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
доктора технічних наук, професора,
професора кафедри менеджменту організацій
Києво-Могилянської бізнес-школи
Національного університету "Києво-Могилянська академія"
Молодецької Катерини Валеріївни
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

Сучасна тенденція до зростання масштабності та динамічності соціоінженерних атак виводить проблему прогнозування таких загроз на рівень пріоритетних досліджень у сфері інформаційної безпеки. Особливу небезпеку становлять багатоетапні атаки, що базуються на використанні складної взаємодії між користувачами корпоративних систем, які формують нелінійні шляхи поширення загроз із високим ризиком компрометації критично важливих інформаційних активів.

Попри значну кількість досліджень у цій галузі, наукові підходи до оцінки ймовірності компрометації користувачів досі залишаються фрагментарними, а існуючі моделі здебільшого не враховують одночасний вплив багатофакторних компонентів, таких як психологічні характеристики користувачів, організаційна культура, технічний рівень захисту та зовнішні інформаційні загрози. Це суттєво обмежує можливості прогнозування та своєчасного виявлення найбільш критичних траєкторій атак.

Актуальність дисертаційної роботи зумовлена необхідністю розроблення інтегративного підходу до прогнозування соціоінженерних атак, що базується на моделюванні профілю захищеності користувача, застосуванні графових моделей взаємодії в корпоративному середовищі та комплексній оцінці ризиків. Такий підхід дозволяє не лише підвищити точність прогнозів ідентифікації вразливих категорій користувачів, а й забезпечити ефективну адаптацію заходів захисту до реальних умов

організації, що має вагоме практичне значення для стратегічного управління інформаційною безпекою.

Обґрунтованість наукових результатів, висновків та рекомендацій

Достовірність і обґрунтованість наукових результатів, отриманих у дисертації, підтверджується логічною послідовністю виконання дослідження, починаючи від коректної постановки наукового завдання до формулювання практичних рекомендацій. Значну роль у забезпеченні наукової обґрунтованості відіграє комплексний підхід до аналізу соціоінженерних атак, що охоплює всебічне теоретичне дослідження та експериментальну перевірку отриманих результатів.

Наукові положення дисертації базуються на використанні апробованих методів дослідження, що дозволило отримати об'єктивні результати. Зокрема, метод експертного оцінювання застосовано для визначення вагомості впливу різних факторів на рівень вразливості користувачів, а метод аналізу ієрархій – для встановлення пріоритетності характеристик профілю захищеності. Графові моделі стали основним інструментом для моделювання поширення атак у корпоративному середовищі, що дало можливість врахувати інтенсивність взаємодії між користувачами та виявити критичні шляхи поширення загроз.

Новизна наукових результатів дослідження

У дисертації одержані такі основні 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 одержаних результатів полягає в можливості ідентифікації найбільш уразливих категорій користувачів і моделювання потенційних траєкторій багатоетапних атак із визначенням ключових точок ризику. Апробація запропонованого методу продемонструвала його ефективність, що підтверджується статистично значущим зниженням рівня ризику одноетапних атак у межах від 10,3% до 42,8% для різних категорій користувачів та зменшенням ймовірності компрометації внаслідок багатоетапних атак у середньому на 21%.

Розроблені в роботі критерії оцінювання компонентів профілю захищеності можуть бути інтегровані у процеси управління інформаційною безпекою для побудови адаптивних стратегій захисту. Запропонований підхід дозволяє фахівцям з кібербезпеки не лише оцінювати рівень індивідуальної вразливості, але й створювати персоналізовані контрзаходи з урахуванням реальних загроз і специфіки організаційного середовища.

Зв'язок роботи з науковими програмами, планами, темами

Напрям дослідження Запорожченка М.М. 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

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.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

Дисертаційна робота Запорожченка М.М. є завершеним науковим дослідженням, що вирізняється логічною послідовністю викладу наукового матеріалу і відповідає чинним вимогам до дисертацій на здобуття наукового

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. Хоча у дисертаційному дослідженні згадано організаційні та технічні аспекти, поверхнево розглянуто відмінності в рівнях ризику для різних посад чи груп користувачів (керівники, адміністратори систем, звичайні співробітники, тимчасові підрядники тощо). Налаштування «профілю захищеності» під кожну роль могло б зробити результати оцінювання вразливості більш прицільними та допомогти у формуванні диференційованих контрзаходів.
2. Внутрішні загрози, зокрема навмисні дії або помилки співробітників, можуть значно підвищувати загальний рівень ризику для корпоративних систем. Включення цього аспекту розширило б застосування методу та підвищило його практичну цінність.
3. Запропонований науково-методичний апарат дієвий для середовищ із помірною кількістю користувачів. Утім, залишається відкритим питання: наскільки ефективно й швидко він масштабується для великих корпорацій із розгалуженою структурою і тисячами працівників. Варто було б розширити експериментальну частину або навести оцінки обчислювальної складності, щоб підтвердити придатність методів у масштабованих середовищах.
4. В дисертаційному дослідженні запропоновано модель оцінювання профілю захищеності користувачів, але детально не розглянуто стійкість методу до динамічних змін факторів, таких як швидка еволюція соціоінженерних технік. Водночас у дисертації менше уваги зосереджено на специфічних сценаріях атак, що активно розвиваються останнім часом, зокрема на телефонному або голосовому вішингу (vishing) і шахрайських чатботах. Розширений аналіз цих технік міг би посилити універсальність запропонованого підходу.

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

Висновок

Сформульована в дисертації мета досліджень досягнута. У результаті проведених досліджень автором вирішено важливе наукове завдання щодо розроблення інтегративного методу прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача. Запропоновані підходи враховують вплив психологічних, організаційних, технічних факторів та фактору інформаційного впливу, що

має суттєве значення для підвищення рівня інформаційної безпеки в корпоративному середовищі.

Новизна і відсутність аналогічних рішень у вітчизняній та зарубіжній практиці роблять отримані результати досліджень значущими як з наукової, так і з практичної точки зору. Запропоновані методи можуть бути інтегровані у систему управління інформаційною безпекою для оптимізації заходів захисту і мінімізації ризиків компрометації критичних активів.

Дисертаційна робота відповідає спеціальності 125 Кібербезпека та чинним вимогам "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. Автор роботи – Запорожченко Михайло Михайлович – заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Офіційний опонент:
професор кафедри менеджменту організацій
Києво-Могилянської бізнес-школи
Національного університету
"Києво-Могилянська академія"
доктор технічних наук, професор Катерина МОЛОДЕЦЬКА

Особистий підпис
ЗАСВІДЧУЮ
Начальник ВК