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

ТЛУСТИЙ ЮРІЙ ОЛЕКСАНДРОВИЧ

УДК 004.021

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ РИЗИКІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

8.05010201 «Комп’ютерні системи та мережі»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2017

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доцент кафедри інформатики і математичного моделювання
Баран Ігор Олегович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри автоматизації технологічних процесів та виробництв
Медвідь Володимир Романович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 22 лютого 2017 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №35 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд.603.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. На даний час організація режиму інформаційної безпеки стає критично важливим стратегічним чинником розвитку будь-якої компанії. При цьому, як правило, основна увага приділяється вимогам і рекомендаціям відповідної нормативно-методичної бази в галузі захисту інформації. Разом з тим багато провідних компаній сьогодні використовують деякі додаткові ініціативи, спрямовані на забезпечення стійкості і стабільності функціонування корпоративних інформаційних систем для підтримки безперервності бізнесу в цілому.

Однією з таких ініціатив є використання мобільних пристроїв для ведення бізнесу. На даний час мобільні пристрої стали поширеним засобом доступу до інформації, додатків та ведення бізнесу, в той же час створюючи нові можливості загроз.

Незважаючи на постійно зростаючий ризик ІБ, підприємства все частіше переходять на використання мобільних пристроїв. Варто зазначити, що пов'язаний з мобільними пристроями ризик ІБ збільшується за рахунок їх зростаючої популярності, збільшення потужностей апаратної частини, функціональності операційних систем та додатків та особливої уваги до них з боку кіберзлочинців. Тому підвищення рівня захисту інформації, що циркулює в інформаційній системі підприємства з елементами мобільних технологій являє собою актуальну задачу.

Мета роботи: Підвищення рівня захисту інформації, що циркулює в інформаційній системі підприємства з використанням мобільних бізнес-рішень.

Об’єкт, методи та джерела дослідження. Процес оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень на підприємстві та в бізнесі.

Наукова новизна отриманих результатів:

Досліджено ризики та загрози інформаційній безпеці при реалізації та використанні мобільних пристроїв. Для дослідження обрано кількісні методи оцінки ризиків. Створено методику оцінки ризиків інформаційній безпеці при реалізації та використанні бізнес-рішень. Розроблено модель оцінки ризиків та загроз для оцінки ризиків інформаційній безпеці при реалізації та використанні бізнес-рішень.

Практичне значення отриманих результатів.

Розроблений програмний продукт може застосовуватися для оцінки ризиків інформаційній безпеці організацій усіх сфер діяльності, так як він характеризує інформаційну систему з боку ризиків і відповідно може бути конкретизована під конкретну організацію

Апробація. Окремі результати роботи доповідались на V Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій», Тернопіль, ТНТУ, 17-18 листопада 2016 року.

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 – *126* арк. формату А4, графічна частина – 9 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі наведено актуальність організації режиму інформаційної безпеки на підприємстві.

В першому розділі розглянуто методи кількісної оцінки ризиків, так як вони дозволяють точно оцінити економічні втрати підприємства. Існують обмеження в застосуванні відомих методів кількісної оцінки ризиків у сфері безпеки інформації, у зв'язку з чим пошук нових підходів, які забезпечують вирішення задач визначення характеристик ймовірності (випадковості) безпеки інформації в умовах недостатніх статистик, являє собою актуальну задачу.

Для визначення переваг та недоліків існуючих програмних продуктів системи захисту інформації ГРИФ, RiskWatch та CRAMM для оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень проведено їх порівняльний аналіз.

Інформаційним системам (ІС), заснованим на мобільних технологіях, притаманні всі загрози, що і звичайним ІС. Але існують і специфічні для мобільних пристроїв загрози. В результаті аналізу для оцінки ризиків та загроз інформаційній безпеці при використанні мобільних пристроїв обрано програмний продукт ГРИФ. Він простий у використанні, не потребує спеціальної підготовки, дозволяє додавати власні загрози та вразливості, має невисоку вартість ліцензії.

Визначено основні етапи дослідження ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень.

В другому розділі для розв’язання задачі кількісної оцінки ризиків були розглянуті два методи: ймовірнісно-статистичний та експертний.

Розроблена методика оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень в інформаційній системі підприємства та визначенні основні поняття методики.

Сформульована математична постановка задачі оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес рішень.

В третьому розділі розроблений алгоритм оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень на підприємстві. Спроектована база даних для оцінки ризиків та загроз інформаційній безпеці підприємства, побудована фізична модель бази даних, створена програмна реалізація бази даних. Було проведене дослідження оцінки ризиків та загроз інформаційній безпеці на онові контрольного прикладу. Для дослідженні використовувалися розроблений програмний продукт та вже існуючий програмний продукт «Гриф». Аналіз отриманих результатів свідчить про високий рівень адекватності та достовірності оцінок ризиків ІБ отриманих за допомогою розробленого програмного продукту та програмного продукту «Гриф».

В спеціальній частині було проаналізовано різні типи атак. Найбільш серйозні атаки на ІТ-системи спрямовані на системи комунікацій, тобто на обмін повідомленнями по комунікаційних каналах в Internet і intranet. Можна класифікувати два типи атак: пасивні і активні.

Пасивні атаки можуть проводитися, наприклад, підключенням затисків, введенням в лінію петель або перехоплюванням сигналів за допомогою спрямованих радіо- і супутникових з'єднань.

Активні атаки можна розбити на дві категорії: атаки, які здійснюються третьою стороною, і атаки, які здійснюються партнерами по комунікаціях. Розрізняють наступні погрози, які виходять від третьої сторони.

При оцінці можливості атаки значну роль грають наступні три чинники:

– чинник місця;

– чинник міри використання даних;

– чинник кількості технічних і матеріальних ресурсів, що вимагаються для здійснення атаки.

В частині «Обґрунтування економічної ефективності» розраховано основні техніко-економічні показники науково-дослідної роботи.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання інженерного захисту персоналу, де застосовується комп'ютерна техніка. Було розглянуто заходи захисту населення в місцях масового скупчення людей та заходи особистої кримінологічної безпеки.

В частині «Екологія» розглянуто інформаційне забезпечення еколого-статистичних досліджень та моніторинг довкілля та система спостережень за впливом на довкілля антропологічних факторів.

У загальних висновках щодо дипломної роботи описано прийняті в роботі технічні рішення.

В графічній частині приведено класифікація загроз для мобільних пристроїв, число доданих сигнатур для нового мобільного шкідливого ПЗ під різні платформи, модель оцінки ризиків та загроз, схема алгоритму «Оцінка ризиків та загроз», опис класів, які реалізують основну бізнес-логіку програмного продукту, фізична модель даних, інтерфейс програмного комплексу.

ВИСНОВКИ

В роботі проаналізовано методи оцінки ризиків інформаційній безпеці, побудовано модель оцінки ризиків та загроз для оцінки ризиків інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень, розроблено програмний продукт, який являє собою систему, здатну вести список ресурсів, загроз, вразливостей, контрзаходів, користувачів системи та проводити оцінку ризиків для кожного ресурсу підприємства. Досліджено ризики та загрози інформаційній безпеці при реалізації та використанні мобільних пристроїв. Для дослідження обрано кількісні методи оцінки ризиків. У результаті кількісної оцінки можна більш точно порівнювати декілька варіантів захисту ІС і таким чином вибирати найбільш ефективний. Створено методику оцінки ризиків інформаційній безпеці при реалізації та використанні бізнес-рішень. Визначено основні поняття методики. Розроблено модель оцінки ризиків та загроз для оцінки ризиків інформаційній безпеці при реалізації та використанні бізнес – рішень. Спроектовано базу даних для оцінки ризиків та загроз інформаційній безпеці СЗІ підприємства, побудовано логічну та фізичну моделі бази даних, створено програмну реалізація

бази даних. Вхідними даними є ймовірності реалізації загроз і вразливостей для кожного ресурсу, вартість ресурсів, що захищаються (оцінка втрат у разі виходу з ладу інформаційного ресурсу). Вихідними даними є кількісна та якісна оцінка для кожного ризику підприємства. Для дослідженні використовувалися розроблений програмний продукт та вже існуючий програмний продукт «Гриф». В результаті проведеного дослідження можна зробити висновок про можливість використання даного програмного продукту для оцінки ризиків та загроз інформаційній безпеці на підприємстві.

Інформаційна система створена на платформі .NET у програмному продукті Microsoft Visual Studio 2010. Програмний продукт реалізував всі необхідні функції. Написано на мові програмування C#.

Розроблений програмний продукт може застосовуватися для оцінки ризиків інформаційній безпеці організацій усіх сфер діяльності, так як він характеризує інформаційну систему з боку ризиків і відповідно може бути конкретизована під конкретну організацію. З іншого боку, враховуючи дуже динамічний розвиток автоматизації процесів розробки програмного забезпечення, даний програмний продукт оцінки ризиків та загроз інформаційній безпеці в системи захисту інформації підприємства дозволяє адміністраторам інформаційної безпеки, на відміну від розглянутих прототипів, вносити доповнення до база даних загроз та вразливостей, що дозволить оцінити ризики для мобільних пристроїв. Ступінь конкретизації залежить від рівня зрілості організації, специфіки її діяльності, необхідного рівня захищеності, моделі зловмисника та інших чинників. Тобто в кожному конкретному випадку програмний продукт може бути адаптовано під конкретні потреби підприємства з урахуванням специфіки його функціонування та ведення бізнесу.

Рівень точності одержуваної на виході оцінки залежить в першу чергу від повноти списку загроз і вразливостей, як основних складових ризику, точності оцінки інформаційних ресурсів, а також точності оцінки ймовірнісних характеристик реалізації загроз. Для оцінки цих характеристик може знадобитися залучення, як технічних фахівців, так і представників управління самої компанії, що дозволить надалі результативніше фінансувати і контролювати процес впровадження системи захисту інформації.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Ю.О. Тлустий. Дослідження методів вирішення задач оцінки загроз інформаційній безпеці при використанні бізнес-рішень / Тлустий Ю.О. – Тези доповіді на V Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій». Том II, Тернопіль, 17-18 листопада 2016 року.– Тернопіль, ТНТУ, 2016. – с. 118-119.

АНОТАЦІЯ

Тлустий Ю.О. Дослідження методів оцінки ризиків в інформаційній безпеці.

Дипломна робота на здобуття освітнього ступеня магістра 8.05010201 – Комп'ютерні системи та мережі. – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль 2017.

В дипломній роботі розглянуто методи кількісної оцінки ризиків, так як вони дозволяють точно оцінити економічні втрати підприємства. Існують обмеження в застосуванні відомих методів кількісної оцінки ризиків у сфері безпеки інформації, у зв'язку з чим пошук нових підходів, які забезпечують вирішення задач визначення характеристик ймовірності (випадковості) безпеки інформації в умовах недостатніх статистик, являє собою актуальну задачу.

Визначено основні етапи дослідження ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень.

Були розглянуті два методи: ймовірнісно-статистичний та експертний. Розроблена методика оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень в інформаційній системі підприємства та визначенні основні поняття методики.

Сформульована математична постановка задачі оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес рішень.

Розроблений алгоритм оцінки ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень на підприємстві. Спроектована база даних для оцінки ризиків та загроз інформаційній безпеці підприємства, побудована фізична модель бази даних, створена програмна реалізація бази даних. Було проведене дослідження оцінки ризиків та загроз інформаційній безпеці на онові контрольного прикладу. Для дослідженні використовувалися розроблений програмний продукт та вже існуючий програмний продукт «Гриф». Аналіз отриманих результатів свідчить про високий рівень адекватності та достовірності оцінок ризиків ІБ отриманих за допомогою розробленого програмного продукту та програмного продукту «Гриф».

Ключові слова: ІНФОРМАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, АНАЛІЗ РИЗИКІВ, ОЦІНКА РИЗИКІВ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, РИЗИК, КОНТРЗАХІД, МОБІЛЬНИЙ ПРИСТРІЙ, СИСТЕМА.

ANNOTATION

Tlustyi Y.O. Analysis of information security risk assessment methods.

The diploma paper for obtaining the Master's degree 8.05010201 – Computer systems and networks – Ivan Puluj Ternopil National Technical University, Ternopil 2017.

Detection of threats, vulnerabilities of mobile devices and their removal will reduce the economic losses of the company. The methods of quantitative risk assessment because they can accurately assess the economic costs of the company.

. There are limitations in the application of known methods of quantitative risk assessment in the field of information security, and therefore the search for new approaches that provide a solution to problems of determination of the probability (chance) of information security in poor statistics, is the actual problem.

The basic stages of research risks and threats to information security in the implementation and use of mobile business solutions.

In the second section were considered two methods: probabilistic and statistical and expert. The method of risk assessment and information security threats in the implementation and use of mobile business solutions in the enterprise information system and determining the basic concepts of the methodology.

Formulated mathematical formulation of the problem of risk assessment and information security threats in the implementation and use of mobile business solutions.

Designed database to assess the risks and threats to information security company, the physical model database created software implementation database. A study was conducted risk assessments and information security threats to refresh the test case. To study used the software developed and existing software "Grief." Analysis of the results indicates a high level of reliability and adequacy of information security risk assessments obtained by the developed software and the software "Grief."

Keywords: INFORMATION SYSTEMS, INFORMATION SECURITY, INFORMATION SECURITY, RISK ANALYSIS, RISK ASSESSMENT, THREAT, VULNERABILITY, RISK, COUNTERMEASURE, MOBILE DEVICE, SYSTEM.