ARTICLE HISTORY: December: 19, 2021 Accepted: February 11, 2021 Published: February 19, 2021

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПОСТРОЕНИЮ ЦЕНТРА МОНИТОРИНГА СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК

Голицын Сергей Александрович
кандидат технических наук,
магистр Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко,
специалист в области организации защиты информации
Шульженко Анастасия Дмитриевна
начальник лаборатории Военно-космической академии
имени А.Ф. Можайского, г. Санкт-Петербург,
специалист в области обработки информации

CONCEPTUAL APPROACH TO THE CONSTRUCTION OF A MONITORING CENTER FOR DETECTION, PREVENTION AND ELIMINATION OF THE CONSEQUENCES OF COMPUTER ATTACKS

Golitsyn Sergey Alexandrovich
candidate of technical sciences,
Master of the Krasnodar Higher Military School
named after General of the Army S.M. Shtemenko,
information security specialist
Shulzhenko Anastasia Dmitrievna
Head of the Laboratory of the Military Space Academy
named after A.F. Mozhaisky, St. Petersburg,
information processing specialist

Аннотация. В данной статье рассмотрены вопросы организации центра мониторинга системы обнаружения, предупреждения и ликвидации последствий компьютерных атак как человеко-машинной системы с интегрированной автоматизированной поддержкой принятия решений. Предложен концептуальный подход к построению системы и её функциональная схема, задачи и процедуры.

Abstarct. This article discusses the issues of organizing a monitoring center for a system for detecting, preventing and eliminating the consequences of computer attacks as a man-machine system with integrated automated decision support. A conceptual approach to building a system and its functional diagram, tasks and procedures are proposed.

Ключевые слова: поддержка принятия решения, экспертная система, интеллектуальный поиск, противодействие компьютерным атакам.

Key words: decision support, expert system, intelligent search, counteraction to computer attacks.

В соответствии с реализацией мероприятий, определенных Федеральным законом от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» приобретает массовый характер создание центров мониторинга системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру России (далее – ЦМ СОПКА), выполняющих функции ситуационно-аналитических центров, также называемых Security Operation Center (SOC).

Сегодня все субъекты критической информационной инфраструктуры (далее – КИИ) обязаны передавать информацию о случившихся компьютерных инцидентах в ЦМ СОПКА. С увеличением количества субъектов КИИ соответственно увеличивается и объем информации, обрабатываемый силами и средствами ЦМ СОПКА.

В свою очередь увеличение объема информации о компьютерных инцидентах, поступающей в ЦМ СОПКА, говорит об актуальности разработки и внедрения системы экспертной поддержки (далее – СЭП) для повышения эффективности функционирования средств СОПКА.

Основное назначение системы экспертной поддержки – это обеспечение эффективной консолидации опыта и знаний, целенаправленного использования и развития организационных возможностей на основе широкого применения новейших информационно-аналитических методов и технологий для обеспечения оперативной выработки управленческих решений в различных ситуациях, с целью обеспечения эффективного и непрерывного функционирования контролируемых систем КИИ [1].

Под контролируемой системой (далее – КС) понимается совокупность функциональных информационных систем и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей объектов критической информационной инфраструктуры.

В самом общем случае ЦМ СОПКА можно определить как человеко-машинную систему с интегрированным программно-аппаратным комплексом, реализующим функции подготовки и поддержки принятия решений (далее – ППР).

Работу ЦМ СОПКА целесообразно представлять в трех режимах функционирования, что существенно облегчает работу лица принимающего решение (далее – ЛПР) и сводит к минимуму основной показатель – затрачиваемое время на выработку решения и принятие мер [2]:

- нормальный режим функционирования;
- режим планирования;
- режим реагирования.

Работа ЦМ СОПКА в нормальном режиме осуществляется взаимодействием всех модулей системы и оценкой ситуации онлайн, предоставления информации ЛПР и группе экспертов на средствах отображения коллективного пользования.

Основными задачами ЦМ СОПКА в нормальном режиме являются:

- сбор и предварительная обработка информации о состоянии КС;
- формирование критериев оптимального состояния КС;
- формирование текущей математической модели состояния КС;
- выбор режима функционирования КС;
- ввод и мониторинг значений в соответствии с системой критериев;
- назначение весов критериев;
- генерация множества решений;
- выбор решающих правил;
- прогнозирование показателей и оценки эффективности КС;
- оптимизация параметров КС в соответствии с управляющим воздействием.

Основное отличие режима планирования от нормального режима функционирования заключается в том, что работа осуществляется по заранее подготовленным сценариям, в виде игры: построением модели ситуации с учетом добавления опасных факторов и введения индикаторов характеризующих наиболее проигрываемую ситуацию, обсуждения между экспертами результатов. Данный режим позволяет проконтролировать работу модулей подсистем мониторинга, моделирования состояний КС, прогнозирования, ППР и выработки управляющих воздействий [3].

Основными задачами ЦМ СОПКА в данном режиме являются:

- получение показателей и системы критериев из баз данных;
- формирование соотношений показателей и системы критериев согласно математической модели;
- формирование множеств состояний системы;
- иерархическое представление деревьев решений для оценки общего состояния системы.

Ситуации, которые вызывают переход из нормального режима функционирования или режима планирования в режим реагирования являются критическими для функционирования КС. В данном режиме формирование сценария принятия решений практически совмещается с процессом принятия решений.

Главное отличие системы экспертной поддержки от традиционных систем автоматизации управления состоит в том, что в процессе проведения совместной работы экспертов в режиме реального времени можно рассчитывать и анализировать последствия любых управленческих решений.

Концептуальный подход к построению СЭП представлен на рисунке **Ошибка! Источник ссылки не найден.**.

При мониторинге и анализе ситуации решаются следующие основные задачи:

- мониторинг и сбор различного формата информации, разнородной и разрозненной по своему составу;
- оперативное отслеживание единого информационного пространства, в котором работают все основные службы;
- предварительная обработка полученных данных, включающая в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию;
- анализ первичных и обработанных данных;
- представление обработанных данных в формализованном виде.

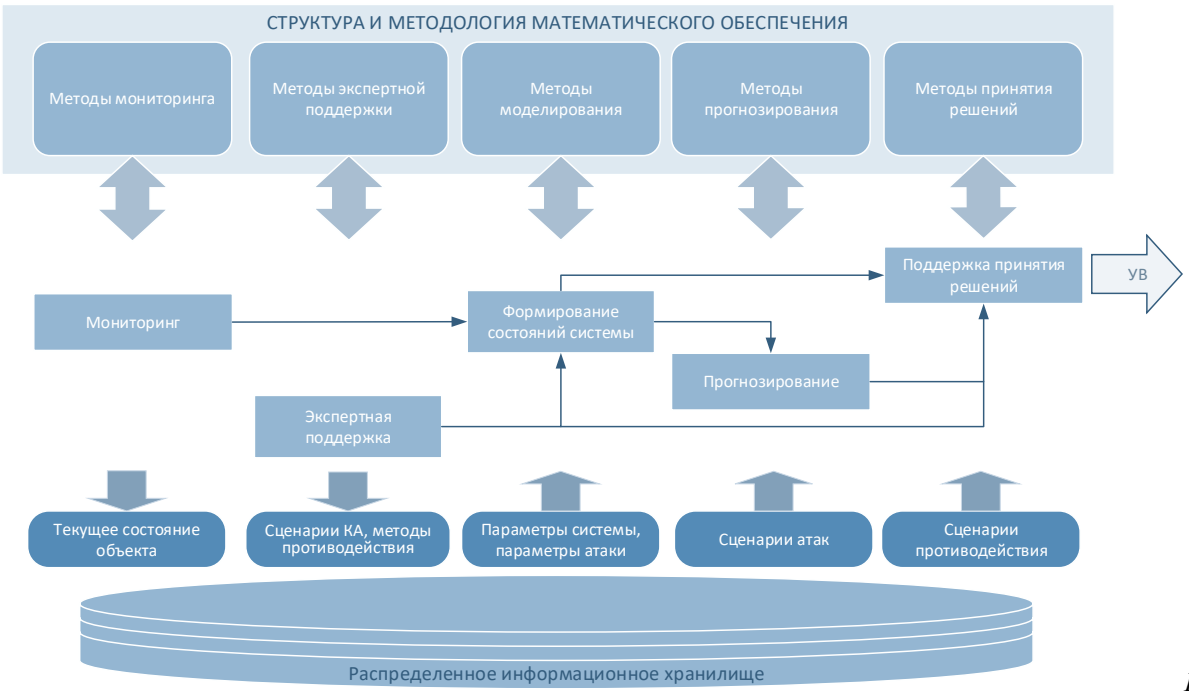

Рисунок 1 – Концептуальный подход к построению ЦМ СОПКА

Общий алгоритм функционирования СЭП СОПКА, отображающий этапы функционирования, целесообразно представить в виде IDEF0-диаграммы, приведенной на рисунке 2.

Основными функциями подсистемы формирования состояний системы являются:

– определение списка контролируемых параметров КС и частоты обновления их значений;

– формирование критериев оптимальности КС – общих признаков значений параметров КС, соответствующих штатному функционированию системы;

– обновления значений вектора параметров КС (согласно списка контролируемых параметров);

– возможность автоматизированного обучения;

– передача подсистеме прогнозирования модели состояний КС при обнаружении первых признаков КА соответствующего типа с указанием списка возможных КА, этапа КА и вероятности проведения этих КА;

– передача подсистеме поддержки принятия решения формализованных критериев оптимальности КС.

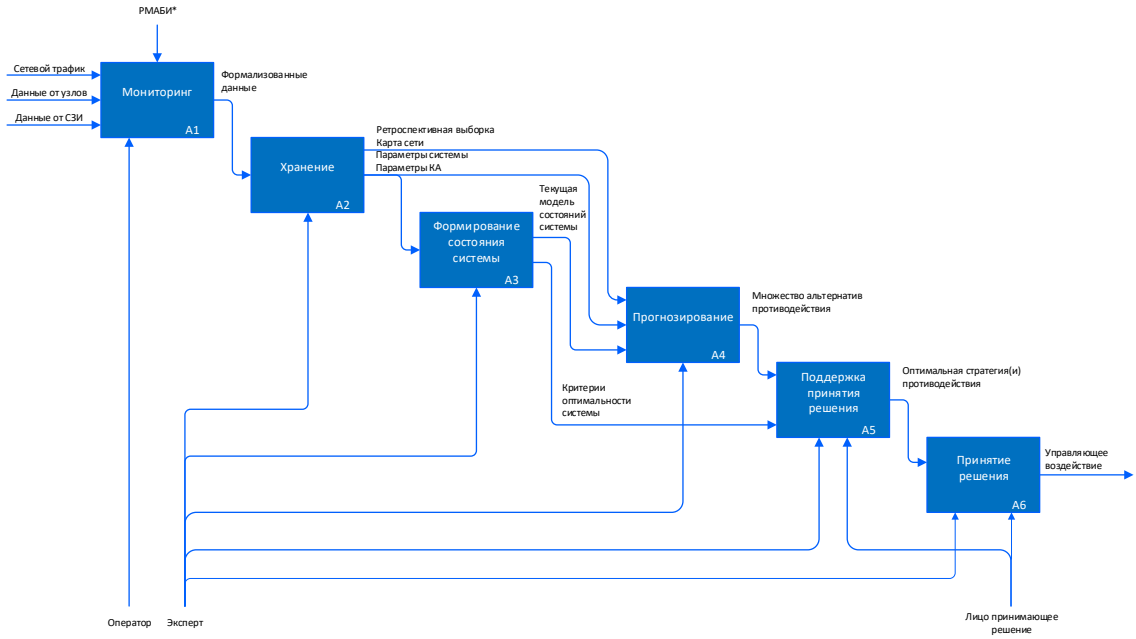

Рисунок 2 – Структурно-функциональная схема СЭП СОПКА

К основным решаемым задачам в процессе прогнозирования относятся:

- прогнозирование показателей различного назначения и формата;
- формирование комплексных интегральных оценок;
- выполнение целевых прогнозных расчетов с учетом различных параметров;
- обоснование значимости и оценка достижимости целей развития.

В процессе поддержки принятия решений определяется оптимальная стратегия, либо некоторый набор оптимальных стратегий противодействия компьютерным атакам, реагирования на компьютерные инциденты.

К основным задачам ППР относятся:

- определение критерия оптимальности выбора стратегии противодействия исходя из условий применения методов ППР;
- определение оптимальной стратегии (стратегий) противодействия с учетом ретроспективных данных и состояния КС.

В процессе принятия решений реализуются основные цели функционирования СЭП – решение задач выбора и утверждения оптимальной стратегии ЛПР, а также формирования управляющего воздействия, предназначенного для противодействия компьютерным атакам.

В процессе моделирования многоаспектных проблем и развития ситуации преследуются следующие основные цели:

- разработка модели объекта исследования;
- адаптация модели к изменениям предметной области;
- выявление структуры анализируемой проблемы;
- выявление наиболее вероятных вариантов и сценариев развития проблемы;
- моделирование на основе комплекса моделей состояния и взаимосвязей различных функциональных показателей.

Вывод. Процедуры экспертной поддержки наиболее эффективны при условии, когда формализованные методы, основанные на традиционном математическом аппарате, не позволяют выработать решения, или в случае, если необходима информация по исследуемой проблеме.

Процедуру интеллектуального поиска данных необходимо применять тогда, когда по принимаемому вопросу не наработана необходимая база первичных данных. Использование интеллектуального поиска данных позволит определить и формализовать слабоструктурированные данные, ранее не участвовавшие в процессе формирования управляющего воздействия.

Применение СЭП в СОПКА позволит значительно сократить временные показатели выполнения мероприятий по противодействию компьютерным атакам, а в случае проведения с помощью СЭП мероприятий по прогнозированию возможных направлений развития компьютерных атак можно добиться сохранения штатных режимов функционирования КС критической информационной инфраструктуры.

Литература

1. Моргунов Е.П. Система поддержки принятия решений при исследовании эффективности сложных систем: принципы разработки, требования и архитектура // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. 2007. №3. С. 59 – 63.

2. Лычкина Н.Н. Имитационные модели в процедурах и системах поддержки принятия стратегических решений на предприятиях // Бизнес-информатика, 2007. №1. С. 29–35.

3. Сороколетов П.В. Построение интеллектуальных систем поддержки принятия решений // Известия ЮФУ. Технические науки. С. 117 – 124.

References

1. Morgunov E.P. Decision support system in the study of the effectiveness of complex systems: design principles, requirements and architecture // Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta imeni akademika M.F.Reshetn'ova. 2007. №3. P. 59 – 63.

2. Lychkina N.N. Simulation models in procedures and systems for supporting strategic decision-making in enterprises // Biznes-informatika, 2007. №1. P. 29–35.

3. Sorokoletov P.V. Building intelligent decision support systems // Izvestia UFU. Tehnicheskie nauki. P. 117 – 124.