**Висновки.** Даний підхід дозволить на практиці значно прискорити дослідження по виявленню об'єктів підвищеної небезпеки.

## ЛІТЕРАТУРА

1. Закон України «Про об'єкти підвищеної небезпеки» 18.01.2001 р.
2. М. Назаров «Промышленная безопасность – вопрос международный» // Всеукраинский научно-технический журнал «Технополис». Вип. 9. Днепропетровск: 2004. – с.22.
3. Постанова Кабінету Міністрів України від 11.07.02. № 956. Порядок ідентифікації та обліку об'єктів підвищеної небезпеки.

**УДК 004.52; 004.56; 004.8; 519.8**

*Новожилова М.В., д-р физ.-мат. наук, зав. каф., ХГТУСА,*
*Овечко К.А., аспирант, ХГТУСА*

# МЕТОДЫ ВЫБОРА ВАРИАНТА ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРЕДУПРЕЖДЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

(представлено д-ром техн. наук Яковлевой Р.А.)

В работе предложена концепция инкапсуляции необходимого математического аппарата в состав разрабатываемой системы поддержки принятия решений по оптимальной структуре информационной подсистемы системы предупреждения чрезвычайных ситуаций

**Постановка проблемы.** Современная автоматизированная система предупреждения чрезвычайных ситуаций включает информационную подсистему как один из своих неотъемлемых элементов [1]. Поскольку нарушение целостности и нормального режима функционирования информационной подсистемы может привести к значительным потерям, сравнимым по величине с результатами стихийных бедствий и других чрезвычайных ситуаций, всё большее значение придается проблеме информационной

защиты автоматизированных систем (АС) [2], в том числе АС предупреждения чрезвычайных ситуаций (ЧС). Согласно действующего законодательства [3-5], АС – система, выполняющая автоматизированную обработку данных и включающая технические средства обработки данных, а также методы, процедуры и программное обеспечение. Неравномерное, спонтанное развитие АС, использование информационных структур, неподвластных руководству АС, человеческий фактор и прочие, делают защиту информации очень сложной и трудно формализуемой задачей.

Все перечисленные факты приводят к необходимости разработки средства поддержки принятия решения (ППР), которое облегчит работы по проектированию, внедрению и сопровождению информационной подсистемы системы предупреждения чрезвычайных ситуаций (ИС СПЧС). Одним из наиболее эффективных средств решения подобного класса задач являются экспертные системы (ЭС), поскольку позволяют объединять и копировать опыт множества экспертов и использовать его в решении сложных проблем.

**Анализ последних исследований и публикаций.** При написании статьи авторами был выполнен анализ существующих подходов по классификации компонентов АС, а также методов защиты информации; были исследованы модели представления знаний в интеллектуальных системах. Большой вклад в разработку методологии решения вопросов информационной безопасности внесли исследования Герасименко В.А., Гроувера Д., Мельникова Ю.М., Мэдника С., Осовецкого Л.Г., Расторгуева С.П., Сяо Д., Хоффмана Л., Щербакова А.Ю. [6]. В области искусственного интеллекта и экспертных систем основополагающими стали работы таких ученых как: Минский М., Поспелов Д.А., Попов Е.В., Уотермен Д., Нейлор К. и др. [7]. Однако, как показал анализ литературных источников, вопросам разработки оптимальной структуры информационной подсистемы системы предупреждения чрезвычайных ситуаций уделено недостаточно внимания.

**Постановка задачи и ее решение.** Цель работы – в рамках решения задачи по созданию ЭС разработать методологию выбора варианта построения ИС СПЧС. Концептуальная модель ЭС, режим извлечения новых знаний и этапы структурирования и параметрической идентификации были рассмотрены авторами в статье [8].

В данном режиме осуществляется проектирование, конфигурирование, мониторинг и анализ состояния ИС СПЧС с использованием ЭС (рис. 1):

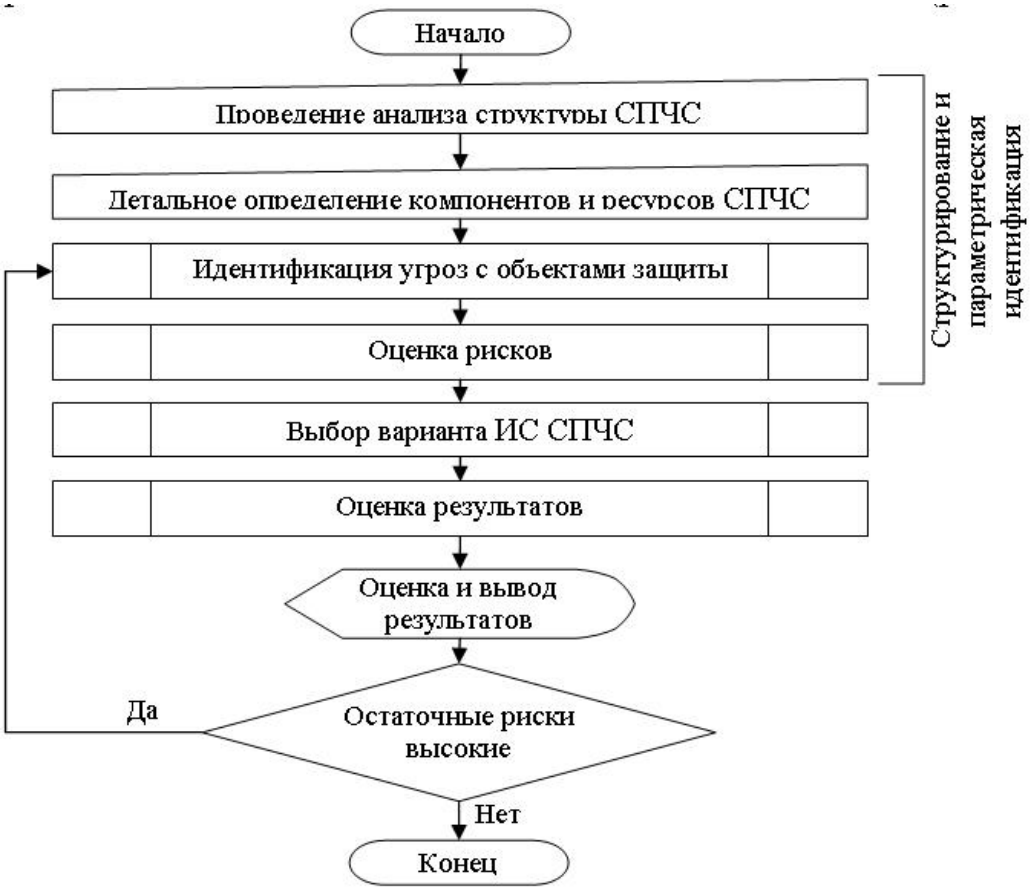


**Рис. 1 – Схема алгоритма работы ЭС с пользователем**

После выполнения структурирования и параметрической идентификации выполняется выбор варианта построения ИС СПЧС.

*Выбор варианта построения ИС СПЧС.* Система предупреждения чрезвычайных ситуаций должна функционировать на всех стадиях жизненного цикла (ЖЦАС) защищаемого объекта, на всех технологических этапах обработки информации и во всех режимах функционирования, включая разработку, внедрение, эксплуатацию и вывод из эксплуатации [**Ошибка! Закладка не определена.**].

Дискретная модель решаемой задачи максимизации величины предотвращенных убытков $U$ на протяжении всего ЖЦАС может быть представлена следующим образом

$$U^0 = \max_{W_t} \sum_{t=0}^{T} \rho_t W_t(Conf) \quad (1)$$

где $\rho_t$ - коэффициент дисконтирования в период времени $t$; $W_t$ – величина предотвращенных убытков за период времени $t$, $Conf$ – вектор конфигурации СПЧС, определяющий наличие различных средств защиты, а также настройки объектов АС и СПЧС, $T < \infty$ – конечный (терминальный) момент функционирования АС.

Расстояния между моментами времени $t$ могут устанавливаться через одинаковые промежутки времени, определенные возможностями предприятия, или назначаться ответственным лицом. В оптимальном случае они должны быть реакцией на изменения в информационной среде, влияющие на эффективность функционирования ИС СПЧС. Такими изменениями могут быть [**Ошибка! Закладка не определена.**]: – установление нового оборудования или модернизация существующего, включение в состав АС новых компонентов; - установление новых систем жизнеобеспечения АС (сигнализации, вентиляции, пожаротушение, кондиционирование и др.); - проведение строительно-ремонтных работ; - организационные изменения в структуре АС, производственных процессах, процедурах обслуживания АС; - изменения в технологии обработки информации; - изменения в программном обеспечении; - любые изменения в составе и функциях СПЧС.

Структурная и параметрическая идентификация функционала $W_t$ в общем случае векторного, является сложной задачей, причем вид и количество частных критериев качества $w_{it}$ могут быть различными в разные моменты времени.

Для решения данной задачи прибегают к использованию опыта экспертов и существующих математических методов. ЭС моделирует деятельность эксперта по предотвращению ЧС в своей работе, используя знания из базы знаний и текущее состояние рабочей памяти (РП). Математический аппарат используется, когда база знаний не содержит других правил для текущего состояния РП. В этом случае в зависимости от имеющейся информации выбирается один из следующих подходов к решению сложившейся подзадачи: 1) методы теории игр; 2) математические методы решения многокритериальной задачи.

Вследствие разнообразия угроз и средств защиты выбор конфигурации СПЧС относится к классу NP-трудных задач. Применение продукционной модели, избавляет от необходимости полно-

го перебора и защищает от «комбинаторного взрыва». Правила продукций строятся на основании знаний экспертов и имеют следующий вид:

ЕСЛИ «Условие» ТО «Действие/Суждение» ПОТОМУ ЧТО «Объяснение».

*Методы теории игр* [9, 10]. Для решения задачи формируется дерево принятия решений (ДПР) из возможных последовательностей действий, оказывающих влияние на функционирование АС. После построения ДПР, проводится анализ результатов в терминальных вершинах ДПР, для каждого из участвующих в "игре" субъектов. Решением задачи, является оптимальная стратегия – последовательность действий со стороны СПЧС, приводящая к максимизации величины предотвращенного ущерба.

Преимуществами данного подхода являются высокая точность и обоснованность получаемого решения. К недостаткам следует отнести высокую трудоемкость и сложность получения информации для построения ДПР. Однако существует возможность решения этих проблем путем использования опыта экспертов для создания ДПР, включающего только наиболее важные из действия субъектов.

*Математические методы решения многокритериальной задачи*. Задачей данного подхода является выбор оптимальной технической реализации *(Conf)* СПЧС, максимизирующей величину предотвращенного ущерба $W_t(Conf)$ в период $t$ [11]. В общем виде она может быть представлена следующим образом:

$$Conf^{O} = \arg\max W(Conf) \qquad (2)$$

Решение задачи (2), как правило, разбивается на 3 этапа. Целью первых двух является аппроксимация функции *W(Conf)*.

1) На основании данных РП производится определение важности требований, предъявляемых к СПЧС с использованием одного из следующих методов: а) в первичных шкалах; б) производных шкалах. Выбор метода определяется: - наличием данных в РП; - сложностью получения данных в случае их отсутствия; - предпочтениями пользователя.

2) Использование методов выбора рационального варианта СПЧС на основе экспертной информации. На данном этапе выбор метода решения многокритериальной задачи определяется харак-

тером экспертной информации о степени предпочтения показателей (табл. 1).

**Таблица 1 – Выбор метода решения многокритериальной задачи**

| Экспертная информация о степени предпочтения показателей | Метод решения многокритериальной задачи |
|---|---|
| Отсутствует | Максиминный метод |
| Существует один главный показатель | Метод главного показателя |
| Показатели упорядочены по важности | Лексикографический метод |
| Определены весовые коэффициенты показателей | Методы результирующего показателя: аддитивный показатель, мультипликативный показатель, максиминный показатель. |

3) В зависимости от формы полученной аппроксимации функции *W(Conf)*, используются методы линейного и математического программирования, полный перебор вариантов, а также методы эвристического поиска с целью определения наиболее подходящего вектора технической реализации СПЧС.

*Оценка результатов использования СПЧС и затрат на её внедрение и содержание*. На данном этапе подводятся итоги внедрения (изменения конфигурации) СПЧС, которые включают: 1) предварительную оценку стоимости изменения конфигурации СПЧС; 2) оценку величины предотвращенного ущерба (в денежном или качественном выражении); 3) оценку остаточных рисков. Предлагается выход из ситуации, когда остаточные риски превышают предельно допустимые, путем изменения параметров ограничений введенных пользователем в ЭС и проведением нового расчета по выбору состава средств и мероприятий защиты.

**Выводы.** Разработка ЭС для проведения работ по созданию СПЧС дает возможность эффективно отслеживать изменения в АС и реагировать на них как на стадии проектирования СПЧС, так и на стадии её эксплуатации. Практическая значимость работы состоит в возможности применения предложенного подхода по использованию эвристических методов выбора конфигурации СПЧС для проведения дальнейших исследований по проектированию и

реализации на языке Clips гибридного инструментария ППР-ЭС СПЧС.

## ЛИТЕРАТУРА


1. Сидоров В.И. Исследования по промышленной безопасности в рамках ГНТП «Безопасность» // Проблемы безопасности и чрезвычайных ситуаций. – М.: ВИНИТИ, №4, 2003. – С.62-68.
2. НД ТЗІ 1.1-002-99. "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу". - 1999 р. - N 22.
3. Закон України "Про захист інформації в автоматизованих системах". від 05.07.1994 р. N 80/94-ВР.
4. Закон України про внесення змін до Закону України "Про захист інформації в автоматизованих системах" від 31.05.2005 р. N 2594-IV.
5. НД ТЗІ 3.7-003-05. "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" від 08.11.2005р. N 125.
6. Домашев А.В.,Попов В.О.,Правиков Д.И.,Прокофьев И.В.,Щербаков А.Ю. "Программирование алгоритмов защиты информации" –М.: Нолидж, 2000.
7. Поспелов Д.А. Моделирование рассуждений. Опыт анализа мыслительных актов. - М.: Радио и связь, 1989. - 184 с.
8. Новожилова М.В., Овечко К.А. "Структура экспертной системы построения комплексных систем защиты информации на виртуальных объектах строительства" // Науковий вісник будівництва. – Харків:ХДТУБА. – вип..38, 2006. – С.75-81.
9. Новожилова М.В., Овечко К.А. "Методы игрового моделирования вопросов защиты информации." // Міжнародна науково-практична конференція „Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій", Запоріжжя, ЗНТУ, 2006.
10. Fudenberg D., Tirole J. Game Theory. Cambridge, MA: MIT Press. 1991.
11. Домарев В.В. "Безопасность информационных технологий. Системный подход": -К.: ООО "ТИД "ДС", 2004.