ОПИС СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Оболонський М.В.[1,2], студент, maksym.obolonskyi.kita@donntu.edu.ua
Любименко О.М.[1,2], студент, к.ф.м.н, доцент, e.n.lyubimenko@gmail.com
Штепа О.А.[1,2], студент, к.т.н, доцент, o.a.shtepa@gmail.com

[1.] ДВНЗ «Донецький національний технічний університет», Луцьк, Україна
[2.] ДВНЗ «Мелітопольський державний педагогічний університет імені Богдана Хмельницького», Запоріжжя, Україна

Ефективне управління ризиками в інформаційній безпеці стає необхідним завданням для підприємств. Вони повинні не лише визначати потенційні загрози, але й розробляти стратегії та механізми для зниження цих ризиків та впровадження відповідних контрзаходів [1]. Робота орієнтована на дослідження та вирішення ключової проблеми інформаційної безпеки підприємств – мінімізації ризиків. Розв'язання цієї актуальної проблеми передбачає використання комплексного підходу та новітніх технологій, серед яких особливе місце відводиться генетичним алгоритмам. Генетичні алгоритми – це ефективні інструменти, які виникають із біологічних еволюційних процесів [2]. Вони здатні вирішувати складні завдання оптимізації та пошуку, надаючи можливості для їх застосування в галузі оцінки ризиків інформаційних систем.

Розробці системи передував ретельний об’єктний аналіз предметної області. Було розглянуто існуючі методи оцінки ризиків ІС, проведено порівняльний аналіз конкуруючих систем, обрано і обґрунтовано сучасні інформаційні технології для створення ефективної системи захисту ІС підприємства.

Реалізація ефективної системи захисту ІС підприємства передбачає необхідність зберігання інформації про активи підприємства, загрози, які пов’язані з ресурсами, їх ймовірність та збиток, а також вразливості та впроваджені контрзаходи [3].

Система передбачає створення матриці ризиків та впровадження контрзаходів для зниження ризиків ІБ. Враховуючи ці вимоги, було спроєктовано базу даних з певними таблицями. На основі наданої інформації, програмну систему було розбито на окремі модулі.

Генетичні алгоритми [4] здатні вирішувати складні оптимізаційні задачі та пошукові завдання, що створює можливості застосування їх в галузі оцінки ризиків ІС.

Генетичні алгоритми (ГА) можуть бути застосовані для оцінки ризиків інформаційної системи та впровадження контрзаходів з метою зменшення цих ризиків. Алгоритм буде мати наступний вигляд. Перш за все необхідно визначити ризики з якими стикається ІС, фактори, які впливають на рівень

ризику та параметри, такі як ймовірність виникнення загрози. Після цього потрібно створити початкову популяцію рішень, яка представляє можливі контрзаходи або стратегії зменшення ризиків в ІС. Кожен рішення може бути представлений як набір параметрів або налаштувань системи. Далі необхідно розробити функцію оцінки (пристосованості) для кожного рішення в популяції, яка визначає, наскільки кожне рішення зменшує ризики згідно з моделлю ризиків. Для розвитку популяції рішень необхідно згідно структури ГА застосувати генетичні операції, а саме схрещування і мутацію Це допоможе знайти оптимальні стратегії зменшення ризиків з часом. Після чого необхідно обрати, які рішення з популяції вважатимуться кращими на основі їхньої функції оцінки. Ці рішення будуть рекомендованими контрзаходами для зменшення ризиків.

Створений алгоритм оцінки ризиків за допомогою генетичних алгоритмів включає:

– створення початкової популяції, яка представляє можливі стратегії зменшення ризиків в ІС;

– розробка функції пристосованості, для оцінки кожного рішення;

– використання схрещування та мутації для розвитку популяції рішень;

– відбір кращих рішень на основі функції оцінки;

– впровадження рекомендованих контрзаходів або стратегій зменшення ризиків в ІС.

– моніторинг стану ІС та рівня ризиків, та адаптація контрзаходів згідно з новими загрозами та змінами в ІС.

Запропонованою методологію та програмне забезпеченням на реальних або симульованих даних для підтвердження ефективності та працездатності системи рисунок 1.

	Загроза	Контрзахід	Примітка	Коефіцієнт	Ймовірність до	Збиток	Ризик до	Ймовірність після	Ризик після	Ефективність
1	Вірусна інфекція	Встановити та ...	Risk1	3.0	4.0	3.0	12.0	1.0	3.0	75.0
2	Втрата ...	Встановлення ...	Risk2	3.0	3.0	2.0	6.0	0.0	0.0	100.0
3	Флуктуація ...	Встановлення ...	Risk3	1.0	3.0	1.0	3.0	2.0	2.0	33.3333333333...
4	Втрата ...	Зберігати ...	Risk4	1.0	2.0	4.0	8.0	1.0	4.0	50.0
5	Потрапляння у...	Встановити ...	Risk5	1.0	2.0	3.0	6.0	1.0	3.0	50.0
6	Використання ...	Багатофактор...	Risk6	1.0	2.0	1.0	2.0	1.0	1.0	50.0
7	Викрадення ...	Встановити ...	Risk7	2.0	3.0	4.0	12.0	1.0	4.0	66.6666666666...
8	Присвоєння ...	Встановити ...	Risk8	2.0	2.0	2.0	4.0	0.0	0.0	100.0
9	Помилка	Реалізувати ...	Risk9	2.0	2.0	2.0	4.0	0.0	0.0	100.0
10	Спотворення ...	Застосувати ...	Risk10	3.0	3.0	3.0	9.0	0.0	0.0	100.0

Рисунок 1 – Вигляд вікна програми розділу застосування контрзаходів за допомогою генетичного алгоритму.

Результат роботи генетичного алгоритму може змінюватися з кожним поколінням. ГА використовують концепції природного відбору та еволюції для пошуку оптимальних рішень у просторі можливих варіантів. Щоразу, коли генерація нових рішень (індивідів) відбувається, можливість знаходження кращих рішень може змінюватися. У перших поколіннях генетичного алгоритму рішення

можуть бути випадковими або неоптимальними. Проте, з кожним поколінням алгоритм застосовує процеси відбору, схрещування та мутації для покращення популяції індивідів. Цей процес може призводити до знаходження більш оптимальних або прийнятних рішень у подальших поколіннях.

Одним з варіантів є можливість підбору оптимальних параметрів для конкретних сценаріїв або типів ризиків. Розширення функціоналу програмної системи, які дозволять краще адаптувати її до змінних умов, нових типів загроз та потенційних вразливостей. Для точніших результатів необхідно використовувати більші об’єми даних, це можна вирішити впровадивши алгоритм у вже існуюче підприємство.

Література

1. А.М. Гребенюк, Л.В. Рибальченко, Основи управління інформаційною безпекою. Дніпро, Україна: Видавництво ДДУВС, 2020.

2. Э. Вирсански, Генетические алгоритмы на Python / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2020.

3. Про засади інформаційної безпеки [Електронний ресурс] – Режим доступу: https://ips.ligazakon.net/document/JG3TH00A?an=3.

4. Генетичні алгоритми. Вступ. [Електронний ресурс] – Режим доступу: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.

Анотація

В роботі представлено розробку ефективної системи захисту інформаційної системи підприємства з використанням генетичних алгоритмів для оцінки ризиків та впровадження контрзаходів. Досліджено процеси створення ефективної системи захисту інформаційної системи підприємства.

Ключові слова: система захисту інформації, ризик, контрзахід, генетичні алгоритми, мінімізація ризиків.

Abstract

The paper presents the development of an effective system for protecting the company's information system using genetic algorithms for risk assessment and implementation of countermeasures. The processes of creating an effective system for protecting the company's information system have been studied.

Keywords: information protection system, risk, countermeasure, genetic algorithms, risk minimization.