ARTICLE HISTORY: Received: February 20, 2022 Accepted: April 12, 2022 Published: April 19, 2022

ЭКСПЕРТНАЯ СИСТЕМА ПОДДЕРЖКИ И ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Фисун В.В.
к.т.н., доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный технологический университет»

EXPERT SYSTEM FOR SUPPORT AND DECISION-MAKING ON THE MANAGEMENT OF INFORMATION SECURITY OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Fisun V.V.
Candidate of Technical Sciences, Associate Professor
Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University"

Аннотация. В статье рассматриваются возможности формирования базы знаний, как многоагентной экспертной системы поддержки и принятия решений должностными лицами объектов критической информационной инфраструктуры (КИИ) и ситуационных ведомственных центров ГосСОПКА, определены решаемые ею задачи, на основе инженерии знаний сделан выбор стратегии получения знаний «формирование знаний». Для реализации выбранной стратегии предлагается подходящий по условиям применимости ДСМ-метод АПНИ (индуктивный метод Д.С. Милля [8], развитый при поддержке агентства перспективных научных исследований) [3]. В развитие метода предлагается весь процесс разрешения неопределенности, гносеологическую цепь «Проблема – Гипотеза» [9] завершить звеном «Закон» с установлением закономерности определения идентификатора компьютерной атаки в блоке ложного сетевого информационного объекта (ЛСИО) системы защиты информации (СЗИ) объекта КИИ [3].

Abstract. The article discusses the possibilities of forming a knowledge base as a multi-agent expert system for support and decision-making by officials of critical information infrastructure (CII) facilities and situational departmental centers of the State SOPKA, determines the tasks it solves, and on the basis of knowledge engineering, the choice of the strategy for obtaining knowledge "knowledge formation" is made. To implement the chosen strategy, the APNI JSM method (inductive D.S. Mill method [8], developed with the support of the Agency for Advanced Research) [3] is proposed, which is suitable for the conditions of applicability. In the development of the method, it is proposed to complete the whole process of resolving uncertainty, the epistemological chain "Problem - Hypothesis" [9] to be completed with the link "Law" with the establishment of a pattern for determining the identifier of a computer attack in the block of a false network information object (LSIO) of the information security system (ISI) of the CII object [3].

Ключевые слова: информационная безопасность (ИБ), критическая информационная инфраструктура (КИИ), информационная система (ИС), искусственный интеллект (ИИ), интеллектуальный анализ данных (ИАД), система поддержки и принятия решений (СППР), база знаний, экспертная система (ЭС).

Keywords: information security (IS), critical information infrastructure (CII), information system (IS), artificial intelligence (AI), data mining (DIA), decision support and decision system (DSS), knowledge base, expert system (ES).

Цель статьи – развитие государственной системы обнаружения и предупреждения компьютерных атак (ГосСОПКА) в направлении интеллектуализации процессов управления информационной безопасностью, дальнейшая разработка основ и принципов функционирования элементов государственной интеллектуальной системы управления информационной безопасностью (ИСУИБ) объектов критической информационной инфраструктуры.

В продолжение исследований в направлении интеллектуализации системы управления информационной безопасностью объектов КИИ, как средства разрешения неопределенности ситуации и целевого воздействия компьютерных атак, а также кибернетических воздействий проявляющихся антропогенных угроз безопасности информации во всем спектре событий, инцидентов и атак, для их необходимого обнаружения и предупреждения [3] предлагается рассмотреть с позиции системного анализа функциональное содержание отдельных структурных элементов ИСУИБ, в частности базы знаний, как многоагентной экспертной системы поддержки и принятия решений должностными лицами объектов КИИ и ситуационных ведомственных центров ГосСОПКА [1].

Центральная парадигма интеллектуальных технологий сегодня — это обработка знаний. Системы, ядром которых является база знаний или модель предметной области, описанная на языке сверхвысокого уровня,

приближенном к естественному, называют интеллектуальными. **Наиболее распространенным видом ИС являются экспертные системы (ЭС) [5].** Наибольшие трудности в разработке ЭС вызывает сегодня не процесс машинной реализации систем, а домашинный этап анализа знаний и проектирования базы знаний. Этим занимается специальная наука — инженерия знаний.

В целом процесс функционирования ЭС можно представить следующим образом: пользователь, желающий получить необходимую информацию, через пользовательский интерфейс посылает запрос к ЭС; решатель, пользуясь базой знаний, генерирует и выдает пользователю подходящую рекомендацию, объясняя ход своих рассуждений при помощи подсистемы объяснений (рисунок 1) [5].

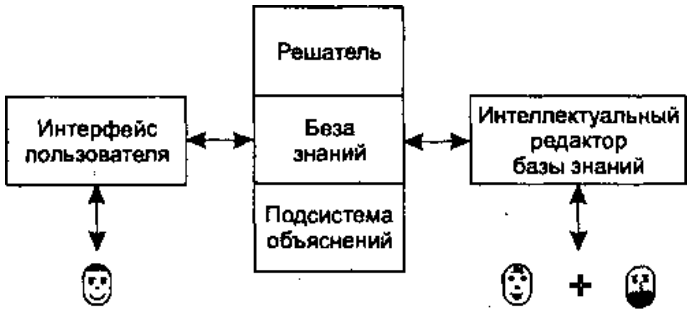

Рисунок 1— Обобщенная структура экспертной системы.

Интерфейс пользователя — комплекс программ, реализующих диалог пользователя с ЭС как на стадии ввода информации, так и при получении результатов.

База знаний (БЗ) — ядро ЭС, совокупность знаний предметной области, записанная на машинный носитель в форме, понятной эксперту и пользователю (обычно на некотором языке, приближенном к естественному). Параллельно такому «человеческому» представлению существует БЗ во внутреннем «машинном» представлении.

Решатель — программа, моделирующая ход рассуждений эксперта на основании знаний, имеющихся в БЗ [2]. Синонимы: ***дедуктивная машина, машина вывода, блок логического вывода.***

Решаемые ЭС задачи, аналогичные задачам ГосСОПКА [4] :

Интерпретация данных. Это одна из традиционных задач для экспертных систем. Под интерпретацией понимается процесс определения смысла данных, результаты которого должны быть согласованными и корректными. Обычно предусматривается многовариантный анализ данных. В частности - обнаружение и идентификация различных типов объектов предметной области (например: типа компьютерной атаки).

Диагностика. Под диагностикой понимается процесс соотнесения объекта с некоторым классом объектов, или обнаружение неисправности в некоторой системе. Неисправность — это отклонение от нормы. Такая трактовка позволяет с единых теоретических позиций рассматривать и неисправность оборудования в технических системах, и заболевания живых организмов, и всевозможные природные аномалии (проявления компьютерных атак).

Мониторинг. Основная задача мониторинга — непрерывная интерпретация данных в реальном масштабе времени и сигнализация о выходе тех или иных параметров за допустимые пределы (к примеру, программного деструктивного воздействия). Главные проблемы — «пропуск» тревожной ситуации и инверсная задача «ложного» срабатывания. Сложность этих проблем в размытости симптомов тревожных ситуаций и необходимость учета временного контекста.

Проектирование. Проектирование состоит в подготовке спецификаций на создание «объектов» с заранее определенными свойствами. Под, спецификацией понимается весь набор необходимых документов — чертёж, пояснительная записка и т. д. Основные проблемы здесь — получение четкого структурного описания знаний об объекте и проблема «следа». В частности, настоящий этап для ИСУИБ можно определить, как этап структурного проектирования [2].

Прогнозирование. Прогнозирование позволяет предсказывать последствия некоторых событий или явлений на основании анализа имеющихся данных. Прогнозирующие системы логически выводят вероятные следствия из заданных ситуаций. В прогнозирующей системе обычно используется параметрическая динамическая модель, в которой значения параметров «подгоняются» под заданную ситуацию. Выводимые из этой модели следствия составляют основу для прогнозов с вероятностными оценками. На основании прогноза решается задача ГосСОПКА предупреждения компьютерных атак.

Обучение. Под обучением понимается использование компьютера для обучения какой-то дисциплине или предмету. Системы обучения, в т.ч. «машинного» [11], диагностируют ошибки при изучении какой-либо дисциплины с помощью ЭВМ и подсказывают правильные решения. Эта задача необходима для целей обучения персонала объектов КИИ работе в среде функционирования экспертной системы [4].

Управление. Под управлением понимается функция организованной системы, поддерживающая определенный режим деятельности. Такого рода ЭС осуществляют управление поведением сложных систем в соответствии с заданными спецификациями. В рамках ИСУИБ задание спецификаций определяет порядок взаимодействия структурных элементов системы.

Поддержка принятия решений. Поддержка принятия решения — это совокупность процедур, обеспечивающая лицо, принимающее решения, необходимой информацией и рекомендациями, облегчающими процесс принятия решения. Эти ЭС помогают специалистам выбрать и/или сформировать нужную альтернативу среди множества выборов при принятии ответственных решений. Это целевая задача разрабатываемой ЭС.

В общем случае все системы, основанные на знаниях, можно подразделить на ***системы, решающие задачи анализа,*** и на ***системы, решающие задачи синтеза [2].*** Основное отличие задач анализа от задач синтеза заключается в том, что если в задачах анализа множество решений может быть перечислено и включено в систему, то в задачах синтеза множество решений потенциально не ограничено и строится из решений компонент или подпроблем. Задачами анализа являются: интерпретация данных, диагностика, поддержка принятия решения; к задачам синтеза относятся проектирование, планирование, управление. Комбинированные: обучение, мониторинг, прогнозирование [2].

Можно выделить три основные стратегии проведения стадии получения знаний при разработке ЭС (рис. 2):

1. С использованием ЭВМ при наличии подходящего программного инструментария, иначе ***приобретение*** знаний.

2. С использованием программ обучения при наличии репрезентативной (то есть достаточно представительной) выборки примеров принятия решений в предметной области и соответствующих пакетов прикладных программ, иначе ***формирование*** знаний.

3. Без использования вычислительной техники путем непосредственного контакта инженера по знаниям и источника знаний (будь то эксперт, специальная литература или другие источники), иначе ***извлечение*** знаний.

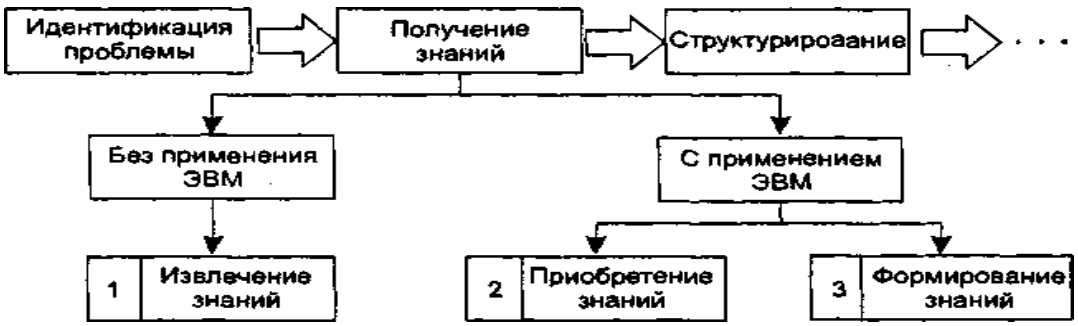

Рисунок 2 — Стратегии получения знаний.

В статье [3] в качестве стратегии получения знаний сделан выбор в пользу «формирование знаний» по следующим основаниям.

Из отмеченных проблем и противоречий следуют научные направления исследований [3]:

- модель представления знаний об атаках во всем спектре их проявлений (База Знаний КА);
- идентификация КА на основе их классификации;
- оценка факта воздействия КА на основе информации от системы защиты информации и базы знаний КА для дальнейшего их предупреждения и ликвидации последствий, уточнение параметров КА, формирование базы фактов (БФ);
- экспертная оценка проявлений КА, модель действий при нарушении ИБ, формирование сценария принятия решения ЛПР по управлению процессами ИБ;
- передача по согласованному с государственным регулятором протоколу описания новой угрозы ИБ (корректировка ранее установленной) и подготовленного сценария принятия решения ЛПР по управлению процессами ИБ в БДУ ФСТЭК.

Рассматривая первые два направления, как первоочередные и актуальные, следует установить, что база знаний, как основа экспертной системы КА для принятия решений ЛПР по подготовленному сценарию управления процессами ИБ критического объекта, представляется как база знаний с реляционной неопределенностью идентичности КА [6].

Разрешение неопределенности идентичности возможно способом, с помощью которого логический вывод в логике первого порядка может быть выполнен посредством логического вывода в пропозициональной логике по эквивалентной пропозициональной базе знаний. Эквивалентная база знаний может оказаться слишком большой (NP- сложной), в силу значительной параметрической размерности описания КА, для выполнения в ней вычислений [7].

С целью локализации разрешения неопределенности предлагается подходящий по условиям применимости [8] ДСМ-метод АПНИ (индуктивный метод Д.С. Милля, развитый при поддержке агентства перспективных научных исследований).

Используя:

- ДСМ-рассуждения сформулированные посредством формального языка JL;
- ДСМ-исследования посредством метаязыка MJL для обнаружения эмпирической закономерности идентификации КА, составляющей базу фактов из событий и инцидентов, представленных по факту источниками СЗИ (МЭ, СРД, SIEM, ОС и логами) и классификации КА (не доопределенный идентификатор КА из БЗ);
- порождение гипотез о причинах и предсказаниях в идентификации КА, имеющих аргументацию и обоснование по результатам сравнения пары шкал оценки качества рассуждений [8], получим рабочую гипотезу определенного идентификатора КА.

Однако представленная ДСМ-методом гипотеза, хотя и максимально правдоподобна, остается таковой.

В целях окончательного разрешения неопределенности идентификации КА, а следовательно и закономерного соответствующего принятия решения ЛПР, предусмотренного сценарием управления процессами ИБ, предлагается весь процесс разрешения неопределенности завершить «установлением закона»:

«Проблема – Гипотеза – Закон», гносеологической цепи следующей из [9].

Установление закономерности из гипотезы об установленном идентификаторе КА возможно, и реализуется в блоке ЛСИО СЗИ, которому на вход поступает вся информация о рассматриваемом процессе - фрагменте неустановленной, не идентифицированной КА и соответствующей информации от СЗИ (МЭ, СРД, СКЗИ, ОС), а также гипотеза идентификации КА.

Имея информацию из гипотезы идентификатора КА, ЛСИО предложит процессу КА информацию для продолжения достижения цели, как правило деструктивной, в рамках виртуальной среды, лишающей действительное нанесение ущерба ИТКС, выявляя тем самым траекторию деструктивных действий по реализации угрозы ИБ, лежащей в основе классификации и позволяющей принять решение ЛПР по противодействию КА, а также предупреждения их последствий.

В случае неприятия информации от гипотезы КА, в ЛСИО будет продолжено инициирование действий КА для идентификации методами машинного обучения: интеллектуального анализа данных, нечеткого анализа динамики поведения КА и нейросетевого подхода [3], [10], однако это уже процесс без критических ограничений по времени для результата.

Вывод: предложенное функциональное содержание отдельных структурных элементов ИСУИБ, в частности базы знаний, как многоагентной экспертной системы поддержки и принятия решений должностными лицами объектов КИИ и ситуационных ведомственных центров ГосСОПКА, позволит разрешить неопределенности ситуации и целевого воздействия компьютерных атак [3], а также кибернетических воздействий проявляющихся антропогенных угроз безопасности информации во всем спектре событий, инцидентов и атак, для их необходимого обнаружения и предупреждения.

Литература

1. Фисун В.В. Интеллектуальная система управления информационной безопасностью объектов критической информационной инфраструктуры / В.В. Фисун // Материалы конференции «АСУ, информационно-коммуникационные системы» / ВИТ «ЭРА». —Анапа. — 2019.
2. Фисун В.В. Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры: монография / Фисун В.В. // - Москва: РУСАЙНС, 2020.- 360 с.
3. Фисун В.В. Интеллектуализация обнаружения, предупреждения, и ликвидации последствий компьютерных атак на объекты критической информационной инфраструктуры / В.В. Фисун // В сборнике: Глобализация науки и техники в условиях кризиса. Материалы XXIX Всероссийской научно-практической конференции. В 2-х частях. Ростов-на-Дону, 2021. С. 138-148.
4. Фисун В.В. Интеллектуальная система управления информационной безопасностью объектов критической информационной инфраструктуры / В.В.Фисун // Перспективы науки. 2020. № 11 (134). С. 181-186.
5. Гаврилова Т.А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский // — СПб: Питер, 2000. — 384 с.: ил.
6. Джордж Ф. Люгер. Искусственный интеллект: стратегии и методы решения сложных проблем / Джордж Ф. Люгер. —4-е издание.: Пер. с англ. — М.: Издательский дом "Вильямс", 2003. —864 с.: ил. —Парал. тит. англ.
7. Рассел Стюарт. Р24 Искусственный интеллект: современный подход / Стюарт Рассел, Питер Норвиг — 2_е изд..: Пер. с англ. —М. :Издательский дом ‘‘Вильямс’’, 2007. —1408 с. : ил. - Парал. тит. англ.
8. Финн В.К. Эвристика обнаружения эмпирических закономерностей и принципы интеллектуального анализа данных / В.К.Финн // Искусственный интеллект и принятие решений. —2018. —№3. —с. 3-19.

9. Карпович В.Н. Проблема, гипотеза, закон / В.Н. Карпович – Новосибирск: Наука, 1980. —176с.

10. Фисун В.В. Синтез адаптивной многомодульной системы активного аудита на основе нечетких нейросетей/ В.В.Фисун, А.В. Петровский // Защита информации. Конфидент. —2003. —№2.

11.Алпайдин Этем. Машинное обучение: новый искусственный интеллект / Этем Алпайдин – Пер. с англ. – М.: Изд.группа «Точка», 2017. – 208с.

References

1. Fisun V.V. Intellectual control system for information security of objects of critical information infrastructure / V.V. Fisun // Materialy konferentsii «ASU, informatsionno-kommunikatsionnyye sistemy» / VIT «ERA». —Anapa. — 2019.

2. Fisun V.V. Artificial Intelligence of Information Security Management of Critical Information Infrastructure Objects: monograph / Fisun V.V. // - Moscow: RUSSIGN, 2020.- 360 p.

3. Fisun V.V. Intellectualization of detection, prevention, and elimination of consequences of computer attacks on objects of critical information infrastructure / V.V. Fisun // V sbornike: Globalizatsiya nauki i tekhniki v usloviyakh krizisa. Materialy XXIX Vserossiyskoy nauchno-prakticheskoy konferentsii. In 2 parts. Rostov-on-Don, 2021. Pp. 138-148.

4. Fisun V.V. Intelligent information security management system for critical information infrastructure facilities / V.V. Fisun // Perspektivy nauki. 2020. № 11 (134). Pp. 181-186.

5. Gavrilova T.A. Knowledge bases of intelligent systems / T. A. Gavrilova, V. F. Khoroshevsky // - St. Petersburg: Peter, 2000. - 384 p.: ill.

6. George F. Luger. Artificial intelligence: strategies and methods for solving complex problems / George F. Luger. -4th edition.: Translation from English. - M.: Williams Publishing House, 2003. - 864 p.: ill. —Parall. tit. English.

7. Russell Stewart. R24 Iskusstvennyy intellekt: sovremennyy podkhod / Stuart Russell, Peter Norvig - 2nd ed.: Per. from English. —M.: Williams Publishing House, 2007. -1408 p.: ill. - Paral. tit. English

8. Finn W.K. Heuristics for detecting empirical patterns and principles of data mining / V.K. Finn // Iskusstvennyy intellekt i prinyatiye resheniy. —2018. —№3. —pp. 3-19.

9. Karpovych V.N. Problema, hypoteza, zakon / V.N. Karpovych – Novosybyrsk: Nauka, 1980. —176p.

10. Fisun V.V. Synthesis of an adaptive multi-module active audit system based on fuzzy neural networks / V.V. Fisun, A.V. Petrovsky // Zashchita informatsii. Confident. —2003. —№2.

11. Alpaydin Etem. Machine Learning: The New Artificial Intelligence / Etem Alpaydin - Translated from English. - M.: Publishing group "Point", 2017. – 208p.