ARTICLE HISTORY: Received: February 04, 2022 Accepted: March 28, 2022 Published: April 04, 2022

УДК 623.61

МЕТОДИКА ФОРМИРОВАНИЯ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА БСТРОМЕНЯЮЩИХСЯ СИТУАЦИЙ ПРИ ОТРАЖЕНИИ КОМПЬЮТЕРНЫХ АТАК И ЛИКВИДАЦИИ ИХ ПОСЛЕДСТВИЙ

Фисун В.В
к.т.н., доцент
Кубанский государственный технологический университет

METHOD OF FORMING DECISION-MAKING BASED ON MULTI-CRITERIA ASSESSMENT WHEN REPELLING COMPUTER ATTACKS AND ELIMINATING THEIR CONSEQUENCES

Fisun V. V.
Ph. D., associate Professor
Krasnodar higher military school named after General of the army S. M. Shtemenko

Аннотация. В рамках концепции Государственной системы обнаружения и предупреждения компьютерных атак (КА) (ГосСОПКА) при формировании базы знаний КА, как многоагентной экспертной системы поддержки и принятия решений должностными лицами объектов критической информационной инфраструктуры (КИИ) и ситуационных ведомственных центров ГосСОПКА, предложено методику формирования сценариев управляющих решений по ситуации информационной безопасности (ИБ), дополнить интеллектуальными инструментами:

•методикой интеллектуального анализа быстроменяющихся ситуаций;

• методикой формирования принятия решений на основе многокритериальной оценки. Это позволит перейти к решению задач синтеза управления ИБ как эффективной оперативно-технической государственной интеллектуальной системы, с учетом решаемых государственными регуляторами задач.

Abstract. Within the concept of the State system of detection and prevention of computer attacks (KA) in the formation of the knowledge base KA, as a multi-agent expert systems and support decision-making by officials of objects of critical information infrastructure (CII) and situational departmental centers, the proposed methods of formation of scenarios of management decisions in a situation of information security (is), complement of intellectual tools:

• the mining technique of rapidly changing situations;

• methodology for forming decision-making based on multi-criteria assessment. This will allow us to move on to solving the problems of synthesizing information security management as an effective operational and technical state intellectual system, taking into account the tasks solved by state regulators.

Keywords: computer attack, classification, knowledge base, expert system, identifier uncertainty, intelligent system, information security management.

Ключевые слова: компьютерная атака, классификация, база знаний, экспертная система, неопределенность идентификатора, интеллектуальная система, управление информационной безопасностью.

Введение

Издание «Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)» [1], Федерального Закона «О безопасности критической информационной инфраструктуры (КИИ)» [2] и последующих от государственных регуляторов ФСТЭК и ФСБ РФ в области информационной безопасности 17 подзаконных актов существенно активизировали научно-исследовательскую деятельность в направлении систем управления процессами информационной безопасности (ИБ) и актуализировали подходы и методы разработки кибернетических систем и систем искусственного интеллекта.

По своей сути изданные нормативно-правовые документы рассматривают в качестве основной функциональности для реализации возможностей аппаратно-программных комплексов (АПК) и должностных лиц органов практически всех звеньев управления, в том числе и объектовых, функцию управления событиями-инцидентами информационной безопасности. Процессы управления ИБ регулируются государственными документами ГОСТ Р 531113.1-2008 [3] и ГОСТ Р ИСО/МЭК ТО 18044-2007 [4], а также корпоративными документами.

Органами непосредственного исполнения и решения указанных концептуально задач и соответственно их должностными лицами принимающими решения (ДЛПР), являются государственные, ведомственные и корпоративные ситуационные центры, а также замыкающиеся на центры объекты информационной инфраструктуры, т.е. собственно центры обработки данных (ЦОД), автоматизированные системы управления (АСУ), информационные системы (ИС) и информационно-телекоммуникационные системы (ИТКС), которые федеральным законом [2] рассматриваются как объекты КИИ.

Как показывает практика, современные конфликты ИБ характеризуются большой динамикой модификаций угроз и использования уязвимостей. Ввиду этого в плане успешного функционирования в конфликтном пространстве ИБ сегодня большую роль играет повышение потенциальных возможностей ИТКС за счет применения систем в состав которых входят алгоритмы принятия решений. Наиболее перспективными являются системы управления ИБ, которые не только самостоятельно обнаруживают КА, идентифицируют их, но и позволяют принимать своевременные управляющие и упреждающие ущерб информационным ресурсам решения. Этим обуславливается постоянная необходимость развития алгоритмов принятия решений. И этим обусловлен выбор для ИСУИБ технологии подготовки сценариев управляющих решений, разработанной ФИЦ ИУ РАН для нужд Института космических исследований.

Формирование принятия решений на основе многокритериальной оценки

Еще один инструмент экспертной системы в развитие алгоритмов поддержки и принятия управляющих решений, в том числе интеллектуальной системы информационной безопасности (ИСУИБ).

В процессе выработки решения лицо, принимающее решения, ЛПР формирует несколько возможных вариантов выполнения задачи (ВВЗ). ВВЗ формируются на основе замысла ЛПР, его целевой функциональности, они ситуационно детализируются, оптимизируются и количественно оцениваются по некоторому интегральному показателю, характеризирующему эффективность выполнения задачи в целом [7]. Зачастую количественная мера получена по результатам моделирования [5], например, как это рассмотрено при оценке угрозы безопасности информации (УБИ).

Наиболее простой подход при выборе управляющего решения, основан на оценке того, в какой мере предложенные варианты решения удовлетворяют основным требованиям ситуации. Часто цена вопроса выбора растет с ростом ограничивающих потребные, в том числе временные, ресурсы критериев. Но и в этом случае следует ограничивать круг возможных вариантов, опираясь на некоторые критерии отбора.

Перечень требований ситуаций при управлении ИБ может меняться в зависимости от самой ситуации. Тем не менее, можно выделить несколько групп критериев, включая возможность оперативного моделирования среды и ситуации по смешанным критериям [10,11].

Завершающим этапом формирования ВВЗ является определение обобщенных критериев оценки его эффективности. При наличии нескольких ВВЗ выполняется их сравнительная оценка, а затем они ранжируются по критерию оптимальности.

Для иллюстрации методики решения оптимизационной задачи определим некоторое конечное множество ВВЗ:

$$\mathbf{X}= (x_1, x_j, \ldots, x_k), \tag{1}$$

Последствия которых оцениваются множеством частных (локальных) критериев эффективности, образующих векторный критерий:

$$\mathbf{F}(x)= (f_1(x), f_2(x), \ldots , f_m(x)), \tag{2}$$

В качестве исходной информации выступает матрица эффективности:

$$A=\begin{bmatrix} x1 & x2 \cdots & xk \\ f11 & f12 \ \ldots & f1k \\ fm1 & fm2 \ \ldots & fmk \end{bmatrix}, \tag{3}$$

содержащая все ВВЗ и оценки их эффективности по всем критериям. Выбор оптимального ВВЗ на множестве критериев формально сводится к подбору оператора φ, который каждому вектору $\mathbf{F}(x_i)$ (столбцу в матрице эффективности **A**) ставит в соответствие действительное число $\mathbf{E}_i=\varphi(\mathbf{E}(x_i))$, оценивающее его эффективность и степень предпочтительности.

Обработка матрицы эффективности осуществляется в три этапа.

Первый этап – унификация и нормализация матрицы **A** за счет максимизации либо минимизации частных критериев, т.е. нормализация нормативами, что позволяет перейти к стратегически эквивалентной матрице, порождающей бинарные отношения эквивалентности между критериями, логика упрощает вычисления.

Второй этап – редукция (упрощение) эквивалентной матрицы отбраковкой заведомо невыгодных ВВЗ по принципу Парето: из двух остается тот, который лучше хотя бы по одному критерию. В результате получим компромиссную матрицу $\mathbf{A}_к$ меньшей размерности по столбцам.

Третий этап обработка матрицы $\mathbf{A}_к$ – выделение оптимального ВВЗ при заданном отношении предпочтения вектором приоритетов:

$$\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_m). \quad (4)$$

При этом вектор приоритетов задается по усмотрению субъективно ЛПР. Определение оптимального ВВЗ x_0 формулами, для min (5) и max (6) соответственно:

$$\mathbf{x_0 = arg\ min}_{i=1,q} \{ \mathbf{max}_{l=1,q} \lambda_e f_e(x) \};\ q \le k, \quad (5)$$

$$\mathbf{x^0 = arg\ max}_{i=1,q} \{ \mathbf{min}_{l=1,m} \lambda_e f_e(x) \};\ q \le k, \quad (6)$$

где $\lambda e > 0$, $\sum_{l=1}^{m} \lambda e = 1$.

Приведенные соотношения могут быть применены к эквивалентной матрице. При этом в случае не единственности полученного ВВЗ – они проверяются на паретооптимальность. Эта задача решается при каждом выборе рационального варианта действий.

Программная реализация этой задачи предполагает межмодульную связь в СУИБ для ЛПР посредством единой базы знаний из которой бы поступала необходимая по параметрам событий и инцидентов ИБ информация для решения рассмотренной задачи, в том числе связь с программными модулями, моделирующими оценку ситуации по критериям УБИ защищаемого информационного ресурса [7,8]. Работоспособность и соответствие целевой функциональности методики проверены и подтверждены математическим моделированием в программной среде пакета MATLAB2009b с привлечением релевантной статистики в качестве параметров процессов из БДУ ФСТЭК.

Как следует из «Методики определения угроз безопасности информации (УБИ) в ИС», применяемой совместно с БДУ БИ (www.fstek.ru), разработанных ФСТЭК, показатель актуальности УБИ в ИС (по сути ближайшая возможность нарушений в ИТКС конфиденциальности, целостности или доступности информации), то что нужно для принятия решения на блокирование/нейтрализацию КА, определен как 2-х компонентный вектор:

$$БИ_j = [\text{вероятность реализации угрозы } (P_j); \text{степень ущерба } (X_j)],$$

где $\mathbf{P_j}$ определяется на основе анализа статистики данных о частоте реализации угрозы/возникновения инцидентов ИБ в ИС [8].

Их значения определяются методом интегрирования уравнений вероятностных моментов, процесс вычисления которых автоматизирован работой [12], в том числе и для нелинейных систем методом статистической линеаризации.

Однако в большинстве практических случаев отражения КА обеспечить необходимую для приемлемых эксплуатационных условий функциональности СОА статистическую выборку не представляется возможным как и в случае оценки $\mathbf{P_j}$ Байесовским методом или нейронной сетью. Не лишен отмеченного недостатка и распространенный в антивирусных средствах и обнаружении большинства сетевых атак сигнатурный метод. Именно этими обстоятельствами объясняется еще не завершенный поиск наиболее эффективного для практики отражения КА метода среди представленного в [4,6] многообразия методов.

Вывод по проблеме

Предложенная методика формирования принятия решений на основе многокритериальной оценки, дополняя интеллектуальный инструментарий лиц принимающих решения при ситуационном управлении ИБ объектов КИИ, повышает эффективность оперативно-технического управления ситуационных центров, снижает время реакции на инциденты ИБ и атаки, при условии их проявления в неопределенности ситуации и целевого воздействия.

Литература

1. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА): указ Президента Российской Федерации от 12.12.2014г. №К-1274.-Система Гарант

2. Федеральный Закон «О безопасности критической информационной инфраструктуры (КИИ)»

3. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

4. Бирюков А.А. Информационная безопасность: защита и нападение. М.:ДМК Пресс, 2016, 474с.

5. Астрахов А.В., Климов С.М., Сычев М.П. Противодействие компьютерным атакам. Технологические основы. 2010, 70с.

6. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасаность открытых систем: Учебник для вузов в 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком, 2006. – 536 с.

7. Новиков Д.А. Кибернетика: Навигатор**.** История кибернетики, современное состояние, перспективы развития**. –** М.: ЛЕНАНД, 2016. – 160 с. (Серия «Умное управление»).

8. Фисун В.В. Применимость методов исследования динамических систем при разработке базы знаний ГосСОПКА. М.: ИКСИ, 22 межведомственная конференция, 2018.-5с.

9. Казаков И.Е., Артемьев В.М. Оптимизация динамических систем случайной структуры. М.: Наука, 1980.

10. Белов В.В., Смирнов А.Е., Чистякова В.И. Распознавание нечетко определяемых состояний технических систем. - М.: Горячая линия-Телеком, 2012. - 138 с.

11 Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью./ Труды ИСА РАН. - 2009, Т.4. - С. 74-103.

12. Фисун В.В., Ерошенков М.Г. «Аналитическое исследование стохастических динамических систем»: Пакет прикладных программ. Государственный фонд алгоритмов и программ СССР.-Минск: РФАП БССР, №432, 1988.

Проверено 11.02.2021г.

Уникальность текста 81% Отлично. Текст уникальный. Некоторые фразы не уникальны.

Сходство

Все совпадения

https://www.gaz-is.ru/reshenija/resheniya/monitori... (9%)
https://www.infosystems.ru/courses/avtorskie_kursy... (9%)
https://zen.yandex.ru/media/info_law_society/proti... (8%)
https://www.garant.ru/products/ipo/prime/doc/56644... (7%)
https://www.ec-rs.ru/resheniya/bezopasnost-kritich... (6%)
http://www.it.ru/press_center/publications/7353/ (6%)
https://krasnodar.postupi.online/vuz/institut-komp... (1%)
https://ens.mil.ru/education/higher/more.htm?id=86... (1%)
https://www.infosystems.ru/courses/kursy_soglasova... (1%)
http://www.ncfu.ru/export/university/institutes/in... (1%)
https://kvvu.mil.ru/Nauka/Nauchno-issledovatelskij... (1%)

Фисун Владимир Владимирович. Кубанский государственный технологический университет, г.Краснодар, РФ. Доцент кафедры КТИиИБ, кандидат технических наук, доцент. Количество печатных работ 63 (в т.ч. 1 монография). Область научных интересов: исследование динамических систем, информационные технологии, информационная безопасность, искусственный интеллект

References

1. the Concept of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation (Gossopka): decree Of the President of the Russian Federation of 12.12.2014. No. K-1274.-Garant System

2. Federal Law "On security of critical information infrastructure (CII)"

3. GOST R ISO/IEC TO 18044-2007 "Information technology. Methods and means of ensuring security. Information security incident management".

4. Biryukov A. A. Information security: protection and attack. Moscow:DMK Press, 2016, 474s.

5. Astrakhov A.V., Klimov S. M., Sychev M. P. Counteraction to computer attacks. Technological basis. 2010, 70s.

6. Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I., Ushakov D. V. Information security of open systems: textbook for universities in 2 volumes. Volume 1 – Threats, vulnerabilities, attacks and approaches to protection. – Moscow: Hotline – Telecom, 2006. – 536 p.

7. Novikov D. A. Cybernetics: Navigator. History of Cybernetics, current state, development prospects. – Moscow: LENAND, 2016. – 160 p. (Smart management series).

8. Fisun V. V. application of methods of research of dynamic systems in development of knowledge base Gossipy. M.: the ICSI, 22 interagency conference, 2018.-5C.

9. Kazakov I. E., Artemiev V. M. Optimization of dynamic systems with random structure. M.: Nauka, 1980.

10. Belov V. V., Smirnov A. E., Chistiakova V. I. Recognition of clearly-defined States of technical systems. - M.: Hot line-Telecom, 2012. - 138 C.

11 Kotenko I. V. Intellectual mechanisms of cybersecurity management./ Proceedings of the ISA RAS. - 2009, T. 4. - Pp. 74-103.

12. Fisun V. V., Eroshenkov M. G. "analytical study of stochastic dynamic systems": a package of applied programs. State Fund of algorithms and programs of the USSR-Minsk: RFAP BSSR, No. 432, 1988.