ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ. БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ ИНФОРМАТИКА. МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ. ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ

МРНТИ 50.47
УДК 004.056

https://doi.org/10.51889/2020-4.1728-7901.25

С.А. Адилжанова[1], Г.А. Тюлепердинова[1], М.Ж. Сакыпбекова[1], Н.А. Текесбаева[2]

[1]Казахский Национальный университет имени аль - Фараби, г.Алматы, Казахстан
[2]Казахский Национальный педагогический университет имени Абая, г.Алматы, Казахстан

АНАЛИЗ МАТЕМАТИЧЕСКИХ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ И ДИНАМИЧЕСКОГО УПРАВЛЕНИЯ РЕСУРСАМИ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Аннотация

В статье рассматривается возможность модификации генетического алгоритма (ГА) для решения задач выбора, оптимизации и управления динамической конфигурацией средств защиты информации для цепи защиты информационно-коммуникационных систем (ИКС). Научная новизна работы заключается в том, что ГА рекомендует использовать суммарную стоимость рисков потери информации, а также показатели затрат для каждого класса систем защиты информации в качестве критерия оптимизации состава системы защиты информации. Генетический алгоритм рассматривается как разновидность задачи, связанной с множественным выбором при оптимизации выбора информационного содержания информационной безопасности и решении задач динамического управления ресурсами кибербезопасности. В данной концепции оптимизация размещения системы защиты информации по цепи защиты рассматривается как модификация задачи комбинированного рюкзака.

Предлагаемый подход позволяет рассчитывать различные версии программно-аппаратных ИС и их комбинаций для ИКС, но и динамически управлять ГА с существующими моделями и алгоритмами для оптимизации состава цепочек кибербезопасности ИКС и ресурсов кибербезопасности различных информационных объектов. Такое сочетание моделей и алгоритмов позволит быстро восстановить защиту ИКС, настроив профили в соответствии с классами новых угроз и кибератак.

Ключевые слова: система поддержки принятия решений, средства защиты информации, многокритериальная оптимизация, задача рюкзака, генетический алгоритм.

Abstract

ANALYSIS OF MATHEMATICAL METHODS OF MULTI-CRITERIA OPTIMIZATION AND DYNAMIC MANAGEMENT OF CYBERSECURITY RESOURCES OF INFORMATIZATION OBJECTS

Adiljanova S.A. [1], Tulepberdinova G.A. [1], SakypbekovaM J. [1], Tekesbayeva N.A. [2]
[1] al-Farabi Kazakh National University, Almaty, Kazakhstan
[2] Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

The article discusses the possibility of modifying the genetic algorithm (GA) to solve the problems of selection, optimization and management of the dynamic configuration of information security means for the security chain of information and communication systems (ICS). The scientific novelty of the work lies in the fact that GA recommends using the total cost of information loss risks, as well as cost indicators for each class of information security systems as a criterion for optimizing the composition of the information security system. The genetic algorithm is considered as a kind of problem associated with multiple choice when optimizing the choice of information content of information security and solving problems of dynamic management of cybersecurity resources. In this concept, the optimization of the placement of the information security system along the security chain is considered as a modification of the combined backpack problem.

The proposed approach allows not only to quickly calculate various versions of software and hardware information systems and their combinations for ICS, but also to dynamically manage the proposed algorithm with existing models and algorithms to optimize the composition of ICS cybersecurity chains and cybersecurity resources of various

information objects. It is possible that such a combination of models and algorithms will quickly restore ICS protection by configuring profiles in accordance with the classes of new threats and cyber attacks.

Keywords: decision support system, information security means, multicriteria optimization, knapsack problem, genetic algorithm.

Аңдатпа

С.А. Адилжанова[1], Г.А. Тюлепбердинова[1], М.Ж. Сакыпбекова[1], Н.А. Текесбаева[2]
[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[2]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан

АҚПАРАТТАНДЫРУ ОБЪЕКТІЛЕРІНІҢ КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН КӨП ӨЛШЕМДІ ОҢТАЙЛАНДЫРУ МЕН ДИНАМИКАЛЫҚ БАСҚАРУДЫҢ МАТЕМАТИКАЛЫҚ ӘДІСТЕРІН ТАЛДАУ

Мақалада ақпараттық-коммуникациялық жүйелердің (АКЖ) қауіпсіздік контуры үшін ақпараттық қауіпсіздік құралдарын (АҚҚ) таңдау, оңтайландыру және динамикалық конфигурация басқару мәселелерін шешу үшін генетикалық алгоритмді (ГА) өзгерту мүмкіндіктері қарастырылған. Жұмыстың ғылыми жаңалығы ГА-да ақпараттық қауіпсіздік жүйесінің құрамын оңтайландыру критерийі ретінде ақпараттың жоғалуынан болатын тәуекелдердің жалпы құнын, сондай-ақ ақпараттық қауіпсіздік жүйелерінің әр класы бойынша шығындар индикаторларын қолдану ұсынылатындығында. Ақпараттық қауіпсіздік ақпаратының құрамын таңдауды оңтайландыру және киберқауіпсіздік ресурстарын динамикалық басқару мәселелерін шешуде генетикалық алгоритм мульти таңдаумен байланысты проблеманың вариациясы ретінде қарастырылады. Бұл тұжырымдамада ақпараттық қауіпсіздік жүйесін АКЖ қорғаныс контуры бойына орналастыруды оңтайландыру комбинациялық рюкзак проблемасының модификациясы ретінде қарастырылады. Ұсынылып отырған тәсіл аппараттық және бағдарламалық қамтамасыздандырудың ақпараттық жүйелеріне арналған әртүрлі нұсқаларды және АКЖ үшін олардың комбинацияларын жылдам санауды жүзеге асыруға ғана емес, сонымен қатар ұсынылған алгоритмді қолданыстағы модельдермен және АКЖ киберқауіпсіздік тізбектерінің құрамын оңтайландыру алгоритмдерімен және әртүрлі ақпараттық объектілердің киберқауіпсіздік қорларын динамикалық басқарумен біріктіруге мүмкіндік береді. Мүмкін, модельдер мен алгоритмдердің мұндай тіркесімі жаңа қауіптер мен кибершабуылдардың кластарына сәйкес профильдерін реттей отырып, АКЖ қорғанысын тез қалпына келтіруге мүмкіндік береді.

Түйін сөздер: шешімдерді қолдау жүйесі, ақпараттық қауіпсіздік құралдары, мультиобъективті оңтайландыру, рюкзактар мәселесі, генетикалық алгоритм.

Введение

Совершенствование любых процессов или явлений всегда базируется на идентификации критериев, которые их характеризуют. Это, в свою очередь, является предпосылкой адекватности формирования путей обеспечения оптимизации исследуемых процессов или явлений.

Подобные многоконтурные системы, содержат большое количество объектов,отвечающих за локальные задачи по защите целостности, конфиденциальности и доступности информационных ресурсов для обеспечения информационной безопасности (ОБИ). Исследование подобных многоконтурных систем, которые на протяжении всего жизненного цикла ОБИ, могут включать в себя самые разнообразные конфигурации аппаратных, программных, организационных средств и методов защиты, представляет сложную задачу. Как правило на стадии проектирования или модернизации подобных многоконтурных систем защиты информации (СЗИ) необходимо решать задачи, связанные с многокритериальной оптимизацией состава средств защиты. При этом следует учитывать и аспекты динамического управления ресурсами защиты. Подобные многокритериальные задачи,прежде всего, следует решать применяя различные методы математического моделирования и многокритериальной оптимизации состава комплексов многоконтурной защиты ОБИ. В этой ситуации, математические модели для решения подобных многокритериальных оптимизационных задач должны отвечать двум противоречивым требованиям:

1) в наибольшей степени отражать свойства системы;

2) избегать при этом излишней детализации, которая может осложнить получение конечных результатов.

Также необходимо учитывать следующее обстоятельство. Проблематика динамического управления ресурсами стороны защиты ОБИ это не только сугубо техническая задача, которая решается путем увеличения числа компонентов защиты в контурах кибербезопасности ОБИ. Но это также и управленческая задача. Причем вторая составлявшая задачи, связана с таким понятием как менеджмент информационная безопасность и кибербезопасность (ИБ и КБ) [1]. Основной задачей менеджмента ИБ и КБ является оптимизация не только технических, но экономических показателей эффективности функционирования СЗИ для ОБИ.

Методы и исследования

Исследованиям вопроса оптимального распределения ресурсов в области ЗИ для ОБИ посвящено достаточно много работ как зарубежных ученных [2, с. 55], так и ученых Республики Казахстан [3, с. 91]. Тематика исследований в этой области актуальна и востребована на различных международных научных конференциях [4, 87].

Так, в работе [5] проанализированы задачи оптимизации расходов на ИБИКС. По сути речь идет о решении задачи многокритериального выбора. Предложена интерактивная процедура выбора рационального варианта распределения расходов на СЗИ для ОБИ.

В работе [6] приведены шесть различных формулировок задачи оптимального распределения ресурсов между различными функциями управления механизмами, обеспечивающими ИБ и КБ для ОБИ. Предлагаются постановки задачи распределения ресурсов, предназначенные для применения как на стадии проектирования систем, обеспечивающих ИБ ОБИ, так и на стадиях совершенствования и развития контуров ИБ. Авторы выделяют семь основных функций обеспечения защиты информации (ЗИ) и предлагают два подхода к детализации и формализации распределения средств между различными функциями СЗИ. Первый подход основан на учете состава и количества средств СЗИ. Второй подход базируется на анализе обобщенных закономерностей и связях между вложенными в процесс обеспечения ОБИ средствами ЗИ и эффективностью их применения. В работе рассмотрены вероятные и стоимостные модели. Последние, из которых представляют значительный интерес для исследователей, уточняя физический смысл параметров задачи распределения ресурсов при вводе данных в предлагаемый авторами программный продукт.

В работе [7] рассматривается модель, в которой распределение ресурсов между объектами СЗИ предлагается выполнять на основе игровой модели и принципа равной защищенности объектов. Задача распределения ресурсов сформулирована как турнир двух игроков - защитника и нападающего с нулевой суммой. Каждый игрок решает задачи линейного программирования при фиксированном решении другого игрока. В работе предложено три алгоритма, которые могут применяться последовательно для гарантированного получения результата. Алгоритмы обоснованы математически, полученные результаты подтверждены тестовыми примерами и обобщены. Игровые модели распределения финансовых ресурсов, направленных на повышение информационной безопасности, также достаточно детально рассмотрены в работах [8, 45].

Большинство программных разработок, реализующих те или иные математические методы, является достаточно универсальными продуктами, которые позволяет решать множество задач в зависимости от подготовленных входных данных. Основной особенностью программного пакета,который описан в работе, является наличие интеллектуального агента, позволяющего выбрать наиболее эффективный по критерию количества вычислительных операций и времени выполнения алгоритм. При этом, весьма важно, что при построении СЗИ, учитывается и своевременное распределение ресурсов, которые работу обеспечивают долгосрочную функциональность СЗИ.

Работа ЛППс системой проходит в online-режиме с учетом требования размещения инструментария для решения задачи на «облачном» сервисе. Это позволяет пользователю, находить решение задачи минуя поиск необходимого программного обеспечения и его инсталляцию.

При подборе методов, которые должны были быть включены в пакет, следовало выполнить постановку задачи исследования, определить тип задачи и подготовить соответствующим образом входные данные. Перечень разделов, включенных в прототиппрограммного пакета для решения задачи по моделированию распределения ресурсов на СЗИ:

- раздел для решения классических задач распределения ресурсов (задача распределения ресурсов между предприятиями и задачи управления запасами);
- раздел для решения сетевых задач распределения ресурсов (задачи о поиске кратчайшего пути и о максимальном потоке);
- раздел для решения прикладных задач (включено задачу распределения денежных ресурсов с целью снижения рисков информационной безопасности за счет ликвидации некоторых видов угроз);
- контрольный раздел, содержащий методы и алгоритмы (метод условной оптимизации, метод ветвей и границ, алгоритмы прямого и обратного прогона, алгоритмы Качмажа и Балаша, генетические алгоритмы и др.). К сожалению данная разработка осталась на уровне макета и авторам исследования не удалось довести ее до логического завершения. Усложнение сценариев противостояния отражается и на структуре математических моделей, которые должны отражать новые условия и возникающие ситуации.

Формирование многокритериальных оптимизационных задач и разработка методов их решения имеет многовековую историю. Не вдаваясь подробно в описание всех существующих методов и моделей для решения подобных задач в рамках настоящего раздела диссертации, мы систематизировали все наиболее известные методы. На рисунке 1 приведена сравнительная характеристика методов многокритериальной оптимизации для решения задачи поиска оптимальных конфигураций многоконтурных систем защиты информации КБ для ОБИ.

Критерием оптимальности может быть один (или несколько) [9] показателей информационной (кибернетической) безопасности – величина ущерба от реализации угроз информации, общие расходы, которые включают ущерб от утечки информации и затраты на ее защиту, прибыль от инвестиций в защиту информации, их рентабельность и тому подобное.

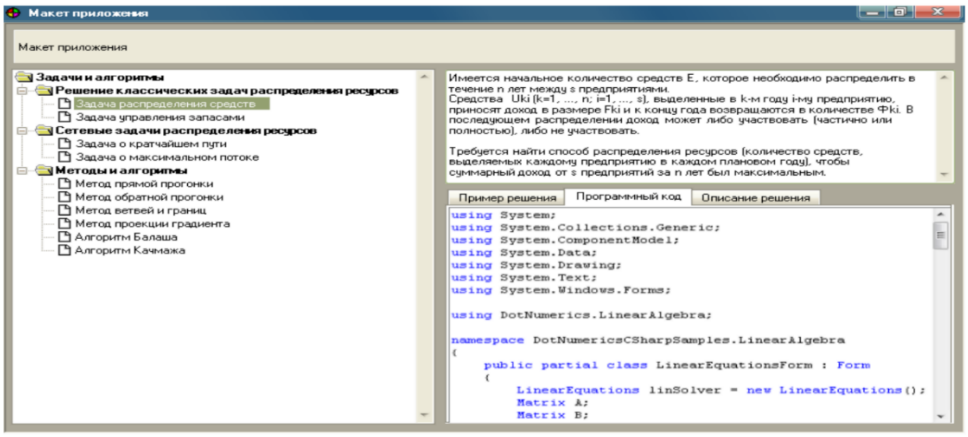

Рисунок 1. Макет системы поддержки принятия решений при поиске рациональных вариантов распределения ресурсов в том числе, выделяемых на системы защиты информации

Решение поставленных задач осложняется рядом причин. Главная из них обусловлена тем, что поиск оптимального решения ведется в условиях неопределенности, когда действия соперника можно предположить лишь с определенной вероятностью, а иногда вообще невозможно. Разнообразие средств и методов защиты, их характеристик, разнообразие схем противостояния,невозможность точного определения уязвимостей отдельных элементов системы защиты, отсутствие статистических данных по нашей стране, тоже накладывают ограничения на перечень приемлемых методов [10].

Приоритетной задачей работы является поиск в динамическом режиме оптимального распределения ресурсов в многоконтурных системах защиты ОБИ и системах разнонаправленного противостояния, где каждая из сторон стремится сохранить свою информацию и получить информацию соперника. Решение этой задачи для широкого класса систем с «привязкой» к конкретным объектам позволит улучшить экономические итехнические показатели многоконтурных СЗИ [11].

Моделирование

Построение математической модели для объекта исследования разделено на несколько этапов:

Этап 1) необходимо выбрать показатель, который определяет целевую функцию и собственно подлежит оптимизации. Такими показателями могут быть: надежность системы, ущерб от утечки информации, количество ресурсов, выделенных на защиту информации, их распределение междуобъектами, рентабельность инвестиций в защиту информации, суммарные потери, которые включают в себя ущерб от утечки информации и затраты на ее защиту и тому подобное.

Этап 2) следует определить параметры и характеристики системы, от которых зависит целевая функция.

Этап 3) необходимо собрать сведения о СЗИ и возможные условия противостояния (распределение информации по объектам, зависимость уязвимости объектов от условий противостояния, вероятности нападений на отдельные объекты, вероятности выделения определенного количества ресурсов нападения на объекты и т.д.).

Этап 4) необходимо установить вид зависимости целевой функции от параметров и характеристик СЗИ, а также от условий противостояние, то есть форму целевой функции.

Этап 5) следует выбрать критерий оптимальности (суммарный ущерб от утечки информации, его среднее значение по объектам, максимально допустимое значение для каждого из объектов и т.п.).

Заключение

Организация расчетов предусматривает такие операции: выбор метода решения задачи; составление и отладку программы для компьютера; проведение расчетов; представление результатов в наиболее удобной форме; формулирование выводов и рекомендаций.

Список использованной литературы:

1 Лахно В.А, Ахметов Б.С., Картбаев Т.С., Досжанова А.А., Маликова Ф.У. Модель и алгоритм выявления шпионских программ в информационных системах // Збірник тексти наукових матеріалів IX міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». 22-27 березня 2019 р. – С. 51-53

2 Ахметов Б.С., Алмасов Н.Ж. Развитие технических средств и систем безопасности в современных условиях// Материалы научной конференции ИИВТ КН МОН РК «Инновационные IT и Smart-технологии», посвященной 70-летнему юбилею профессора Утепбергенова И.Т.– С. 86-91

3 Ахметов Б.С., Бодесова Айдана, Данин Роман Определения причины обрушения строительных конструкций// Материалы научной конференции ИИВТ КН МОН РК «Инновационные IT и Smart-технологии», посвященной 70-летнему юбилею профессора Утепбергенова И.Т.– С. 91-95

4 Ахметов Б.С., Лахно В.А., Касаткин Д.Ю., Блозва А.И. Модель для системы поддержки принятия решений по инвестированию в технологии smart city// Материалы научной конференции ИИВТ КН МОН РК «Инновационные IT и Smart-технологии», посвященной 70-летнему юбилею профессора Утепбергенова И.Т. – С. 96-98

5 Ахметов Б.С., Лахно В.А., Малюков В.П., Касаткин Д.Ю. Система поддержки принятия решения о инвестировании в smart city в условиях неполной информации // Материалы научной конференции ИИВТ КН МОН РК «Инновационные IT и Smart-технологии», посвященной 70-летнему юбилею профессора Утепбергенова И.Т. – С. 99-101

6 Жаутиков Б.А., Ахметов Б.С., Яворский В.В., Чванова А.О. Корпоративная система университета на основе онтологических описаний // Материалы научной конференции ИИВТ КН МОН РК «Инновационные IT и Smart-технологии», посвященной 70-летнему юбилею профессора Утепбергенова И.Т. – С. 127-131

7 Akhmetov, S. Gnatyuk, T. Okhrimenko, V.V. Kinzeryavyy, Kh. Yubuzova Experimental research of the corrective ability of interferrence stable reed-solomon codes over the gf(32)galuis field at transfering information on a deterministic quantum and christochological code // Вестник КазНИТУ, - 2019, №2. – С. 61-69

8 Ахметов Б.С., Лахно В.А., Абуова А.К. Интеллектуальные технологии для анализа чрезвычайных ситуаций на железнодорожном транспорте // Вестник ПГУ, Серия энергетическая. № 1. 2019. – С. 43-51

9 Ахметов Б.С., Лахно В.А., Еркелдесова Г.Т. Автоматизация и диспетчеризация движения высокоскоростного транспорта в условиях временных ограничений // Вестник ПГУ, Серия энергетическая. № 1. 2019. – С. 52-60

10 Ахметов Б.С., Лахно В.А., Оралбекова А.О. Средства и методы неразрушающего контроля, диагностирования и детектирования состояния систем высокоскоростного железнодорожного транспорта // Вестник ПГУ, Серия энергетическая. № 1. 2019. – С. 61-71

11 Лахно В.А., Сауанова К.Т., Адилжанова С.А., Семятова А.Н. Генетикалық алгоритмді киберқауіпсіздік ресурстарының динамикалық бақылау есептерінде қолдану. // КазНИТУ им.К.И. Сатпаева, № 6 (142), 2020 – С. 565-572.

References:

1 Lahno V.A, Ahmetov B.S., Kartbaev T.S., Doszhanova A.A., Malikova F.U. (2019) Model' i algoritm vyjavlenija shpionskih programm v informacionnyh sistemah [Model and algorithm of detection of spy programs in Information Systems]. Zbirnik teksti naukovih materialiv IH mizhnarodnoї naukovo-tehnichnoї konferenciї «ITSec: Bezpeka informacijnih tehnologij»., 51-53. (In Russian)

2 Ahmetov B.S., Almasov N.Zh. Razvitie tehnicheskih sredstv i sistem bezopasnosti v sovremennyh uslovijah [Development of technical means and security system in modern conditions]. Materialy nauchnoj konferencii IIVT KN MON RK «Innovacionnye IT i Smart-tehnologii», posvjashhennoj 70-letnemu jubileju professora Utepbergenova I.T., 86-91. (In Russian)

3 Ahmetov B.S., Bodesova Ajdana, Danin Roman. Opredelenija prichiny obrushenija stroitel'nyh konstrukcij [Determination of the reasons for the destruction of building structures]. Materialy nauchnoj konferencii IIVT KN MON RK «Innovacionnye IT i Smart-tehnologii», posvjashhennoj 70-letnemu jubileju professora Utepbergenova I.T., 91-95. (In Russian)

4 Ahmetov B.S., Lahno V.A., Kasatkin D.Ju., Blozva A.I. Model' dlja sistemy podderzhki prinjatija reshenij po investirovaniju v tehnologii smart city [Model for supporting the system of decisions on investment in smart city technology]. Materialy nauchnoj konferencii IIVT KN MON RK «Innovacionnye IT i Smart-tehnologii», posvjashhennoj 70-letnemu jubileju professora Utepbergenova I.T.,96-98. (In Russian)

5 Ahmetov B.S., Lahno V.A., Maljukov V.P., Kasatkin D.Ju. Sistema podderzhki prinjatija reshenija o investirovanii v smart sity v uslovijah nepolnoj informacii [Support system decision on investment in smart city under the conditions of incomplete information]. Materialy nauchnoj konferencii IIVT KN MON RK «Innovacionnye IT i Smart-tehnologii», posvjashhennoj 70-letnemu jubileju professora Utepbergenova I.T., 99-101. (In Russian)

6 Zhautikov B.A., Ahmetov B.S., Javorskij V.V., Chvanova A.O. Korporativnaja sistema universiteta na osnove ontologicheskih opisanij [corporate system of the University on the basis of ontological descriptions].Materialy nauchnoj konferencii IIVT KN MON RK «Innovacionnye IT i Smart-tehnologii», posvjashhennoj 70-letnemu jubileju professora Utepbergenova I.T.,127-131. (In Russian)

7 Akhmetov, S. Gnatyuk, T. Okhrimenko, V.V. Kinzeryavyy, Kh. Yubuzova (2019) Experimental research of the corrective ability of interferrence stable reed-solomon codes over the gf(32)galuis field at transfering information on a deterministic quantum and christochological code.Vestnik KazNITU, №2,61-69. (In Russian)

8 Ahmetov B.S., Lahno V.A., Abuova A.K. (2019) Intellektual'nye tehnologii dlja analiza chrezvychajnyh situacij na zheleznodorozhnom transporte [Intelligent technologies for the analysis of clear situations on railway transport].Vestnik PGU, Serija jenergeticheskaja. № 1, 43-51. (In Russian)

9 Ahmetov B.S., Lahno V.A., Erkeldesova G.T. (2019) Avtomatizacija i dispetcherizacija dvizhenija vysokoskorostnogo transporta v uslovijah vremennyh ogranichenij [Automation and dispatching of high-speed transport under the conditions of current restrictions].Vestnik PGU, Serija jenergeticheskaja. № 1, 52-60. (In Russian)

10 Ahmetov B.S., Lahno V.A., Oralbekova A.O. (2019) Sredstva i metody nerazrushajushhego kontrolja, diagnostirovanija i detektirovanija sostojanija sistem vysokoskorostnogo zheleznodorozhnogo transporta [Funds and methods of non-destructive control, diagnostics and detection of high-speed railway transport system]. Vestnik PGU, Serija jenergeticheskaja. № 1, 61-71. (In Russian)

11 Lahno V.A., Sauanova K.T., Adilzhanova S.A., Semjatova A.N.(2020) Genetikalyk algoritmdi kiberkauipsizdik resurstarynyn dinamikalyk bakylau esepterinde koldanu [Application of the genetic algorithm in dynamic control problems of cybersecurity resources]. KazNITU im.K.I. Satpaeva, № 6 (142), 565-572. (In Kazakh)