

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Факультет систем управління літальних апаратів

Кафедра комп'ютерних наук та інформаційних технологій

Пояснювальна записка
до кваліфікаційної роботи
(тип кваліфікаційної роботи)

_____магістра

(освітній ступінь)

на тему «Імітаційне моделювання ризиків кіберзагроз та ефективності заходів
безпеки для підприємств»

ХАІ.302.366.23О.122. 1122244 ПЗ

Виконав: студент 6 курсу групи № 366
Спеціальність 122 «Комп'ютерні науки»
(код та найменування)

Освітня програма Комп'ютеризація
обробки інформації та управління

_____Сергійчук А.А.

(прізвище й ініціали студента)

Керівник: _____доц. каф. 302, к.т.н.

_____Малєєва Ю.А.

(прізвище й ініціали)

Рецензент: _____Гамаюн І.П.

(прізвище й ініціали)

Харків – 2023

Міністерство освіти і науки України
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

Факультет систем управління літальних апаратів
 Кафедра комп'ютерних наук та інформаційних технологій
 Рівень вищої освіти другий (магістерський)
 Галузь знань 12 «Інформаційні технології»
 (код та найменування)
 Спеціальність 122 «Комп'ютерні науки»
 Освітня програма Комп'ютеризація обробки інформації та управління

ЗАТВЕРДЖУЮ

Завідувач кафедри

Олег ФЕДОРОВИЧ

(підпис)

(ім'я та прізвище)

«07» листопада 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Сергійчуку Андрію Анатолійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Імітаційне моделювання ризиків кіберзагроз та ефективності заходів безпеки для підприємств

керівник кваліфікаційної роботи Малєєва Ю.А., к.т.н., доц. каф. 302,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Університету № 1968-уч. від « 06» листопада 2023 року

2. Термін подання студентом кваліфікаційної роботи 10.01.2024

3. Вихідні дані до проекту (роботи) статистичні дані щодо кібербезпеки підприємств, оцінки витрат на контроль та захист

4. Зміст пояснювальної записки (перелік завдань, які потрібно розв'язати) аналіз проблем кібербезпеки малих підприємств; аналіз існуючих моделей для встановлення пріоритетів засобів контролю та захисту від кіберзагроз; розробка імітаційної моделі кіберзагроз; розробка механізмів моделювання та розрахунку параметрів; проведення експериментів з моделювання кіберзагроз для малих підприємств та аналіз результатів

5. Перелік графічного матеріалу моделювання ризиків кіберзагроз та ефективності заходів безпеки; ціль та задачі дослідження; важливість моделювання кібератак; модель аналізу кібербезпеки для малих підприємств;

модель агенту зловмисника ThreatActor; модель агенту елемента керування Control; модель агенту вузла мережі NetworkNode; база даних для моделі; розрахункові моделі; алгоритми системи; візуалізація результатів; хід моделювання; експеримент 1 для малого бізнесу з 5 працівниками; експеримент 2 для малого бізнесу з 25 працівниками; експеримент 3 для малого бізнесу з 50 працівниками; випробувальний стенд у процесі моделювання

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
з основної частини	Малєєва Ю. А. доц. каф. 302		
з спеціального розділу	Малєєва Ю. А. доц. каф. 302		
з економіки та управління	Малєєва Ю. А. доц. каф. 302		

Нормоконтроль _____ Олександр ПРОХОРОВ «__» _____ 20__ р.
(підпис) (імя та прізвище)

7. Дата видачі завдання «_06_» _вересня_ 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	АНАЛІЗ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ТА ОСОБЛИВОСТЕЙ МОДЕЛЮВАННЯ ЗАСОБІВ КОНТРОЛЮ ТА ЗАХИСТУ	06.09 – 20.09	
2	ПОБУДОВА ІМІТАЦІЙНОЇ МОДЕЛІ КІБЕРЗАГРОЗ	21.09 – 28.09	
3	РОЗРОБКА АЛГОРИТМІВ ТА ВІЗУАЛІЗАЦІЇ ІМІТАЦІЙНОЇ МОДЕЛІ КІБЕРЗАГРОЗ	29.09 – 20.11	
4	ПРОВЕДЕННЯ ЕКСПЕРИМЕНТІВ З ІМІТАЦІЙНОЮ МОДЕЛЮ	21.11 – 20.12	
5	ЕКОНОМІЧНІ РОЗРАХУНКИ	20.12 – 25.12	

Студент _____ Андрій СЕРГІЙЧУК
(підпис) (імя та прізвище)

Керівник кваліфікаційної роботи _____ Юлія МАЛЄЄВА
(підпис) (імя та прізвище)

УДК 004.8

РЕФЕРАТ

Імітаційне моделювання ризиків кіберзагроз та ефективності заходів безпеки для підприємств – Сергійчук Андрій, кваліфікаційна робота магістра, Харків, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», кількість сторінок, враховуючи додатки 81, кількість таблиць 26, кількість рисунків 30, кількість джерел літератури 20.

КЛЮЧОВІ СЛОВА: кіберзагрози, безпека, імітаційна модель, бюджет, рентабельність інвестицій.

ЦІЛЬ: підвищення ефективності заходів для захисту від кібератак для малих підприємств, щоб максимізувати віддачу від інвестицій в умовах обмежень бюджету та нестачі персоналу.

ОБ’ЄКТ ДОСЛІДЖЕННЯ: процеси захисту від кібератак.

ПРЕДМЕТ ДОСЛІДЖЕННЯ: методи, моделі та засоби максимізації загальної безпеки організації від кібератак в умовах обмежень бюджету та нестачі персоналу.

ЗАДАЧІ:

- аналіз проблем кібербезпеки малих підприємств;
- аналіз існуючих моделей для встановлення пріоритетів засобів контролю та захисту від кіберзагроз;
- розробка імітаційної моделі кіберзагроз;
- розробка механізмів моделювання та розрахунку параметрів;
- проведення експериментів з моделювання кіберзагроз для малих підприємств та аналіз результатів.

МЕТОДИ ДОСЛІДЖЕННЯ: методи кібербезпеки, економічні методи, імітаційне моделювання.

ОТРИМАНІ РЕЗУЛЬТАТИ: розроблено імітаційну модель оцінки ризиків кіберзагроз та ефективності заходів безпеки для малих підприємств.

UDC 004.8

ABSTRACT

Simulation modeling of cyber threat risks and the effectiveness of security measures for enterprises – Andriy Sergiychuk, Master Thesis, Kharkiv, National Aerospace University “KhAI”, amount of pages 81, amount of tables 26, amount of figures 30, amount of literature’s sources 20.

KEYWORDS: cyber threats, security, simulation model, budget, return on investment.

PURPOSE OF RESEARCH: Increase the effectiveness of cyber defence measures for small businesses to maximise the return on investment in the face of budgetary constraints and staff shortages.

OBJECT OF RESEARCH: processes to protect against cyber attacks.

SUBJECT OF RESEARCH: methods, models and tools for maximising the overall security of an organisation against cyberattacks in the face of budgetary constraints and staff shortages.

TASKS:

- Analysis of cybersecurity issues of small businesses;
- analysis of existing models to prioritise control and protection against cyber threats;
- development of a simulation model of cyber threats;
- development of modelling and parameter calculation mechanisms;
- conducting experiments on modelling cyber threats to small businesses and analysing the results.

METHODS OF RESEARCH: cybersecurity methods, economic methods, simulation modelling.

RESULTS: a simulation model for assessing the risks of cyber threats and the effectiveness of security measures for small businesses was developed.

ЗМІСТ

ВСТУП.....	8
1 АНАЛІЗ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ТА ОСОБЛИВОСТЕЙ МОДЕЛЮВАННЯ ЗАСОБІВ КОНТРОЛЮ ТА ЗАХИСТУ	9
1.1 Важливість моделювання кібератак	9
1.2 Вартість і поширеність інцидентів кібербезпеки	11
1.3 Структури для максимального підвищення загальної безпеки	12
1.4 Основи максимізації бюджетів безпеки	14
1.4 Оцінка бюджетів кібербезпеки	17
1.5 Існуючі моделі для встановлення пріоритетів засобів контролю безпеки....	17
1.6 Загальні вектори атак та ефективність індивідуальних заходів безпеки	19
1.7 Роль суб'єктів загрози	21
1.8 Вартість індивідуальних заходів безпеки	22
Висновки за розділом.....	24
2 ПОБУДОВА ІМІТАЦІЙНОЇ МОДЕЛІ КІБЕРЗАГРОЗ.....	25
2.1 Основні положення при моделюванні	25
2.2 Розробка існуючих оцінок витрат	25
2.3 Кількісна оцінка ефективності суб'єкта загрози	30
2.4 Оцінка вартості витоків даних.....	33
2.5 Оцінка річного чистого прибутку та ROI	33
Висновки за розділом.....	36
3 РОЗРОБКА АЛГОРИТМІВ ТА ВІЗУАЛІЗАЦІЇ ІМІТАЦІЙНОЇ МОДЕЛІ КІБЕРЗАГРОЗ	37
3.1 Оптимізація для річного чистого прибутку та ROI.....	37
3.2 Проведення однорічної симуляції	38
3.3 Візуалізація	41
Висновки за розділом.....	45
4 ПРОВЕДЕННЯ ЕКСПЕРИМЕНТІВ З ІМІТАЦІЙНОЮ МОДЕЛЮ	46
4.1 Випробувальний стенд для моделювання.....	46
4.2 Експеримент для малого бізнесу з 5 працівниками	47
4.3 Експеримент для малого бізнесу з 25 працівниками.....	50
4.4 Експеримент для малого бізнесу з 50 працівниками.....	53
4.5 Обмеження та результати	56
Висновки за розділом.....	57
5 ЕКОНОМІЧНИЙ РОЗДІЛ	58
5.1 Мета розділу	58
5.2 Визначення тривалості та розрахунок собівартості виконання проекту (перший варіант)	58

5.3 Визначення тривалості та розрахунок собівартості виконання проекту (другий варіант).....	64
5.4 Висновки за розділом	68
ВИСНОВКИ	69
ПЕРЕЛІК ПОСИЛАНЬ	70
ДОДАТОК А. Графічні матеріали	72

ВСТУП

Актуальність теми дослідження.

Підприємства будь-якого розміру стикаються з постійно зростаючою загрозою кібератак. Успішні кібератаки можуть призвести до витоку даних, що може призвести до фінансових втрат, перерв у бізнесі, регулятивних штрафів і шкоди репутації. Протистояти загрозі кібератак може бути особливо складно для малого бізнесу, який повинен захищатися, використовуючи менший бюджет і меншу кількість кадрів, збалансовуючи прагнення до зростання. Оцінка ризиків є одним із методів для організацій визначити, як найкраще використовувати свої бюджети на кібербезпеку. Однак для малих підприємств оцінка ризиків може вимагати значної частини бюджету, який інакше можна було б використати для впровадження засобів контролю кібербезпеки. Це дослідження присвячено моделюванню фішингової атаки, щоб представити, які стратегії захисту малий бізнес може використовувати та оцінити ризики.

Мета дослідження – підвищення ефективності заходів для захисту від кібератак для малих підприємств, щоб максимізувати віддачу від інвестицій в умовах обмежень бюджету та нестачі персоналу.

Для досягнення мети необхідно виконати наступні **завдання**:

- аналіз проблем кібербезпеки малих підприємств;
- аналіз існуючих моделей для встановлення пріоритетів засобів контролю та захисту від кіберзагроз;
- розробка імітаційної моделі кіберзагроз;
- розробка механізмів моделювання та розрахунку параметрів;
- проведення експериментів з моделювання кіберзагроз для малих підприємств та аналіз результатів.

Об'єкт дослідження – процеси захисту від кібератак.

Предмет дослідження – методи, моделі та засоби максимізації загальної безпеки організації від кібератак в умовах обмежень бюджету та нестачі персоналу.

Практичне значення отриманих результатів. Розроблено імітаційну модель оцінки ризиків кіберзагроз та ефективності заходів безпеки для малих підприємств.

Структура та обсяг кваліфікаційної роботи магістра. Кваліфікаційна робота магістра складається зі вступу, 5 розділів, висновків, додатків та переліку посилань. Повний обсяг кваліфікаційної роботи магістра становить 81 сторінку, в тому числі: 30 рисунків; 26 таблиць; 1 додаток на 12 сторінках; перелік посилань з 20 найменувань на 2 сторінках.