода полученные подмножества подвергаются анализу на предмет наличия в нем оптимального решения. Если рассматривается задача на минимум, то проверка осуществляется путем сравнения нижней оценки значения целевой функции на данном подмножестве с верхней оценкой функционала.

В случае применения верхней оценки на некотором допустимом промежутке решения рекордом считается то, что дает наибольшее значение

оценки. Если значение целевой функции на очередном решении больше рекордного, то происходит смена рекорда. Из этого следует, что подмножество решений проверено и достигнуто условие, при котором не содержится решения лучше рекорда.

Результаты исследования, представленные в статье, могут быть использованы для осуществления технико-экономического обоснования принимаемых решений при выборе СОА для нужд центров мониторинга Российской Федерации. Предложенная методика положена в основу проведения соответствующих исследований для каждого средства системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Литература

1. Малофеев В.А. Технико-экономическое обоснование выбора программных средств обнаружения сетевых атак на телекоммуникационные сети // Материалы XII Санкт-Петербургской межрегиональной конференции Информационная безопасность регионов России (ИБРР-2021). СПб: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 173-175.

2. Половко И.Ю. Разработка требований к составу характеристик для сравнения СОА // Известия ЮФУ. Технические науки. 2013. №12. С. 126-135.

3. Домбровский Я.А., Малофеев В.А., Паращук И.Б. Анализ современных программных средств защиты инфокоммуникаций от сетевых атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Том 1. СПб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 310-314.

4. Паращук И.Б., Малофеев В.А., Морозов И.В. Программные средства защиты телекоммуникаций от сетевых атак, анализ их возможностей и специфики применения // Информационная безопасность регионов России. СПб: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 185-187.

5. Десницкий В.А., Мелешко А.В.Компонент выбора параметров имитационных моделей для решения задач обнаружения атак в реальном времени // URL: elibrary.ru/item.asp?id=47435300 (дата обращения: 17.10.2023).

6. Ефремов А.В., Панамарев Г.Е. Анализ существующих методик оценки средств аудита информационной безопасности // Вестник военного инновационного технополиса «ЭРА». 2021. №4. С. 28-45.

7. Muhammad Hilmi Kamarudin, Carsten Maple, Tim Watson Hybrid feature selection technique for intrusion detection system // International Journal of High Performance Computing and Networking. 2019. №13. pp. 232-240.

8. Herrera-Semenets V., Bustio-Martinez L., Hernandez-Leon R., Berg Jan van den. A multi-measure feature selection algorithm for efficacious intrusion detection // Knowledge-Based Systems. 2021. №227. pp. 215-228.

9. Acharya Neha, Singh Shailendra An IWD-based feature selection method for intrusion detection system // Methodologies and application. Bhopal: Springer-Verlag GmbH, 2018. pp. 407-416.

10. Ndiaye Ndèye Fatma Algorithmes d'optimisation pour la résolution du problème de stockage de conteneurs dans un terminal portuaire. Paris: Laboratoire de Mathématiques Appliquées du Havre Université du Havre, 1973. 244 p.

11. Козырь Н.С., Бирбасова А.В. Аспекты идентификации объектов критической информационной инфраструктуры РФ // Электронный сетевой полиметрический журнал «Научные труды КубГТУ». 2022. №2. С. 163-172.

12. Козырь Н.С. Актуальные вопросы цифровизации социально-экономических систем // Вестник университета. 2023. №7. С. 54-59.

13. Козырь Н.С. Вопросы эвентуальности цифровой трансформации социально-экономических систем // E-management. 2023. №1. С. 51-60.

14. Оганесян Л.Л., Козырь Н.С. Проектное управление в информационной безопасности // Вестник Академии знаний. 2023. №4. С. 207-209.

References

1. Malofeev V.A. Materialy XII Sankt-Peterburgskoj mezhregional'noj konferencii Informacionnaya bezopasnost' regionov Rossii (IBRR-2021). SPb: Regional'naya obshchestvennaya organizatsiya «Sankt-Peterburgskoe Obshchestvo informatiki, vychislitel'noy tekhniki, sistem svyazi i upravleniya», 2021. pp. 173-175.

2. Polovko I.Yu. Izvestiya YUFU. Tekhnicheskie nauki. 2013. №12. pp. 126-135.

3. Dombrovskiy Ya.A., Malofeev V.A., Parashchuk I.B. Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii. Sbornik nauchnyh statej: v 4h tomah. Tom 1. SPb: Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. prof. M.A. Bonch-Bruevicha, 2021. pp. 310-314.

4. Parashchuk I.B., Malofeev V.A., Morozov I.V. Informacionnaya bezopasnost' regionov Rossii. SPb: Regional'naya obshchestvennaya organizatsiya «Sankt-Peterburgskoe Obshchestvo informatiki, vychislitel'noy tekhniki, sistem svyazi i upravleniya», 2021. pp. 185-187.

5. Desnitskiy V.A., Meleshko A.V. Komponent vybora parametrov imitatsionnykh modeley dlya resheniya zadach obnaruzheniya atak v real'nom vremeni. URL: elibrary.ru/item.asp?id=47435300 (date accessed 17.10.2023).

6. Efremov A.V., Panamarev G.E. Vestnik voennogo innovacionnogo tekhnopolisa «ERA». 2021. №4. pp. 28-45.

7. Muhammad Hilmi Kamarudin, Carsten Maple, Tim Watson International Journal of High Performance Computing and Networking. 2019. №13. pp. 232-240.

8. Herrera-Semenets V., Bustio-Martinez L., Hernandez-Leon R., Berg Jan van den Knowledge-Based Systems. 2021. №227. pp. 215-228.

9. Acharya Neha, Singh Shailendra Methodologies and application. Bhopal: Springer-Verlag GmbH. 2018. pp. 407-416.

10. Ndiaye Ndèye Fatma Algorithmes d'optimisation pour la résolution du problème de stockage de conteneurs dans un terminal portuaire. Paris: Laboratoire de Mathématiques Appliquées du Havre Université du Havre, 1973. 244 p.

11. Kozyr' N.S., Birbasova A.V. Elektronnyj setevoj polimetricheskij zhurnal «Nauchnye trudy KubGTU». 2022. №2. pp. 163-172.

12. Kozyr' N.S. Vestnik universiteta. 2023. №7. pp. 54-59.

13. Kozyr' N.S. E-management. 2023. №1. pp. 51-60.

14. Oganesyan L.L., Kozyr' N.S. Vestnik Akademii znanij. 2023. №4. P. 207.