РЕЦЕНЗІЯ

рецензента
доктора технічних наук, професора,
завідувача кафедри Систем та технологій кібербезпеки
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
Гайдур Галини Іванівни
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

Одним із ключових завдань сучасних корпоративних інформаційних систем є забезпечення стійкості їх функціонування в умовах постійної ескалації кіберзагроз, складність яких постійно зростає. Актуальні загрози інформаційній безпеці спричиняють ризики компрометації інформаційних ресурсів та активів організації, що може призвести до суттєвих негативних наслідків, зокрема втрати ділової репутації, фінансової стабільності та порушення безперервності бізнес-процесів. Аналітичні дані останніх років свідчать про те, що соціоінженерні атаки, зокрема фішинг, залишаються однією з найбільш поширених та ефективних тактик компрометації корпоративних інформаційних систем. Ці атаки базуються на маніпуляції людським фактором, що уможливлює обхід сучасних технічних засобів кіберзахисту та значно підвищує ймовірність реалізації атакувального сценарію.

Особливої актуальності дослідження набуває в умовах глобалізації кіберпростору, коли атаки можуть бути масштабовані на великі групи користувачів, а фактори впливу стають багатовимірними та динамічними. Традиційні підходи до оцінки ризиків соціоінженерних атак часто не враховують комплексну взаємодію факторів вразливості, що значно знижує ефективність контрзаходів. Таким чином, виникає потреба у розробленні нових методів прогнозування ймовірності компрометації користувачів з урахуванням багатофакторного впливу, що дозволить своєчасно виявляти критичні точки вразливості та впроваджувати адаптивні стратегії протидії.

Актуальність роботи також зумовлена необхідністю створення інструментарію для прогнозування поширення соціоінженерних атак у корпоративному середовищі, що дозволить оптимізувати процеси управління інформаційною безпекою та підвищити ефективність системи захисту на стратегічному рівні. Використання запропонованого підходу дозволить посилити не лише захищеність окремих користувачів, але й знизити ризик ескалації атак на критично важливі інформаційні активи організацій.

Тому розробка методів прогнозування соціоінженерних атак для створення профілю захищеності користувачів та моделювання можливих

траєкторій таких атак на корпоративну інформаційну систему є надзвичайно актуальним завданням і має вагоме значення як для теоретичних досліджень, так і для практичної діяльності у сфері кібербезпеки.

Обґрунтованість наукових результатів, висновків та рекомендацій

Достовірність отриманих наукових результатів Запорожченка М.М. забезпечується використанням апробованого математичного апарату та збіжністю теоретичних результатів з результатами моделювання на основі експертних оцінок, побудованих на основі аналізу 1000 аналогічних випадків, що гарантує середню похибку у 2,4% з ймовірністю $p = 0{,}95$.

Новизна наукових результатів дослідження

Метою дослідження є підвищення рівня захищеності корпоративних інформаційних систем від соціоінженерних атак на основі прогнозування вразливості шляхом створення профілю захищеності користувача.

Для досягнення мети дослідження автором одержано нові наукові результати:

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

Практичне значення отриманих результатів полягає у тому, що запропонований метод прогнозування соціоінженерних атак на корпоративні інформаційні системи дозволяє оцінювати ймовірність компрометації користувачів, визначати найбільш вразливі категорії та впроваджувати цільові контрзаходи, що підвищує загальний рівень безпеки

корпоративної інформаційної системи. В запропонованому методі оцінки компонентів профілю захищеності користувача впроваджено критерії для оцінювання психологічного, організаційного, технічного факторів та фактору інформаційного впливу, які можуть бути використані фахівцями з кібербезпеки для формування адаптивних стратегій протидії соціоінженерним загрозам при оцінці ризиків.

Зв'язок роботи з науковими програмами, планами, темами

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), де автором запропоновані рекомендації щодо навчання співробітників і підвищення їх стійкості до соціоінженерних загроз через цільові тренінги та практичні симуляції, визначено ризики, пов'язані із використанням методів соціальної інженерії в конкурентній розвідці, розроблено заходи для їх виявлення і мінімізації, а також здійснено класифікацію соціоінженерних загроз у соціальних мережах із формуванням рекомендацій щодо їх протидії.

Повнота викладу основних результатів дисертації в публікаціях

За результатами дисертаційних досліджень Запорожченка М.М. опубліковано 20 наукових праць. Основні наукові результати викладені в 11 наукових статтях, серед яких 3 статті опубліковані у наукових виданнях, які індексуються в міжнародних наукометричних базах Scopus та Web of Science, 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. В роботі не вказано, яким чином розрахована оцінка фактору

інформаційного впливу на профіль захищеності користувача. Доцільно було б показати шкалу щодо зміни цих значень для кращого розуміння рівня захищеності профіля користувача.

2. На ст. 153 для підтвердження проходження одноетапної атаки проведено аналіз чутливості моделі, який дозволив оцінити внесок кожного коригувального коефіцієнта у загальну ймовірність успішності атаки, але формулу розрахунку автор в роботі не відобразив.

3. Прогнозування траєкторій атак та оцінка ймовірності компрометації користувачів внаслідок багатоетапної соціоінженерної атаки доцільно було висвітлити порівняння на ієрархічній графовій моделі взаємозв'язків користувачів в інформаційній системі організації.

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

Висновок

За рівнем наукової новизни, якістю досліджень, достовірністю та обґрунтованістю висновків дисертація Запорожченка М.М. на тему "Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача" відповідає спеціальності 125 Кібербезпека і чинним вимогам п. 6-9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", затвердженому 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 Систем та технологій
кібербезпеки Державного університету
інформаційно-комунікаційних технологій,
доктор технічних наук, професор Галина ГАЙДУР

Підпис д.т.н., професора Г. Гайдур засвідчую:

Учений секретар
Державного університету
інформаційно-комунікаційних технологій Галина ЄНЧЕВА

"10" Березня 2025 р.