МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ОМЕЛЯНЮК ДМИТРО СЕРГІЙОВИЧ

УДК 004.056.5

МЕТОД МІНІМІЗАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПОБУДОВІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

125 «Кібербезпека»

Автореферат
дипломної роботи на здобуття
освітнього рівня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, зав. кафедри кібербезпеки
Загородна Наталія Володимирівна,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: доктор наук із соціальних комунікацій, професор кафедри комп'ютерних наук
Кунанець Наталія Едуардівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 24 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №32 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Одним із основних етапів забезпечення інформаційної безпеки є розробка політики безпеки інформації. Головною метою політики безпеки інформації є забезпечення інформаційної безпеки, котра циркулює в рамках виробничої діяльності всіх підрозділів підприємства і збереження головних якостей інформації таких, як цілісність, конфіденційність та доступність. Управління ризиками є одним з важливих етапів розробки власної політики безпеки. Методи оцінки ризиків є доволі стандартизованими і описаними і міжнародних стандартах, а суть управління ризиками зводиться до того, що переконатися, що ризики знаходяться в прийнятних межах і залишаються такими. Актуальною задачею є дослідження методів мінімізації ризиків на основі побудованих експертних оцінок.

Мета роботи: розробка методу мінімізації ризиків інформаційної безпеки при побудові системи захисту інформації для забезпечення необхідного рівня захищеності з врахуванням обмежених витрат на систему захисту інформації.

Об'єкт, предмет та методи дослідження. Об'єкт дослідження – процес побудови системи безпеки підприємства. Предмет дослідження – моделі політики безпеки та методи оцінки і мінімізації ризиків на підприємстві. Методами дослідження є як загальнонаукові методи пізнання: порівняння, системний аналіз, так і спеціальні: методи математичного програмування, методи теорії ігор, методи оцінки ризиків, методи математичної статистики.

Наукова новизна отриманих результатів: запропонована в роботі комплексна математична модель системи безпеки враховує не лише ймовірності настання загроз, а й ймовірності спрацювання тих чи інших засобів захисту при різних видах загроз.

Практичне значення отриманих результатів полягає в тому, що запропонований метод мінімізації ризиків є досить універсальним і може бути використаним для широкого кола організацій.

Апробація. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 108 арк. формату А4, ілюстративна частина– 10 слайдів.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі сформульовано актуальність досліджень методів оцінки та мінімізації ризиків інформаційної безпеки та сформульовано мету і основні завдання роботи.

У першому розділі проведено аналітичний огляд політики безпеки інформації, світових стандартів із захисту даних, розглянуто поняття ризиків та основні методи їх оцінки.

У другому розділі наведено основну інформацію щодо побудови моделі загроз та порушника. Визначено, що це є одним з основних етапів побудови подітики безпеки на підприємстві. Наведено причини порушення інформаційної безпеки.

У третьому розділі наведено основні засади теорії ігор, побудовано оптимізаційну задачу мінімізації ризиків при заданих обмеженнях на виділені ресурси, проведено зведення нелінійної задачі до лінійної, проведено дослідження щодо статистичних даних ризиків та ймовірності спрацювання різних засобів захисту на ті чи ніші ризики, результати якого використано для практичної частини роботи.

В **спеціальній частині** описано середовище розробки Matlab та функції, які використовуються для розв'язку задач математичного програмування

В розділі "**Обґрунтування економічної ефективності**" проведено оцінку основних показників економічної ефективності проекту.

В підрозділі "**Охорона праці**" висвітлено питання, що стосуються стандарту OHSAS 18001 та дій керівництва у разі нещасного випадку на виробництві. В підрозділі "**Безпека життєдіяльності**" описано надійність захисту персоналу та питання безпеки життєдіяльності при роботі з ПК

В розділі "**Екологія**" проведено аналіз сучасних програмних продуктів для обробки великих масивів екологічної інформації та наведено вимоги до моніторів.

У загальних висновках щодо дипломної роботи наведено короткий опис основної частини; сформульовано основні результати, отримані в роботі.

В додатках до пояснювальної записки приведено тези.

В ілюстративній частині приведено Рівні політики інформаційної безпеки, Причини порушень інформаційної безпеки, Схема гри «Зловмисник-захисник», Математична модель, Вихідні дані – модель загроз, Дані для побудови платіжної матриці гри, Побудова системи захисту в залежності від виділених ресурсів Висновки.

ВИСНОВКИ

В результаті виконання дипломної роботи було:

- проведено літературних джерел в області досліджень;
- досліджено математичні підходи для формування політики безпеки;
- розглянуто модель загроз та порушника;
- створено математичну модель у формі гри конфліктуючих сторін – захисника та зловмисника;
- запропоновано метод мінімізації ризиків в залежності від виділених ресурсів.
- проведено вибір компонентів системи захисту організації для практичної задачі на основі оцінок ризиків та ефективності тих чи інших засобів захисту, доступних в інтернеті..

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Омелянюк Д. МІНІМІЗАЦІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПОБУДОВІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ [Текст] / Омелянюк Д. Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11 – 12 грудня 2019 р.), ТНТУ, 2019. – с.77

АНОТАЦІЯ

В роботі проведено огляд літературних джерел в області дослідження. Проведено порівняльний аналіз методів оцінки ризиків та класифікаційних моделей загроз та порушника. Визначено, що одним із основних етапів розробки політики безпеки на підприємстві є управління ризиками, що включає в себе методи їх оцінки та мінімізації. Запропоновано метод мінімізації ризиків інформаційної системи, що дозволяє формувати структуру системи захисту інформації з мінімальними значення ризику інформаційної безпеки. Використання математичного апарату теорії ігор, у тому числі максимінної стратегії, забезпечує отримання мінімального гарантованого значення ризику інформації, що відрізняє розроблений підхід від методів експертної оцінки. Розроблений підхід є гнучким, що дозволяє змоделювати поведінку порушників різного типу.

Ключові слова: ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА ЗАХИСТУ, РИЗИК, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ТЕОРІЯ ІГОР, ДЕТЕРМІНОВАНА ГРА.

ANNOTATION

The paper reviews literature sources in the field of research. A comparative analysis of risk assessment methods and classification models of threats and offenders is conducted. It has been determined that one of the main stages of enterprise security policy development is risk management, which includes methods of their assessment and minimization. The method of minimizing the risks of the information system is proposed, which allows to form the structure of the information security system with minimal values of the risk of the information security. The use of mathematical core of game theory, including the maximum strategy, ensures the minimum guaranteed value of information risk, which distinguishes the developed approach from the methods of expert evaluation. The developed approach is flexible, allowing to model the behavior of offenders of different types.

Key words: INFORMATION SECURITY POLICY, PROTECTION SYSTEM, RISK, INFORMATION AND COMMUNICATION SYSTEM, OFFENDER MODEL, THREAT MODEL, GAME THEORY, DETERMINISTIC GAME.