УДК 519.21:681.142 **Р.В. Резниченко, Л.А Тимашова**

ІНТЕЛЕКТУАЛЬНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІРТУАЛЬНОГО ПІДПРИЄМСТВА НА ОСНОВІ ЕВОЛЮЦІЙНИХ АЛГОРИТМІВ

Розроблена концепція безпеки віртуального підприємства з використанням еволюційних алгоритмів. Розглянуті генетичні алгоритми для шифрування даних, метод рою частинок при плануванні бюджету на безпеку віртуального підприємства, метод рою частинок для оцінки ризиків віртуального підприємства.
***Ключові слова**: віртуальне підприємство, еволюційні алгоритми, генетичні алгоритми, метод рою частинок, шифрування, крипто аналіз, безпека віртуального підприємства.*

Разработана концепция безопасности виртуального предприятия с использованием эволюционных алгоритмов. Рассмотрены генетические алгоритмы для шифрования данных, метод роя частиц при планировании бюджета на безопасность виртуального предприятия, метод роя частиц для оценки рисков виртуального предприятия.
***Ключевые слова**: виртуальное предприятие, эволюционные алгоритмы, генетические алгоритмы, метод роя частиц, шифрование, криптоанализ, безопасность виртуального предприятия.*

A security concept of the virtual enterprise by using evolutionary algorithms. Considered genetic algorithms to encrypt the data, the method of particle swarm in the planning of the budget for the security of virtual enterprise, particle swarm method to assess the risks of the virtual enterprise.

Keywords: virtual enterprise, evolutionary algorithms, genetic algorithms, particle swarm method, encryption, cryptanalysis, the security of virtual enterprise.

Актуальність.

При вирішенні багатьох проблем забезпечення безпеки виникають питання пов'язані з багатоцільовим характером процесу забезпечення безпеки віртуального підприємства. Однією з основних причин, що зумовлює необхідність розгляду багатоцільових задач у сфері безпеки віртуального підприємства є невизначеність багатьох характеристик системи. На сьогодні спроби застосування еволюційних алгоритмів при вирішенні прикладних проблем охоплюють не тільки клас традиційних задач оптимізації але і розповсюджуються на інші напрямки штучного інтелекту, наприклад управління складними динамічними об'єктами в умовах невизначеності, прийняття рішень на основі нечіткого багатокритеріального вибору. У більшості випадків в задачах безпеки невизначеність пов'язана зі складністю об'єкта і відсутністю інформації про можливі загрози. Саме тому, в роботі розглядаються проблеми ефективності використання еволюційних алгоритмів в сфері безпеки.

В останній час значного розповсюдження набули обчислювальні методи і алгоритми, що базуються на еволюційних принципах. Вони швидко поширюються, оскільки більшість управлінських задач характеризується NP-складністю, тому у більшості випадків основним критерієм ефективності є швидке обчислення наближених рішень.

Аналіз останніх досліджень і публікацій.

Еволюційні алгоритми показали високу ефективність у сфері безпеки віртуальних підприємств. Дослідження T. Kirt та J. Kivimaa [1] показують високу ефективність еволюційних алгоритмів, при розрахунку найбільш

доцільних витрат на інформаційну безпеку враховуючи найбільш важливі ризики інформаційної безпеки. Чернишовим Ю.О. [5] було розглянуто застосування біоінспірованних методів для вирішення завдання криптоаналізу, отримані експериментальні результати свідчать про можливість застосування даних методів для криптоаналізу методів шифрування. Автор застосовує конструктивні евристичні методи, в яких рішення задачі будується поетапно шляхом додавання нового компонента до частково побудованого рішення.

Різні моделі та алгоритми розроблені для забезпечення більш наукових і ефективних способів управління ризиками ВП. J.Ma and Q. Zhang аналізують всі види ризиків організації ВП. Huang, K. [3] введена нечітка синтетична еволюційна модель для оцінки еволюційних ризиків ВП, що зосереджена на проектному режимі і невизначених характеристиках ВП. W. H. Ip, M. Huang, K. L. Yung, and D. Wang пропонують модель, з урахуванням ризиків вибору партнера, що розглядає зведення до мінімуму ризику вибору партнерів на основі правил генетичного алгоритму, з врахуванням досвіду календарного планування. X. Sun, M. Huang, and X. Wang досліджують конструкційні розподілення рішень DDM (distributed decision making) моделі для зменшення ризиків ВП., яка зосереджується на ситуації в команді де існують вимушені стосунки між партнерами. F.-Q. Lu, M. Huang, W.-K. Ching, X.-W. Wang, and X.-L. [3] Sun представили DDM модель ВП управління ризиками, яка має два рівні, а саме топ-модель та базову модель, що описують процеси прийняття рішень між власниками і партнерами. В результаті був розроблений підхід для вирішення задачі оптимізації на основі еволюційного алгоритму оптимізації рою частинок.

У сучасній економічній літературі існують роботи, в яких відображені питання оцінки та управління ризиками у підприємницькій діяльності. Проте їх наукову розробленість в цілому не можна визнати задовільною. Тому виникла необхідність більш глибокого дослідження і узагальнення зарубіжного і вітчизняного досвіду.

Невирішені проблеми.

Використання новітніх інформаційних технологій та централізованої системи управління дозволяє здійснювати збір, аналіз, групування, зберігання великих обсягів інформації; забезпечує обмін інформацією між усіма агентами ВП без прямого фізичного контакту; надає можливість автоматизувати (повністю або частково) бізнес-процеси, що мають стандартні умови вирішення і, відповідно, усунути можливий вплив суб'єктивного фактору та додаткових ризиків, що з ним пов'язані. Система управління дозволяє відслідковувати всі наявні бізнес-процеси ВП у будь який час його роботи. Однак використання спільних інформаційних технологій зумовлює додаткові ризики пов'язані з роботою самих агентів ВП, адже стає можливою, внаслідок несанкціонованих дій, втрата важливої інформації. Крім цього, побудова системи управління вимагає значних фінансових та інтелектуальних ресурсів саме на початковому етапі, коли ефективність ВП ще не можливо остаточно визначити. Зрозуміло, що не враховані на початковому етапі побудови ВП фактори, у майбутньому можуть спричинити значні проблеми і поставити під сумнів ефективність функціонування проекту в цілому.

Завдання забезпечення безпеки віртуальних підприємств близькі до аналогічних завдань в інших автоматизованих системах (АС) обробки інформації, для вирішення яких в даний момент вже існує законодавча і

нормативна база, а також організаційно-технічні рішення. Проте, на відміну від безпеки в окремій організації, безпека віртуального підприємства має свою специфіку[4]. В якості головних особливостей можна вказати:

- географічно розподілена структура;
- різнорідність використовуваних програмно-технічних рішень;
- необхідність захисту інформації та інтелектуальної власності, що належить кільком власникам.

Під інформаційною безпекою віртуального підприємства (далі ВП) розуміється стан захищеності його інтересів від існуючих і ймовірних зовнішніх і внутрішніх загроз інформаційних ресурсів.

Мета заходів щодо забезпечення безпеки ВП - скоротити можливий економічний і моральний збиток віртуального підприємства, пов'язаний з пошкодженням або неправомірним використанням інформаційних ресурсів.

Метою статті є дослідження можливостей та ефективності застосування еволюційних алгоритмів для підвищення безпеки віртуального підприємства.

Постановка завдання.

Забезпечення безпеки ВП являє собою складний комплекс технічних, юридичних та організаційних проблем. Ми пропонуємо власну концепцію безпеки ВП з використанням еволюційних алгоритмів. Ми використовуємо еволюційні алгоритми оскільки, еволюційні алгоритми використовуються при комбінаторної оптимізації, зокрема при вирішенні класичних NP-повних проблем, таких як задача комівояжера, задача упаковки ранця, розбиття чисел, максимально незалежну безліч і замальовка графів. Еволюційні алгоритми показують високу ефективність при

оцінці ризиків, розрахунку бюджету на безпеку ВП, шифруванні даних.

Виклад основного матеріалу.

Основою для системного вирішення завдань забезпечення безпеки є: аналіз можливих ризиків, політика інформаційної безпеки (ІБ) і план забезпечення безпеки ВП.

Узагальнену концепцію безпеки віртуального підприємства необхідно представити на рис.1.

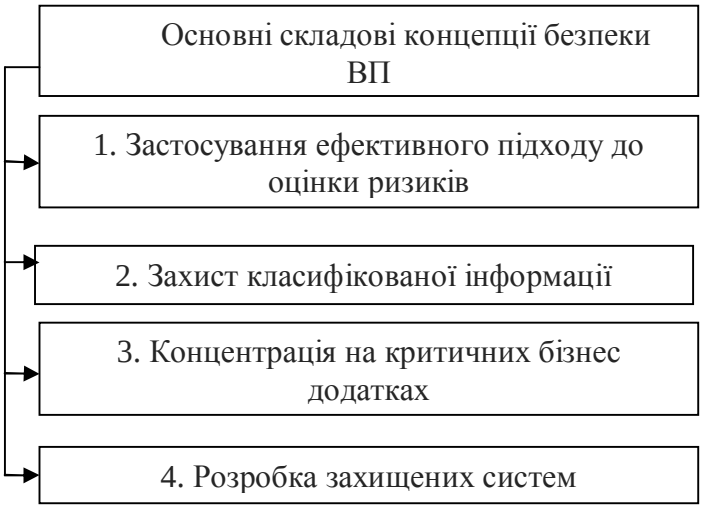

Рис.1 Основні принципи концепції безпеки ВП

Розглянемо більш детально кожний принцип концепції безпеки ВП (таблиця 1).

Еволюційні алгоритми успішно використовуються для завдань функціональної оптимізації і можуть легко бути описані на математичній мові. Для ефективної реалізації моделі оптимізації управління ризиками ВП використовуються методи ройового інтелекту, а саме

метод рою частинок (Particle Swarm Optimization (далі-PSO)) [3]

Таблиця 1

Концепція безпеки віртуального підприємства.
Застосування ефективного підходу до оцінки ризиків

Принцип	Мета	Опис	Математична модель	Реалізація математичної моделі/ Методу
Застосування ефективного підходу до оцінки ризиків	Оцінити ризики та переконатися, що управління ризиками здійснюється послідовно та ефективно	Для ефективної реалізації моделі оптимізації управління ризиками ВП використовуються методи ройового інтелекту, а саме метод рою частинок (Particle Swarm Optimization (далі-PSO))	$\min_I F_T(I) = \sum_{i=0}^{n} w_i R_i(I_i)$ $\sum_{i=o}^{n} I_i \le I_{max}$, $R_i(I_i) \le R_{max}$, де, $R_i(I_i)$ - рівень ризику i-го члена в умовах ризику інвестиційних витрат; I_{max} - максимальний бюджет інвестицій; R_{max} - максимальний рівень ризику для кожного члена ВП.	Дворівнева модель управління ризиками була застосована для опису процесів прийняття рішень власника і партнерів.

Робота з ризиками для безпеки інформації повинна бути організована таким чином, щоб була можливість

приймати документовані рішення на підставі достатньої кількості відомостей. Для управління ризиками фахівець має право задіяти один або кілька різних методів: прийняття ризиків, уникнення ризиків, делегування ризиків, врегулювання ризиків, яке традиційно асоціюється з прийняттям певних заходів безпеки - таких, як установка спеціалізованого програмного забезпечення для управління доступом, моніторингу мережевої активності і т. д.

Розроблена модель оптимізації для мінімізації ризиків віртуального підприємства на основі еволюційних алгоритмів і методів ройового інтелекту. Дворівнева модель управління ризиками була застосована для опису процесів прийняття рішень власника і партнерів. Ця модель показує ситуацію, коли власник виділяє бюджет кожному члену ВП з метою мінімізації рівня ризиків ВП.

Розглянемо наступний принцип концепції – захист класифікованої інформації (таблиця 2)

Останнім часом при розробці комп'ютерних технологій, забезпеченні інформаційної безпеки і захисті інформації, широке застосування знаходять криптографічні методи захисту. Основними завданнями в криптографії є розробка нових способів шифрування, складних для розкриття, і розкриття існуючих шифрів. Для вирішення цього завдання, що відноситься до класу NP-повних, в останні роки застосовуються алгоритми, засновані на природних системах. До них відносяться генетичні алгоритми (ГА), еволюційні методи, алгоритми ройового інтелекту і т.д. У моделях і алгоритмах еволюційних обчислень ключовим елементом є побудова початкової моделі і правил, за якими вона може змінюватися (еволюціонувати).

Таблиця 2

Концепція безпеки віртуального підприємства.

Принцип	Мета	Опис	Метод	Реалізація методу
Захист класифікованої інформації	Запобігти проникненню конфіденційної інформації або даних особливої важливості до неавторизованих осіб	Інформацію необхідно проаналізувати і класифікувати відповідно до ступеня її конфіденційності Класифікована інформація повинна належним чином захищатися на всіх етапах її життєвого циклу, наприклад, мандатний контроль або шифрування.	Шифрування/Алгоритм RSA Генетичний алгоритм розкладання заданого числа на множники	1. Задається число в десятковій формі. 2. Задається популяція хромосом 10000x2. 3. Виконуються генетичні операції (кросинговер, мутація, інверсія, елітна селекція). 4. Підраховується цільова функція шляхом множення відповідних хромосом в двійковій формі з ідентичними номерами з кожної частини. 5. Кінець.

Протягом останніх років були запропоновані різноманітні схеми еволюційних обчислень, в т.ч. генетичний алгоритм, генетичне програмування, еволюційні стратегії, еволюційне програмування.

Чернишовим Ю.О. [5] було розглянуто застосування біоінспірованних методів для вирішення завдання криптоаналізу, отримані експериментальні результати свідчать про можливість застосування даних методів для криптоаналізу методів шифрування. Автор застосовує конструктивні евристичні методи, в яких рішення задачі будується поетапно шляхом додавання нового компонента до частково побудованого рішення. До методів даного виду відносять і мурашині алгоритми, основу яких складає імітація самоорганізації мурашиної колонії. Наводиться опис застосування біоінспірованних методів для вирішення завдання криптоаналізу асиметричних алгоритмів шифрування на основі факторизації складених чисел. Представлені алгоритми мурашиних і бджолиних колоній для розкладання складених чисел на множники шляхом визначення дільника числа із заданою точністю в заданому інтервалі. Показано, як ця проблема може бути зведена до класичної задачі знаходження найкоротшого шляху в графі, що вирішується за допомогою алгоритму мурашиних колоній. Наводиться алгоритм рішення, а також приклад роботи мурашиного і бджолиного алгоритму.

Наступний принцип концепції безпеки ВП – концентрація на критичних бізнес-додатках (таблиця 3)

Наступний принцип концепції безпеки ВП – розробка захищених систем (таблиця 4).

При плануванні та проектуванні ефективної системи захисту даних, згідно концепції, ми використовуємо

генетичні алгоритми для розрахунку оптимального бюджету на безпеку ВП

Таблиця 3

Концепція безпеки ВП. Концентрація на критичних бізнес-додатках

Принцип	Мета	Опис
Концент-рація на критичних бізнес додатках	Розподіляти дефіцитні ресурси безпеки на основі пріоритетності, забезпечуючи захист в першу чергу для тих бізнес-додатків, успішна атака проти яких завдасть найбільшої шкоди	Оцінити потенційні збитки, які буде завдано бізнесу в разі порушення цілісності та / або доступності цих даних. Після цього можна визначити вимоги до ресурсів, які виділяються на забезпечення безпеки, і пріоритезувати процес їх розподілу, захистивши в першу чергу найбільш важливі інформаційні активи.

При плануванні, проектуванні, побудові та перевірці (простіше кажучи, на всіх стадіях життєвого циклу) інформаційної системи ВП захист даних повинен бути її одним з головних завдань. Ключову роль на будь-якому етапі розробки системи повинно займати ретельне тестування на уразливості, перевірка на стійкість до помилок, винятків і надзвичайних ситуацій.

Таблиця 4

Концепція безпеки ВП. Розробка захищених систем

Принцип	Мета	Опис	Математична модель	Реалізація математичної моделі
Розробка захищених систем	Побудувати якісну, надійну і низьковитратну систему роботи з даними	При плануванні, проектуванні, побудові та перевірці (на всіх стадіях життєвого циклу) інформаційної системи ВП захист даних повинен бути її одним з головних завдань.	$R_{max} = \sum_{i=1}^{n} a_i q_{max\,i}$ $\sum_{i=1}^{n} a_i = 1$ де, q_{max} максимальний рівень довіри де безпеки *i*-ої групи, та a_i вага *i*-ої групи	Розрахунок адекватних і еквівалентних профілів безпеки для кожного рівня витрат з розумним періодом часу

.

Головним завданням в області ІТ-безпеки ВП є забезпечення необхідної інформаційної безпеки відповідно до умов невизначеності. Для досягнення поставленої мети

організація повинна визначити адекватний рівень безпеки і визначити відповідні заходи для підвищення кібербезпеки і найбільш ефективного розподілу ресурсів. Як правило, деякі методи оцінки ризику використовуються для проведення детального аналізу ризику. Для малих і середніх підприємств, детальний аналіз ризиків є відносно дорогим, а також наявні ресурси для IT-безпеки обмежені. Тому необхідна спрощена версія моделі безпеки, яка забезпечує можливість для досягнення максимально можливого довіри з обмеженими ресурсами. Таку модель запропонував Toomas Kirt[2].

Для експериментів Toomas Kirt використовував дані для 9 рівнів інформаційної безпеки:

- функціональні модулі (навчання користувачів);
- самодостатність (надмірність) системи;
- Access контроль;
- антивірус;
- резервне копіювання;
- відключення (роз'єднання);
- шифрування;
- брандмауер;
- виявлення вторгнень.

Метою оптимізації було знайти найвищий середній рівень довіри для даної кількості ресурсів. Задача оптимізації формулюється як запитання: "Для кожного можливого рівня бюджету яку максимальну впевненість можна очікувати? "У завданнях оптимізації кількість ресурсів (бюджету) була зумовлена від 1 до макс + 1. Максимальне значення становлять витрати, пов'язані із заходами безпеки найвищого рівня. Мета дослідження полягала в тому, щоб оцінити, наскільки еволюційний підхід застосовується до безпеки та завдань оптимізації витрат/довіри і дозволяє створювати еквівалентні профілі

безпеки для кожного рівня витрат. В результаті Toomas Kirt визначив, що еволюційний підхід є життєздатним для таких завдань. Результати показали, що еволюційний алгоритм досить швидко забезпечує результати і виявився більш гнучкими, ніж дискретний метод динамічного програмування. Еволюційний підхід забезпечив результати протягом розумного строку та оптимізації витрат/довіри 9 областей діяльності безпеки і зайняв 0.4-0.45 секунд. Основна перевага еволюційного алгоритму в тому, що він надав кілька адекватних і еквівалентних профілів безпеки для кожного рівня витрат з розумним періодом часу. Тим самим еволюційний підхід може допомогти забезпечити більш високий рівень довіри.

Висновки.

При забезпеченні інформаційної безпеки і захисті інформації, широке застосування знаходять криптографічні методи захисту. Основними завданнями яких є розробка нових способів шифрування, складних для розкриття, і розкриття існуючих шифрів. Актуально та ефективно для вирішення цього завдання, що відноситься до класу NP-повних, в останні роки застосовуються алгоритми, засновані на природних системах. Також, еволюційні алгоритми ефективні при розрахунку найбільш доцільних витрат на інформаційну безпеку враховуючи найбільш важливі ризики інформаційної безпеки. Основна перевага еволюційного алгоритму в тому, що він надає кілька адекватних і еквівалентних профілів безпеки для кожного рівня витрат з розумним періодом часу. Розроблена концепція безпеки віртуального підприємства з використанням еволюційних алгоритмів що, показує високу ефективність при оцінці ризиків, розрахунку бюджету на безпеку ВП, підвищує ефективність шифрування даних.

Список використаних джерел

1. Kivimaa, J., 2009. Applying a costs optimizing model for IT security. In H. Santos (Ed.), Proceedings of the 8th European Conference on Information Warfare and Security (pp. 142□153). Reading, UK: Academic Publishing Limited
2. Kivimaa, J., Ojamaa, A., Tyugu, E., 2009. Graded Security Expert System, Critical Information Infrastructure protection, Berlin: Springer
3. F.-Q. Lu, M. Huang, W.-K. Ching, X.-W. Wang, and X.-L. Sun, "Multi-swarm particle swarm optimization based risk management model for virtual enterprise," in Proceedings of the 1st ACM/SIGEVO Summit on Genetic and Evolutionary Computation (GEC '09), pp. 387–392, Shanghai, China, June 2009
4. Тимашова Л.А. Задачи мониторинга и управления бизнес-процессами виртуального предприятия / Тимашова Л.А., Тур Л.П., Музалева В.А., Лещенко В.А., Яненко Л.А. // Матеріали XVI Міжнародной. конф. з автоматичного управління „Автоматика 2007", (Севастополь, 10–14 вересня 2007 р.). Ч. 2. – Севастополь: СНУЯЄ та П, 2007. – С. 63–64.
5. Чернышев Ю.О, Сергеев А.С., Дубров Е.О. Применение биоинспирированных алгоритмов оптимиза- ции для реализации криптоанализа классических и асимметричных криптосистем // Информатика: про- блемы, методология, технологии: материалы XIV Международной научно-методической конференции /ВГУ. – Воронеж: Издательский дом ВГУ, 2014, с. 206-210.

УДК 330.46+332.14+336.02

С.М. Руденко

ОСНОВНІ КОНЦЕПТУАЛЬНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЇ ПРО ФІНАНСОВИЙ СТАН РЕГІОНІВ ТА ЙОГО АНАЛІЗУ В ЄДИНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Представлено основні концептуальні засади формування інформації про фінансовий стан регіонів та його аналізу в єдиному інформаційному простор.