РЕЦЕНЗІЯ

рецензента
доктора технічних наук, професора,
завідувача кафедри Технічних систем кіберзахисту
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
Туровського Олександра Леонідовича
на дисертаційну роботу **Запорожченка Михайла Михайловича** на тему:
"Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача",
подану на здобуття наукового ступеня доктора філософії за спеціальністю
125 Кібербезпека

Актуальність теми

Аналіз сучасного стану та напрямків вирішення актуальних проблем кібербезпеки та захисту інформації показує, що широке впровадження інформаційних технологій та перехід до цифровізації бізнесу, посилення стану кіберзахисту об'єктів інформаційної діяльності спонукає зловмисників до пошуку нових технологій та методів порушень цілісності та конфіденційності нформації, яка циркулює в корпоративних інформаційно-комунікаційних мережах.

Одним з таких методів є широке застосування соціоінженерних атак на користувачів корпоративної інформаційно-комунікаційної мережі об'єкту інформаційної діяльності через розгалужену мережу соціальних інформаційно-комунікаційних каналів. Особливу небезпеку становлять багатоетапні соціоінженерні атаки, які дозволяють зловмисникам поступово поширювати свій вплив у межах корпоративної інфраструктури, використовуючи взаємодію між співробітниками.

В якості ефективного підходу до протидії соціоінженерним атакам як правило розглядаються методи та технології, зосереджені на підвищенні технічного рівня захисту корпоративних мереж або втілення комплексу загальних рекомендаціях щодо кібергігієни. В свою чергу, комплексний підхід до оцінювання ймовірності компрометації користувачів з урахуванням психологічного, організаційного, технічного факторів та фактору інформаційного впливу залишається недостатньо розробленим.

Актуальність дисертаційної роботи обґрунтовується необхідністю розробки низки методів та моделей, які в комплексі повинні забезпечити підвищення рівня кіберзахисту корпоративних інформаційних систем від соціоінженерних атак, яке в даній роботі вирішується шляхом прогнозування вразливості на основі розробки профілю захищеності користувач, що функціонують в корпоративні мережі обраного об'єкту інформаційної діяльності.

Обґрунтованість наукових результатів, висновків та рекомендацій

У дисертаційній роботі використано широкий спектр сучасних методів дослідження, що забезпечує комплексний підхід до вирішення поставленого наукового

завдання. Зокрема, метод аналізу ієрархій застосовано для визначення вагових коефіцієнтів впливу факторів на рівень вразливості користувачів та обґрунтування значущості окремих характеристик профілю захищеності. Для моделювання механізмів поширення соціоінженерних атак у корпоративному середовищі ефективно використано графові моделі, що дозволило врахувати взаємозв'язки між користувачами та потенційні шляхи компрометації.

Методи статистичного аналізу застосовано для оцінки точності отриманих результатів, що підвищує обґрунтованість зроблених висновків. Використання компаративного аналізу дозволило провести критичне оцінювання існуючих методів прогнозування соціоінженерних атак, визначити їхні обмеження та порівняти ефективність запропонованого підходу. Достовірність отриманих результатів підтверджена за допомогою методів валідації, включно зі статистичним аналізом, тестуванням сценаріїв атак та експертними оцінками. Верифікація розробленого методу на основі математичного моделювання підтвердила його ефективність та практичну застосовність у корпоративних інформаційних системах різного масштабу.

Новизна наукових результатів дослідження

У дисертаційній роботі отримано нові наукові результати, що мають значення для розвитку методів прогнозування соціоінженерних атак на корпоративні інформаційні системи:

вперше розроблено комплексну модель профілю захищеності користувача як основу для інтегративного методу прогнозування соціоінженерних атак на корпоративні інформаційні системи, яка базується на мультиплікативній згортці результатів дослідження психологічного, організаційного, технічного факторів та фактору інформаційного впливу відносно конкретного користувача і дає можливість визначення потенційної вразливості користувачів організації до соціоінженерних атак;

удосконалено метод оцінки компонентів профілю захищеності користувача, який відрізняється від базового підходу, заснованого на методі аналізу ієрархій, використанням динамічно змінюваного набору показників, що забезпечує комплексну та адаптивну оцінку впливу факторів профілю захищеності на рівень вразливості користувача з урахуванням зміни його індивідуальних характеристик та специфіки організаційного середовища;

удосконалено метод виявлення найбільш ймовірних траєкторій соціоінженерних атак, який відрізняється від відомих підходів застосуванням графової моделі взаємодії користувачів корпоративної інформаційної системи з урахуванням типів і інтенсивності їх комунікаційних зв'язків, що забезпечує можливість ідентифікації найбільш уразливих користувачів і визначення критичних траєкторій багатоетапних соціоінженерних атак для оцінювання ризиків компрометації корпоративної інформаційної системи.

Практична цінність отриманих результатів

У роботі запропоновано низку рекомендацій, що сприяють підвищенню рівня захищеності корпоративної інформаційної системи від впливу соціоінженерних атак. Подані рекомендації обґрунтовані на основі особисто одержаних автором

практичних даних оцінки вразливості користувачів корпоративної інформаційної системи під впливом соціоінженерних атак.

Результати наукових досліджень прийняті до впровадження в діяльність ДП "ЕС ЕНД ТІ УКРАЇНА" та ТОВ "ІТ СПЕЦІАЛІСТ", а також реалізовані в освітньому процесі на кафедрі управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій.

Зв'язок роботи з науковими програмами, планами, темами

Напрям дослідження безпосередньо пов'язаний з реалізацією Законів України "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-комунікаційних системах", "Про інформацію", "Про захист персональних даних", "Про національну безпеку України". Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідних робіт "Кадрові технології в управлінні інформаційною безпекою підприємства" (№ держ. реєстрації 0120U105132, ДУІКТ, м. Київ), "Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства" (№ держ. реєстрації 0118U100058, ДУІКТ, м. Київ), "Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства" (№ держ. реєстрації 0123U100743, ДУІКТ, м. Київ).

Повнота викладу основних результатів дисертації в публікаціях

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. У наукових роботах, опублікованих у співавторстві, чітко визначено внесок автора. Всього за результатами дисертаційних досліджень Запорожченка М.М. опубліковано 20 наукових праць: 11 наукових статей, серед яких 3 статті опубліковані у наукових виданнях, які індексуються в міжнародних наукометричних базах Scopus та Web of 5 статей опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України, 3 статті опубліковані в інших виданнях. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 9 збірниках тез доповідей.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

Дисертація Запорожченка М.М. є завершеною науковою працею. Її обсяг, структура та зміст відповідають вимогам, що висувають до дисертацій, встановлених наказом Міністерства освіти і науки України від 12.01.2017 №40 за спеціальністю 125 Кібербезпека.

Дисертація виконана українською мовою, текстове подання матеріалу відповідає стилю наукової літератури.

Недоліки та зауваження

1. Врахування специфіки різних секторів економіки, зокрема державних установ, підприємств фінансового сектору чи критично важливої інфраструктури, могло б підвищити універсальність запропонованого методу. Особливості

організаційної структури, різноманітність інформаційних потоків і регуляторні обмеження потребують адаптації підходу до конкретних умов.

2. Розширення роботи за рахунок аналізу постінцидентного реагування могло б суттєво підвищити її практичну цінність. Такий підхід дозволив би забезпечити комплексне управління ризиками – від прогнозування до реагування на інциденти, що важливо для оперативного відновлення системи після атаки.

3. Моделювання потенційних економічних втрат дало б змогу не лише оцінити фінансові ризики соціоінженерних атак, але й обґрунтувати доцільність інвестицій у заходи та засоби захисту. Це підвищило б практичну значущість методу для прийняття управлінських рішень.

Вказані недоліки не знижують наукової цінності та практичного значення одержаних наукових результатів і не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок

Сформульована в дисертації мета досягнута і вирішене важливе наукове завдання щодо розробки інтегративного методу прогнозування соціоінженерних атак на корпоративні інформаційні системи, яке має суттєве значення для теорії та практики оцінки ризиків та вдосконалення методів забезпечення корпоративної інформаційної безпеки, спрямованих на зниження рівня вразливості користувачів до соціоінженерних атак. Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

Дисертація відповідає спеціальності 125 Кібербезпека і чинним вимогам "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а автор поданої роботи – Запорожченко Михайло Михайлович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензент
завідувач кафедри Технічних систем
кіберзахисту Державного університету
інформаційно-комунікаційних технологій,
доктор технічних наук, професор Олександр ТУРОВСЬКИЙ

Підпис д.т.н., професора О. Туровського засвідчую:

Учений секретар
Державного університету
інформаційно-комунікаційних технологій Галина ЄНЧЕВА

"11" березня 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ * ідентифікаційний код 38853249 * УКРАЇНА

Документ підписано у сервісі Вчасно (продовження)
Рецензія_О.Л.Туровський.pdf

Документ відправлено: 11:48 12.03.2025

Відправник документу

Електронний підпис
11:48 12.03.2025
Ідентифікаційний код: 2366017015
Туровський Олександр Леонідович
Власник ключа: Туровський Олександр Леонідович
Час перевірки КЕП/ЕЦП: 11:48 12.03.2025
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 382367105294AF9704000000A3C33200B0614602
Тип підпису: кваліфікований
Тип сертифікату: кваліфікований