Голові разової спеціалізованої
вченої ради Державного
університету інформаційно-
комунікаційних технологій
доктору технічних наук, професору
Віталію САВЧЕНКУ
вул. Солом'янська, 7, м. Київ, 03110

ВІДГУК

офіційного опонента
кандидата технічних наук, доцента,
завідувача кафедри Інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка
Складанного Павла Миколайовича
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

Зростання кількості соціоінженерних атак на корпоративні інформаційні системи вимагає пошуку нових підходів до їх прогнозування та запобігання. Традиційні методи кіберзахисту зосереджені переважно на технічних засобах, часто залишаючи поза увагою людський фактор як одну з головних причин успішних атак. Використання соціоінженерних технік дозволяє зловмисникам впливати на поведінку користувачів, обходячи технічні бар'єри захисту, що робить такі загрози особливо небезпечними для сучасних організацій.

Відсутність комплексного підходу до оцінки вразливості користувачів із урахуванням взаємодії психологічних, організаційних, технічних та інформаційних факторів значно ускладнює прогнозування ймовірності успішних атак, що обумовлює актуальність теми дослідження та поставленого наукового завдання. Особливої актуальності дослідження набуває в умовах динамічного розвитку цифрового середовища, коли масштаби й інтенсивність взаємодії між користувачами можуть впливати на ризик поширення атак всередині організації.

В дисертаційній роботі автором пропонується метод прогнозування соціоінженерних атак на основі оцінки профілю захищеності користувача, що дозволяє ідентифікувати вразливі категорії користувачів, оцінювати ризики багатоетапних атак та формувати адаптивні стратегії захисту, що має важливе практичне значення для підвищення рівня безпеки корпоративних інформаційних систем.

Обґрунтованість наукових результатів, висновків та рекомендацій

Обґрунтованість і достовірність наукових результатів, висновків та рекомендацій, викладених у дисертації, забезпечується чіткою постановкою наукового завдання, ґрунтовним аналізом широкого кола науково-технічних джерел за тематикою роботи, а також всебічним теоретичним та експериментальним опрацюванням об'єкта дослідження. Достовірність отриманих результатів підтверджується застосуванням перевірених методів, зокрема: метод експертного оцінювання використано для визначення вагових коефіцієнтів впливу факторів на вразливість користувачів, метод аналізу ієрархій – для обґрунтування значущості характеристик профілю захищеності. Для моделювання поширення соціоінженерних атак у корпоративному середовищі ефективно застосовано графові моделі, що дало змогу врахувати взаємозв'язки між користувачами та ідентифікувати потенційні траєкторії компрометації.

Новизна наукових результатів дослідження

Наукова новизна одержаних результатів полягає у тому, що в дисертаційній роботі:

вперше розроблено комплексну модель профілю захищеності користувача як основу для 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

Запропонований у дисертаційній роботі метод прогнозування соціоінженерних атак на корпоративні інформаційні системи дозволяє оцінити ймовірність компрометації користувачів, ідентифікувати найбільш вразливі категорії та впроваджувати цільові заходи захисту, що значно підвищує рівень безпеки корпоративного середовища. Впровадження рекомендованих заходів сприяло підвищенню захищеності від одноетапних соціоінженерних атак на 10,3% – 42,8% залежно від категорії користувачів, а загальне зниження ймовірності компрометації внаслідок багатоетапних атак становить у середньому 21% (від 19% до 24,3%).

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота Запорожченка М.М. 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

Наукові результати дисертаційної роботи Запорожченка М.М. опубліковані у 20 наукових працях, 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:

1) V Всеукраїнська науково-практична конференція молодих учених, студентів і курсантів (26 листопада 2021 року);

2) Всеукраїнська науково-практична Інтернет-конференція "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" (24 лютого 2022 року);

3) Всеукраїнська науково-практична конференція "Актуальні проблеми кібербезпеки" (27 жовтня 2022 року);

4) Всеукраїнська науково-практична конференція "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" (23 лютого 2023 року);

5) IV міжнародна науково-практична конференція "Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи" (27 вересня 2023 року);

6) IV міжнародна науково-практична конференція "The World of

Modern Technologies and Inventions" (10-13 жовтня 2023 року);

7) Всеукраїнська науково-практична конференція "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" (28 лютого 2024 року);

8) XIII Міжнародна науково-технічна конференція "ITSec: Безпека інформаційних технологій" (9-11 травня 2024 року);

9) Науково-практична конференція "Перспективи та проблематика інтелектуальних систем" (31 травня 2024 року).

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

Дисертаційна робота Запорожченка М.М. відповідає діючим вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії, передбаченим "Порядком 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.

Недоліки та зауваження

1. Формалізація алгоритму з використанням математичних виразів і псевдокоду спростила б впровадження запропонованого методу у практичні рішення. Це також полегшило б його адаптацію для інтеграції з існуючими програмними засобами в організаціях.

2. Порівняння ефективності запропонованого методу з іншими підходами дало б змогу чітко визначити його переваги та обмеження, що є важливим для оцінки його практичної цінності.

3. Автоматизація процесу оцінювання факторів захищеності є важливим елементом для застосування методу у великих організаціях з численними користувачами. Її деталізація дозволила б знизити суб'єктивність оцінок і підвищити ефективність.

4. Інтеграція з методами машинного навчання могла б значно підвищити точність і адаптивність запропонованого підходу до прогнозування соціоінженерних атак, дозволяючи використовувати великі обсяги даних для самооновлення моделей.

5. Різні професійні категорії мають специфічні поведінкові характеристики та рівні обізнаності щодо інформаційних ризиків, що могло б вплинути на результати оцінки психологічного та організаційного факторів вразливості. Диференціація цих груп надала б можливість створити більш точні моделі ризику.

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

Висновок

Дисертація Запорожченка М.М. відповідає вимогам "Порядку підготовки здобувачів вищих ступенів доктора філософії та доктора наук у закладах вищої освіти (наукових установах)", затвердженому постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, "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.

Офіційний опонент:
завідувач кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного
університету імені Бориса Грінченка,
кандидат технічних наук, доцент Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
П. Складанного (ПІБ) ЗАСВІДЧУЮ
пров. фах. ВК Лисогор І.В (посада)