

---

---

# ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.5

<https://doi.org/10.47533/2024.1606-146X.01>

**С. А. АДИЛЖАНОВА<sup>1\*</sup>, Л. Ш. ЧЕРИКБАЕВА<sup>1</sup>, М. Ж. САКЫПБЕКОВА<sup>1</sup>,  
Г. А. ТЮЛЕПБЕРДИНОВА<sup>1</sup>, Б. Д. ШАРИПОВА<sup>2</sup>, В. А. ЛАХНО<sup>3</sup>**

<sup>1</sup>Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;

<sup>2</sup>Алматинский технологический университет, Алматы, Казахстан;

<sup>3</sup>Национальный университет биоресурсов и природопользования Украины  
[asaltanat81@gmail.com](mailto:asaltanat81@gmail.com), [lailash01@gmail.com](mailto:lailash01@gmail.com), [sakypbekova.meruyert@gmail.com](mailto:sakypbekova.meruyert@gmail.com),  
[tyulepberdinova@gmail.com](mailto:tyulepberdinova@gmail.com), [Birjzn2103@mail.ru](mailto:Birjzn2103@mail.ru), [lva964@gmail.com](mailto:lva964@gmail.com)

## КОНЦЕПТУАЛЬНОЕ ПРОЕКТИРОВАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ЗАДАЧИ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ СТОРОНЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

*В статье рассматривается система поддержки принятия решений в процессе распределения ресурсов стороны защиты информации для конкретного объекта информатизации, которая создается с целью ее использования любыми заинтересованными лицами во всех учреждениях или предприятиях, для которых актуальна задача поиска рациональной стратегии распределения ресурсов стороной защиты в условиях роста количества и сложности деструктивных воздействий на информационные ресурсы со стороны компьютерных злоумышленников. Выбор рациональной стратегии динамического распределения ресурсов стороны защиты объектов информатизации реализован с помощью: программной реализации аналитических моделей, использования экспертных подсистем систем; генерации сценариев путем комбинации различных моделей, заданных лицом, принимающим решение, или взятых из базы знаний система поддержки принятия решений.*

**Ключевые слова:** система поддержки принятия решений, кибербезопасность, объекты информатизации.

**Введение.** Система поддержки принятия решений призвана решить следующие задачи: создание баз знаний и баз данных, баз по различным ситуациям, связанным с выбором стратегии распределения ресурсов стороны защиты информации, разработка программного обеспечения для ведения единого электронного архива стратегий динамического распределения ресурсов стороны защиты объекты информатизации с разграничением доступа пользователей; создание единого информационного пространства в сфере учета рациональных стратегий распределения ресурсов стороны защиты информации, обеспечения информационного взаимодействия между под-

---

\* E-mail корреспондирующего автора: [asaltanat81@gmail.com](mailto:asaltanat81@gmail.com)

системами, системами поддержки принятия решений за счет внутренней стандартизации форматов данных и протоколов обмена; обеспечение системности, комплексности и согласованности развития информатизации задачи распределения ресурсов стороны защиты информации с использованием традиционных форм и методов сопровождения и контроля.

**Методика и результаты исследования.** Основные функции системы поддержки принятия решений для программ информационной и кибернетической безопасности обычно регламентируют исходя из необходимости соблюдения: принципов комплексного анализа проблематики кибербезопасности; возможностей комбинирования формальных и неформальных методов, используемых в процессе поддержки принятия решений; принципов достоверности и актуальности информации, касающейся текущего состояния проблемы. При этом как правило используют всевозможные отчеты, статистические данные, аналитические обзоры, а также данные, получаемые от подсистем мониторинга; принципов автоматизированного выбора методов и моделей для интеллектуализации поддержки принятия решений; принципов дальнейшего развития состояний системы поддержки принятия решений; принципов динамического управления системы поддержки принятия решений с целью повышения эффективности ее функционирования и обоснованности получаемых рекомендаций и выводов, которые могут быть использованы лицом, принимающим решение, в процесс выработки управляющих воздействий; потенциала модулей анализа, оперативного управления и контроля над решаемой задачей [1].

Для обеспечения полноценного функционирования системы поддержки принятия решений должна, как правило, включать в себя следующие основные модули и подсистемы (см. рис. 1).

1. Модули базы данных, базы знаний, базы моделей и правил, используемых для принятия решения.

2. Систему управления интерфейсом, которая проектируется исходя из архитектуры система поддержки принятия решений – локальная или клиент-серверная.

3. Другие модули и подсистемы, необходимость, которых продиктована спецификой предметной области.

Система поддержки принятия решений должна обеспечивать следующие виды поддержки принятия решений: экспертная поддержка; автоматизированный вывод решения; комбинированное решение.

Ядром системы поддержки принятия решений является база знаний. В данной предметной базе знаний будут аккумулироваться знания экспертов в задачах динамического распределения ресурсов стороны защиты информации. Знания целесообразно представить в формате эвристических правил.

Обучение и накопления новых знаний в базы знаний происходит следующим образом: при рассмотрении конкретной задачи динамического распределения ресурсов стороны защиты информации формируется правило, которое обеспечивает ее решение; разработанные правила в зависимости от специфики конкретной задачи помещаются в базу правил.

Поиск необходимого правила в базе правил системы поддержки принятия решений реализует, например, на основе семантических моделей.

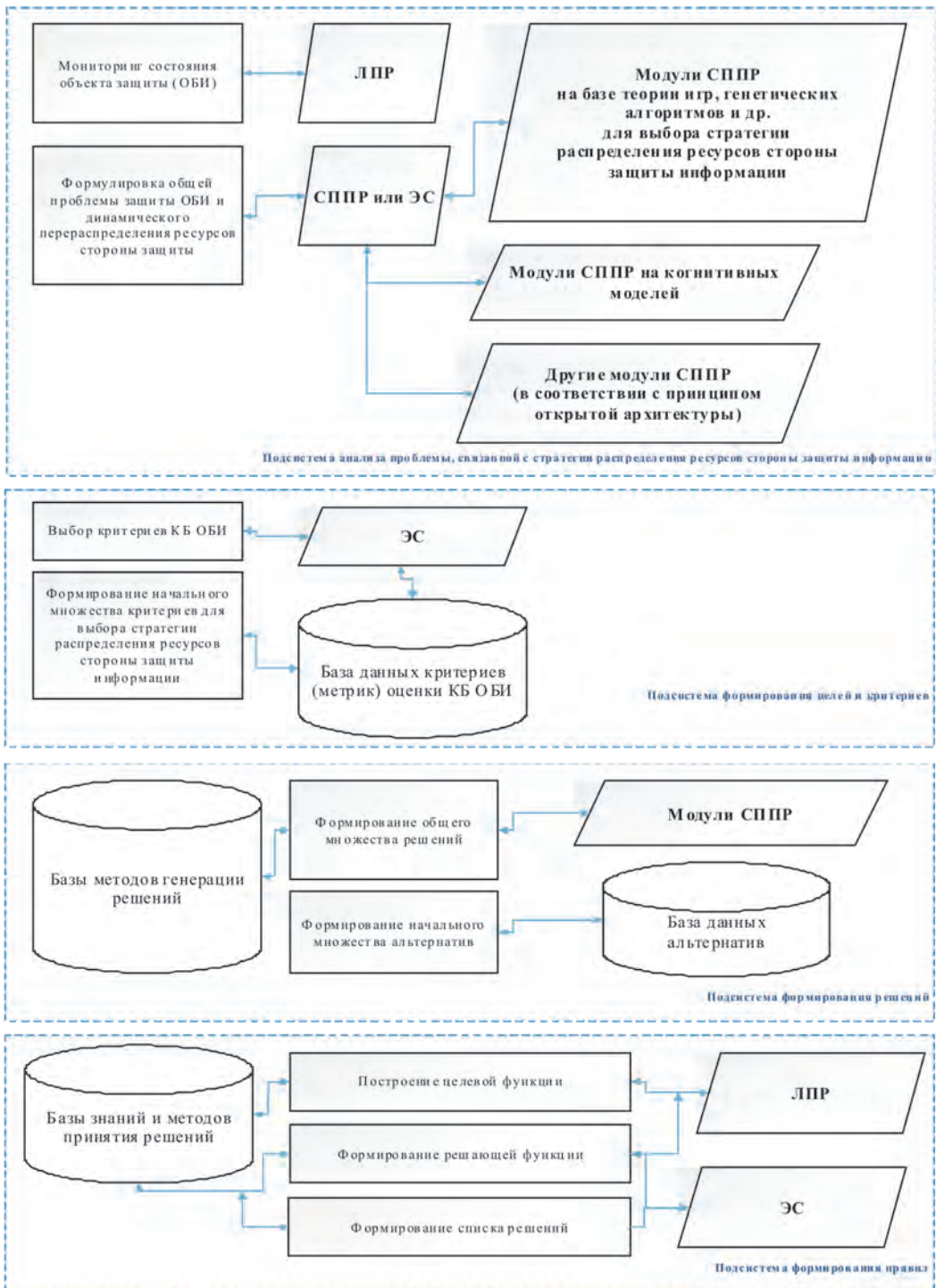


Рисунок 1 – Архитектура системы поддержки принятия решений, касающихся выбора рациональной стратегии распределения ресурсов стороны защиты информации

Блок-схема алгоритма функционирования подсистемы «Анализ проблем и рисков динамического распределения ресурсов стороны защиты информации объекта информатизации» представлена на рис. 2.

Существует четыре класса наиболее распространенных проблем при динамическом распределении ресурсов стороны защиты информации:

1. Стандартные проблемы. Проблемы этого класса, как правило, требуют применения инструкций, установленных лицом, принимающим решения.

2. Хорошо структурированные проблемы. Проблемы этого класса имеют количественные характеристики и показатели. Для решения подобного класса проблем, как правило, используют экономико-математические методы.

3. Плохо структурированные проблемы. Проблемы этого класса имеют не только количественные, но и качественные характеристики. Для решения подобных проблем необходимо задействовать в система поддержки принятия решений методы системного анализа.

4. Неструктурированные проблемы. Решение подобных проблем влечёт за собой необходимость привлечения экспертов в конкретной предметной области [2].

Подсистема «Анализ проблем и рисков для динамического распределения ресурсов стороны защиты информации объекта информатизации» должна обеспечивать поиск и формулирование проблемы с целью ее дальнейшего решения. К основным направлениям функционирования данной подсистемы можно отнести:

мониторинг объектов динамического распределения ресурсов стороны защиты информации;

определение количественных критериев и показателей для динамического распределения ресурсов стороны защиты информации объекта информатизации;

определение источников проблем с реализацией динамического распределения ресурсов стороны защиты информации объекта информатизации на основе аргументов;

выбор метода формулировки проблемы, связанной с динамическим распределением ресурсов стороны защиты информации объекта информатизации;

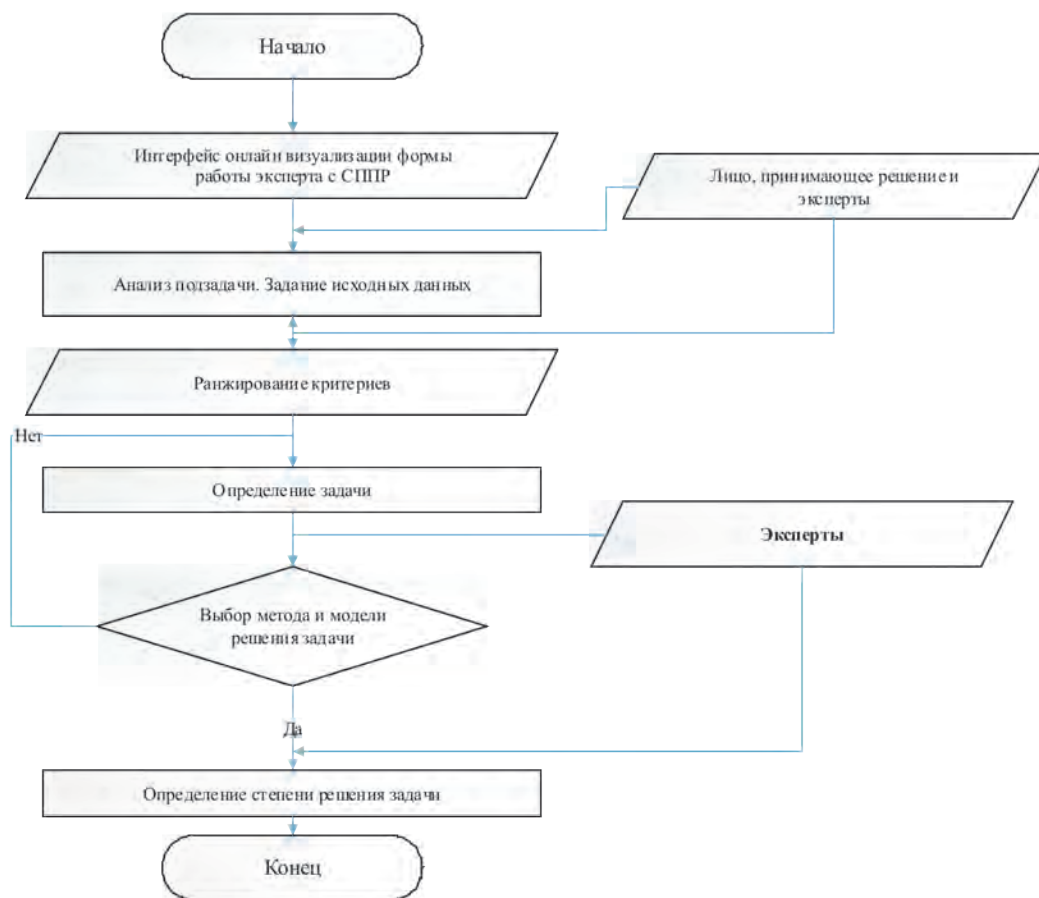
формулировка общей проблемы;

определение степени неопределенности проблемы;

определение отдельных задач в рамках общей проблемы.

После определения проблемы необходимо сформировать перечень целей и систему критериев эффективности реализации динамического распределения ресурсов стороны защиты информации объекта информатизации. Это необходимо для последующей оценки проблемы и поиска путей ее дальнейшего решения. Для этого в система поддержки принятия решений существует отдельная подсистема – «Формирование целей и системы критериев для оценивания стратегии динамического распределения ресурсов стороны защиты информации объекта информатизации», см. рис. 3.

В ходе формирования цели или множества целей, которых необходимо достигнуть в ходе динамического распределения ресурсов стороны защиты информации объекта информатизации, могут возникать различные задачи. Эти задачи могут: объединяться; противоречить одна другой; быть взаимоисключающими и т.д. [3]



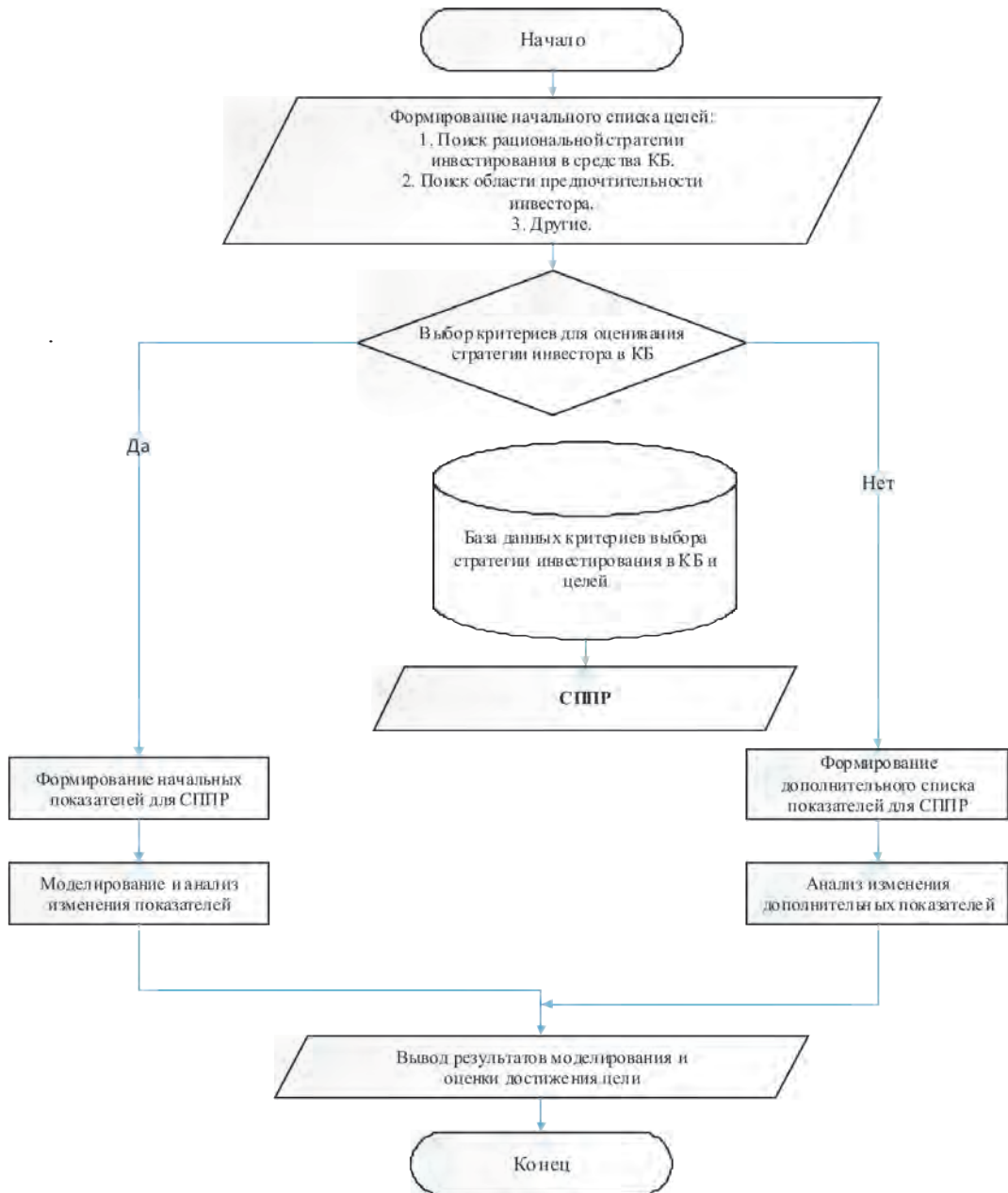
**Рисунок 2** – Блок-схема алгоритма функционирования подсистемы «Анализ проблем и рисков для задачи динамического распределения ресурсов стороны защиты информации объекта информатизации»

Для столь сложной проблематики как поиск рациональной стратегии динамического распределения ресурсов стороны защиты информации объекта информатизации, формирование целей и системы критериев оценки эффективности, целесообразно разделять на: принципиально новые новаторские цели, которые формулируют эксперты; типичные цели, по аналогии с целями, которые возникали в аналогичных ситуациях; комбинированные цели, генерация которых доступна для конкретной системы поддержки принятия решений. Наиболее эффективным способом формирования целей и критериев эффективности являются программные системы во взаимодействии с экспертами.

Для дальнейшего анализа проблемы выбора рациональной стратегии динамического распределения ресурсов стороны защиты информации объекта информатизации, необходимо сформировать альтернативные варианты решений.

Эти альтернативные варианты будут формироваться в подсистеме «Формирование решений, принимаемых в процессе динамического распределения ресурсов стороны защиты информации объекта информатизации». [4]

Формирование возможных решений для задач поиска рациональных стратегий динамического распределения ресурсов стороны защиты объекта информатизации, в настоящий момент реализовано на основе применения математического аппарата теории игр или динамического программирования.



**Рисунок 3** – Блок-схема алгоритма функционирования подсистемы «Формирование целей и системы критериев для оценивания стратегии динамического распределения ресурсов стороны защиты информации объекта информатизации»

Процесс формирования решений в система поддержки принятия решений разделен на два вида:

новаторские решения, которые пока система поддержки принятия решений работать не в состоянии (например, модель для ситуации отсутствует пока в базе знаний);

решения, основанные на типовых сценариях, т.е. используя аналогию с известными решениями.

Экспертная подсистема система поддержки принятия решений является одним из основных приложений искусственного интеллекта и предназначена для решения задач, относящихся конкретной предметной области, знания о которой хранятся в базы знаний.

Основным назначением экспертной подсистемы, как основы система поддержки принятия решений для поиска рациональной стратегии динамического распределения ресурсов стороны защиты объектов информатизации, является ориентация на решение различных задач, на основе ранее описанных в [5] моделей.

Экспертная подсистема обеспечивает выработку и оценку возможных альтернатив стратегии динамического распределения ресурсов стороны защиты объекта информатизации пользователем за счет знаний, которые были получены от специалистов-экспертов.

Экспертная подсистема состоит из: базы знаний, которая предназначена для хранения исходных и промежуточных фактов, накопленных в ходе решения задачи. Также в базы знаний хранятся модели и правила манипулирования моделями. Возможно также проектирование отдельной базы правил, если правил, используемых в процессе решения задачи выбора рациональной стратегии динамического распределения ресурсов стороны защиты объектов информатизации, становится достаточно много;

блока решения задач, связанных с выбором рациональной стратегии динамического распределения ресурсов стороны защиты объекта информатизации. Данный блок будет обеспечивать реализацию последовательности выполнения правил для решения конкретной задачи динамического распределения ресурсов стороны защиты объекта информатизации на основе критериев и правил, хранящейся в базы данных и базы знаний;

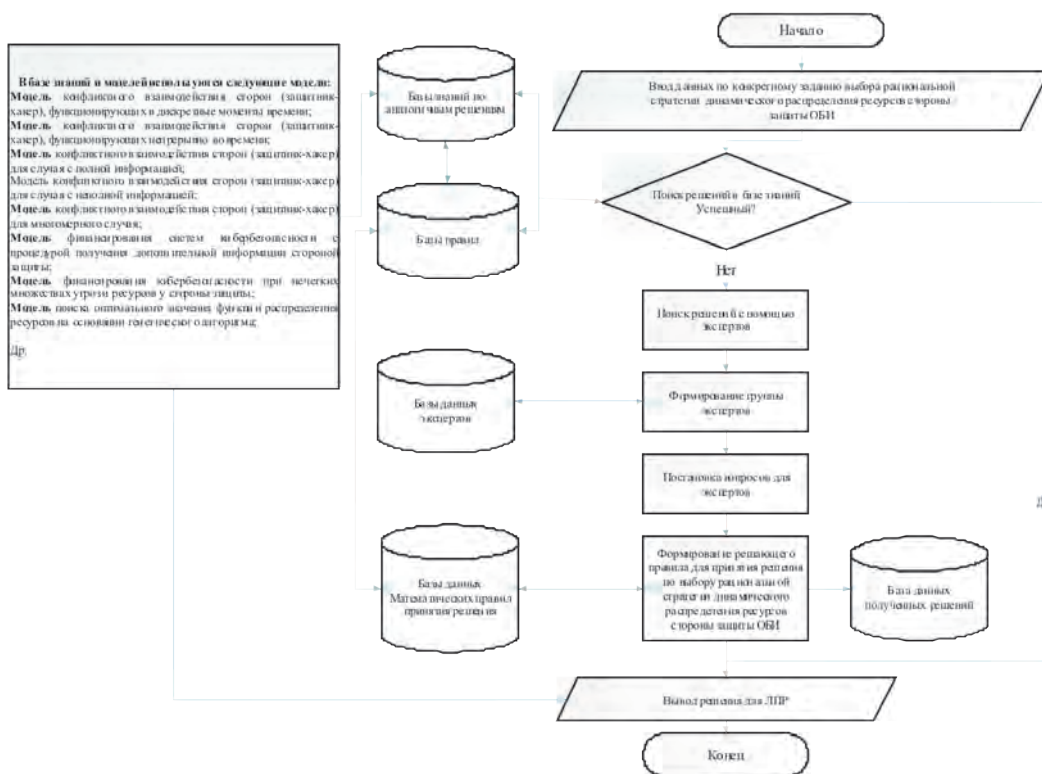
подсистемы пояснения, которая позволит лицу, принимающему решение, разобраться в причине такого решения, которое предложено системой поддержки принятия решений;

модуль формирования правил, который предназначен для добавления в базы знаний новых правил и/или их модификаций;

диалогового интерфейса, который призван реализовать удобный диалог пользователя с подсистемой и система поддержки принятия решений в целом.

Последовательность действий функционирования алгоритма, показанного на рис. 4, заключается в следующем.

При получении информации о задачах происходит поиск решения в существующей базе данных. Если аналогичная ситуация встречалась ранее и определены правила принятия решений, то однозначно определяется решение и по данной задаче.



**Рисунок 4** – Блок-схема алгоритма функционирования экспертной подсистемы для проектируемой системы поддержки принятия решений

Если решения для начальной постановки задачи отсутствует, то формируется проблемно-ориентированный экспертная группа. Далее происходит рассылка экспертам вопросов, которые помогут в дальнейшем сформировать новое решающее правило. Эксперты формируют решающее правило для выбора лучшего альтернативного варианта и соответствующей подсистемы системы поддержки принятия решений. На следующем этапе определяется выбор наилучшего решения. В случае соответствия решения исходной постановки задачи правило записывается в базы данных правил, а решение – в базы знаний.

Данный алгоритм функционирования система поддержки принятия решений обеспечивает возможность анализа и нахождения решения для любой задачи, связанной с выбором стратегии динамического распределения ресурсов стороны защиты объектов информатизации.

## ЛИТЕРАТУРА

- 1 Баранова, Е. К. (2015). Методики анализа и оценки рисков информационной безопасности. Образовательные ресурсы и технологии, (1 (9)). С. 73-79.
- 2 Грищук, Р. В. (2012). Использование дифференциальных игр для оптимизации управления в системах защиты информации / Грищук Р.В., Хорошко В.А., Хохлачева Ю.Е. Современная защита информации (2), с. 21–26.



3 Lakhno, V., Akhmetov, B., Malyukov, V., Kartbayev, T. S. (2018). Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium of a bilinear multistep quality game with several terminal surfaces. *International Journal of Electronics and Telecommunications*, 64(4), 467-472.

4 Котенко, И. В., &Новикова, Е. С. (2013). Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей. Вопросы защиты информации, (3), 33-42.

5 Гришук Р.В. Теоретические основы моделирования процессов нападения на информацию методами теории дифференциальных игр и дифференциальных преобразований: Монография / Р.В. Гришук. – Житомир: Рута, 2010. – 280 с.

## REFERENCES

1 Baranova, E. K. (2015). Metodiki analiza i ocenki riskov informacionnoj bezopasnosti. *Obrazovatelnye resursy i tehnologii*, (1 (9)). S. 73-79.

2 Grishuk, R. V. (2012). Ispolzovanie differencialnyh igr dlya optimizacii upravleniya v sistemah zashity informacii / Grishuk R.V., Horoshko V.A., Hohlacheva Yu.E. *Sovremennaya zashita informacii* (2), s. 21–26.

3 Lakhno, V., Akhmetov, B., Malyukov, V., Kartbayev, T. S. (2018). Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium of a bilinear multistep quality game with several terminal surfaces. *International Journal of Electronics and Telecommunications*, 64(4), 467-472.

4 Kotenko, I. V., &Novikova, E. S. (2013). Metodiki vizualnogo analiza v sistemah upravleniya informacionnoj bezopasnostyu kompyuternyh setej. *Voprosy zashity informacii*, (3), 33-42.

5 Grishuk R.V. Teoreticheskie osnovy modelirovaniya processov napadeniya na informaciyu metodami teorii differencialnyh igr i differencialnyh preobrazovanij: Monografiya / R.V. Grishuk. – Zhitomir: Ruta, 2010. – 280 s.

**С. А. АДИЛЖАНОВА<sup>1</sup>, Л. Ш. ЧЕРИКБАЕВА<sup>1</sup>, М. Ж. САКЫПБЕКОВА<sup>1</sup>,  
Г. А. ТЮЛЕПБЕРДИНОВА<sup>1</sup>, Б. Д. ШАРИПОВА<sup>2</sup>, В. А. ЛАХНО<sup>3</sup>**

<sup>1</sup>әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан;

<sup>2</sup>Алматы технология университеті, Алматы, Қазақстан;

<sup>3</sup>Биоресурстар және қоршаған ортаны басқару ұлттық университеті,  
Киев, Украина

## ТҰЖЫРЫМДАМАЛЫҚ ЖОБАЛАУ АҚПАРАТТЫ ҚОРҒАУ ТАРАПЫНЫҢ РЕСУРСТАРЫН АҚПАРАТТАНДЫРУ ОБЪЕКТИЛЕРІНДЕ БӨЛУ МІНДЕТІ ҮШІН ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ ЖҮЙЕСІ

Мақалада белгілі бір ақпараттандыру объектісі үшін ақпаратты қорғау тарапының ресурстарын бөлу процесінде шешімдер қабылдауды қолдау жүйесі қарастырылады, оны компьютерлік зиянкестер тарапынан ақпараттық ресурстарға деструктивті әсерлердің саны мен күрделілігінің өсуі жағдайында қорғаныс тарапының ресурстарды бөлудің ұтымды стратегиясын іздеу міндеті өзекті болып табылатын барлық мекемелерде немесе кәсіпорындарда кез келген мүдделі тұлғалар пайдалану мақсатында құрылады. Ақпараттандыру объектілерінде қорғаныс тарапының ресурстарын динамикалық бөлудің ұтымды стратегиясын таңдау мыналардың көмегімен жүзеге

асырылады: аналитикалық модельдерді бағдарламалық іске асыру, жүйелердің сараптамалық ішкі жүйелерін қолдану арқылы орындалады; шешім қабылдаушы берген немесе білім базасынан алынған әртүрлі модельдердің жиынтығы арқылы сценарийлерді құру арқылы шешім қабылдауды қолдау жүйесі.

**Түйін сөздер:** шешімдерді қолдау жүйесі, киберқауіпсіздік, ақпараттандыру объектілері.

**S. ADILZHANOVA<sup>1</sup>, L. CHERIKBAYEVA<sup>1</sup>, M. SAKYPBEKOVA<sup>1</sup>,  
G. TYULEPBERDINOVA<sup>1</sup>, B. SHARIPOVA<sup>2</sup>, V. LAKHNO<sup>3</sup>**

<sup>1</sup>*Al-Farabi Kazakh National University, Almaty, Kazakhstan;*

<sup>2</sup>*Almaty Technological University;*

<sup>3</sup>*National University of Bioresources and Environmental Management of Ukraine*

### **CONCEPTUAL DESIGN OF A DECISION SUPPORT SYSTEM FOR THE TASK OF INFORMATION PROTECTION RESOURCE ALLOCATION AT INFORMATIZATION OBJECTS**

*The article considers a decision support system in the process of allocating resources of the information protection side for a specific object of informatization is created for the purpose of its use by any interested persons in all institutions or enterprises for which the task of finding a rational strategy for resource allocation by the protection side is relevant in conditions of increasing number and complexity of destructive impacts on information resources by computer intruders. The choice of a rational strategy for the dynamic allocation of resources on the part of the protection of informatization objects is implemented using: software implementation of analytical models, performed by using expert subsystems of systems; by generating scenarios by combining various models set by the decision maker or taken from the knowledge base of the decision support system.*

**Key words:** decision support system, cybersecurity, informatization objects.