АННОТАЦИЯ

диссертационной работы Адилжановой Салтанат Альмуханбетовны на тему «Методы, модели и информационные технологии для динамического управления ресурсами кибербезопасности» представленной на соискание степени доктора философии (PhD) по специальности «8D06301- Системы информационной безопасности»

Актуальность темы исследования. В условиях перманентного противостояния сторон защиты и нападения целью службы защиты информации любого объекта информатизации является минимизация возможностей ее хищения, искажения, утраты конфиденциальности, как следствия действий нападающей стороны. В тоже время у атакующих диаметрально противоположные задачи – распределение своих ресурсов таким образом, чтобы минимизировать затраты на получение доступа к информационным ресурсам.

Распределение ограниченных ресурсов стороны защиты надлежащим образом составляет сущность многих направлений исследования в области кибернетической или информационной безопасности. Такой подход по отношению к информационной безопасности приводит к постановке задачи рационального распределения ресурсов между объектами защиты.

В условиях неопределенности, когда действия соперника можно предположить лишь с определенной вероятностью, поиск рационального распределения ограниченных ресурсов между объектами защиты информации за счет использования теоретико-игровых методов и учета динамики изменения условий противостояние, позволит уменьшить величину причиненного вреда от реализации угроз информации. При этом представляется целесообразным сосредоточить внимание на развитии эволюционных методов и генетических алгоритмов для генерации множества решений в ходе поиска предпочтительных конфигураций многоконтурных систем защиты информации и кибербезопасность для объекта информатизации, а также применения генетического алгоритма для решения задачи по динамическому перераспределению ресурсов стороны защиты, исходя из актуальности существующих угроз.

Рост стоимости средств защиты информации актуализирует проблему рационального использования ресурсов защиты. В процессе поиска решений следует учитывать изменение условий противостояния с атакующей стороной во времени. Это связано со «старением» информационных ресурсов, их обновлением, появлением новых средств нападения, модернизацией средств защиты информации и тому подобное. В результате приходим к необходимости решения задачи динамического управления ресурсами в сложных структурах защиты.

Таким образом, для построения эффективной средств защиты информации необходимо учитывать достаточно большое количество показателей, которые в комплексе и определяют ее эффективность. Одновременно достичь оптимальных значений различных показателей из-за противоречивости их требований достаточно сложно, а зачастую и невозможно. В результате мы

приходим к многокритериальной задаче. Решение подобной задачи – это всегда компромисс в удовлетворении требований по отдельным показателям.

Научным вкладом данной работы заключается в разработке модифицированного генетического алгоритма для решение многокритериальной оптимизационной задачи распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибербезопасности объекта информатизации.

Цель диссертационный работы. Основной целью данной работы является повышение уровня защищенности объекта информатизации за счет рационального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника.

Задачи исследования:

1- проанализировать модели управления безопасностью информационно-коммуникационных системах объектов информатизации, в частности, модели для поиска оптимального распределения средств между объектами защиты информации;

2- разработать модифицированный генетический алгоритм для решения задачи рационального распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению КБ объекта информатизации;

3- дополнить генетический алгоритм для решения задачи, связанной с подбором и оптимизацией вариантов конфигураций средств защиты информации для контуров безопасности информационно-коммуникационных системах;

4 - программно реализовать многомодульную систему поддержки принятия решений (СППР) для анализа и выбора рационального варианта распределения ресурсов стороной защиты информации.

Объект исследования – процесс динамического управления ресурсами защиты информации в многоконтурных системах защиты с учетом уязвимости объектов.

Предмет исследования – методы и модели управления ресурсами стороны защиты при построении систем защиты информации.

Методы исследования. Метод динамического программирования Белмана-Заде – для нахождения оптимальных ресурсов стороны защиты. Эволюционные алгоритмы – для решения задачи рационального распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибербезопасности объекта информатизации.

Научная новизна исследования:

дополнена методика выбора целевой функции модели, описывающей причиненный ущерб от реализации угроз и уязвимость информационных ресурсов объекта информатизации.

впервые разработан модифицированный генетический алгоритм, который в отличие от существующих, позволяет упростить решение многокритериальной оптимизационной задачи распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибербезопасности объекта информатизации.

получил дальнейшее развитие генетического алгоритма для решения задачи, связанной с подбором и оптимизацией вариантов конфигураций средств защиты информации для контуров безопасности информационно-коммуникационных систем.

Теоретическая значимость исследования: Дополнена методика выбора целевой функции модели, описывающей причиненный ущерб от реализации угроз и уязвимость информационных ресурсов объектов информатизации. Также разработан модифицированный генетический алгоритм, который позволяет облегчить решение задачи рационального распределения ресурсов стороны защиты в ходе реализации проектов по обеспечению кибернетической безопасности объекта информатизации. Также получил дальнейшее развитие генетического алгоритма для решения задачи, связанной с подбором и оптимизацией вариантов конфигураций средств защиты информации для контуров безопасности информационно-коммуникационных системах.

Практическая значимость исследования. Разработана модульная СППР, в частности доказана эффективность открытой многомодульной архитектуры СППР с возможностью по мере расширения функционала СППР и добавлены модули в ее архитектуру динамически присоединяемые библиотеки для вычислительного ядра.

Основные положения, выносимые на защиту.

1. Методика выбора целевой функции модели, описывающей причиненный ущерб от реализации угроз и уязвимость информационных ресурсов объекта информатизации.
2. Модифицированный генетический алгоритм, который позволяет облегчить решение многокритериальной оптимизационной задачи распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибербезопасности объекта информатизации.
3. Генетический алгоритм для решения задачи, связанной с подбором вариантов конфигураций средств защиты информации для контуров безопасности информационно-коммуникационных системах.

Личный вклад соискателя. Все результаты диссертационной работы, которые вынесены на защиту, получены докторантом лично. Среди основных результатов: модифицированный генетический алгоритм для решения многокритериальной задачи оптимизации распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибербезопасности, генетического алгоритма для решения задачи, связанной с подбором и эфективности вариантов конфигураций средств защиты информации для контуров безопасности информационно-коммуникационных системах. Программная реализация модуля в виде динамически присоединяемой библиотеки для вычислительного ядра СППР на основе предложенного модификации генетического алгоритма с учетом суммарной величины рисков от потери информации, интегральных показателей средств защиты информации, а также стоимостных показателей для каждого класса средств защиты информации.

Уровень достоверности и результаты апробации. Достоверность полученных результатов показывается результатами программной реализации модуля в виде динамически присоединяемой библиотеки для вычислительного

ядра СППР на основе предложенного модификации генетического алгоритма результатов публикациями в журналах и трудах международных конференций. Основные положения диссертации и результаты исследования докладывались и обсуждались на научных семинарах кафедры информационных систем Казахского национального университета имени аль-Фараби; кафедры компьютерных систем, сетей и кибербезопасности Национального университета биоресурсов и природопользования Украины; Института информационных и вычислительных технологий МОН РК и других международных конференциях.

Вклад докторанта в подготовке каждой публикации. В опубликованных статьях и научных трудах описаны результаты исследования по теме диссертации. За время научной работы было написано 11 научных работ, в том числе 4 статьи в журналах, рекомендованных Комитетом по Контролю в Сфере Образования и Науки Министерства образования и науки Республики Казахстан; 2 публикации в материалах международных конференций, 5 статьи в журналах, входящих в базу Scopus.

Журнальные статьи в базе данных Scopus:

1. Akhmetov B., Lakhno V., Adilzhanova S., Yagaliyeva B. Conseptual Diagram of intelligent Decision Support System in the Prosses of Investing in Cybercecurity Systems . Journal of Theoretical and Applied Information Technology, 2021, 99(18), стр. 4297–4310 .
2. Akhmetov, B., Lakhno V., Adilzhanova S. Automation of Information Security Risk Assessment. International Journal of Electronics and Telecommunications 2022, 68(3), pp. 549–555.
3. Lakhno V., Adilzhanova S., Kryvoruchko O. Genetic algorithm for solving the problem of scaling a cloud-oriented object of information. Journal of Theoretical and Applied Information Technology, 2022, 100(7), стр. 1693–1705.
4. Lakhno V., Adilzhanova S., Kryvoruchko O., Desiatko A. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. Informatics and Cybernetics in Intelligent Systems. CSOC 2021. Lecture Notes in Networks and Systems, vol 228. Springer, Cham.
5. Akhmetov B., Lakhno V., Adilzhanova S.The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, стр. 251–254, 9349310

В журналах, рекомендованных Комитетом по Контролю в Сфере Образования и Науки Министерства образования и науки:

1. Лахно В. А., Адилжанова С.А., Сауанова К. Т. Генетикалық алгоритмді кибер қауіпсіздік ресурстарының динамикалық бақылау есептерінде қолдану. Сатпаев атындағы ҚазҰТЗУ Хабаршысы №6 (142). – 2020. – С. 565-568
2. Адилжанова С.А., Тюлепбердинова Г.А., Сакыпбекова М.Ж. Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарын көп өлшемді оңтайландыру мен динамикалық басқарудың математикалық әдістерін

талдау. Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы, №4(72), 2020 с. 145-148.

3. Адилжанова С.А., Ахметов Б.С., Абуова А.К., Сагындыкова Ш. Қорғаныс объектілері арасында ресурстарды бөлуді оңтайландыру кезінде шешім қабылдауды қолдаудың модульдік жүйесі. Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы №4(76), 2021 г. – С. 128 - 135 .
4. Адилжанова С.А., Ахметов Б.С., Лахно В. А. Ақпаратты қорғау тарапының ресурстарын іріктеу, оңтайландыру және қайта бөлу мәселесін шешу үшін генетикалық алгоритмді дамыту. Алматы энергетика және байланыс университетінің хабаршысы № 1 (56) 2022. – С. 116 - 123

На международных конференциях:

1. Адилжанова С.А. Киберқауіпсіздік ресурстарын динамикалық басқарудың математикалық әдістерін талдау. Международная научная конференция студентов и молодых ученых «Фараби әлемі», КазНУ имени аль-Фараби, 2020. – С.41
2. Адилжанова С.А. Использование генетического алгоритма в задаче динамического управления ресурсами кибербезопасности. Международная научная конференция студентов и молодых ученых «Фараби әлемі», КазНУ имени аль-Фараби, 2021. – С.73

Структура и объем диссертации. Диссертация состоит из введения, четырех разделов, заключения, изложенных на 128 страницах и содержит 23 рисунков, 9 таблиц, 93 использованных источников и 2 приложения.

Во введении обосновывается актуальность диссертации. Сформулированы цель работы, объект и предмет исследования. Выявлена научная новизна и практическая значимость. Описаны результаты исследования. Приводится информация об апробации результатов исследования и публикации.

В первом разделе представлен анализ математических методов многокритериальной оптимизации и динамического управления ресурсами кибербезопасности объектов информатизации.

Во втором разделе описывается генетический алгоритм для решения задачи оптимизации распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению кибернетической безопасности.

В третьем разделе описывается работа поддержка принятия решений по оптимизации размещения средств защиты информации на основе использования модифицированного генетического алгоритма.

В четвертом разделе представлены результаты и программная реализация модулей СППР в ходе поиска рациональных стратегий динамического распределения ресурсов стороны защиты.

В заключении сформулированы основные полученные результаты в диссертации.