Лунгол Ольга Миколаївна
к.пед.н., доц., доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки,
Макаринська Анна Вадимівна
рядова поліції, курсантка 210 н.вз. факультету підготовки фахівців для підрозділів кримінальної поліції, Донецький державний університет внутрішніх справ, м. Кропивницький, Україна

СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ ТА АНАЛІЗУ СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В еру високорозвинених технологій інформаційної безпеки соціально-інженерні атаки визначаються як одна з найпоширеніших та найсерйозніших загроз кібербезпеці. Ці атаки не базуються на зламі коду чи вразливостях програмного забезпечення, а, навпаки, використовують людський фактор та мистецтво обману.

Соціально-інженерні атаки – це психологічні стратегії, спрямовані на обман людей з метою отримання несанкціонованого доступу до конфіденційної інформації, паролів чи фінансових ресурсів. Науковці Юдін О. К., Матвійчук-Юдіна О. В. та Супрун О. М. [1] зазначають, що «метою соціальної інженерії є спонукання людей виконувати певні дії, які вони за звичайних умов ніколи б не вчинили». Буров О. [2] у своїх дослідженнях відносить «соціально-інженерні атаки, що використовують страх, невпевненість та сумніви» до основних елементів, що впливають на кіберризик організації компаній.

Розрізняють різні види соціально-інженерних атак: фішинг (використання підроблених веб-сайтів або електронних повідомлень для отримання особистих даних), технічні шахрайські маніпуляції (використання технічних засобів для обману або впливу на цільову аудиторію), використання загроз та обіцянок (спроби вплинути на жертву через погрози або обіцянки невеликих вигод) тощо. До інструментів соціально-інженерних атак можна віднести: мережеві ресурси (коли зловмисники використовують соціальні мережі для збору інформації), телефонні дзвінки (через вивчення голосу, намагання досягти довіри через телефонні переговори), спостереження (включає особистий контакт для збору додаткової інформації) тощо.

До методів виявлення та аналізу соціально-інженерних атак в інформаційних системах ми відносимо: аналіз звернень користувачів (для визначення нетипових звернень або невідповідностей в способі комунікації), використання антивірусних програм (системи антивірусного захисту можуть виявляти спроби фішингу та інші шахрайські види), моніторинг поведінки користувачів (через аналіз навчальних програм та змін у поведінці користувачів для виявлення можливих загроз), аналіз попередніх інцидентів

(вивчення попередніх соціально-інженерних атак допомагає розробити більш ефективні стратегії захисту та підвищити рівень свідомості серед користувачів).

Збалансований підхід, що включає технічні та організаційні заходи, дозволяє ефективно впоратися з сучасними соціально-інженерними загрозами. При цьому усвідомленість та постійна освіта [3] стають ключовими факторами в запобіганні та виявленні атак. Саме на антропогенному засобі захисту інформаційних систем від соціально-інженерних атак наголошують Войтко Б. С., Марченко М. М. та Антонов Ю. С. [2] через: залучення уваги людей до питань безпеки; усвідомлення користувачами всієї серйозності проблеми і прийняття політики безпеки системи; вивчення та впровадження необхідних методів і дій для підвищення захисту інформаційного забезпечення. Науковці акцентують увагу, що дані методи мають один спільний недолік: вони пасивні і величезний відсоток користувачів не звертає увагу на попередження, навіть написані самим помітним шрифтом.

Сучасні методи виявлення та аналізу соціально-інженерних атак в інформаційних системах є критично важливими для забезпечення кібербезпеки. Загрози, пов’язані з використанням соціально-інженерних технік, стають все більш досконалими, вимагаючи від фахівців у галузі кібербезпеки постійного навчання та адаптації. Своєчасне реагування на нетипові звернення та навчання користувачів виявляти підозрілі ситуації є ключовими компонентами успішної боротьби з соціально-інженерними атаками. Досвід аналізу попередніх інцидентів дозволяє розпізнавати патерни та розробляти ефективні стратегії захисту. Застосування збалансованого підходу, який об’єднує технічні та організаційні заходи, сприяє створенню стійкої системи кібербезпеки.

Загалом, ефективна протидія соціально-інженерним атакам потребує не лише вдосконалених технічних рішень, але й постійного навчання та свідомості серед користувачів. Отже, захист від соціально-інженерних атак вимагає комплексного підходу та поєднання технічних й організаційних заходів. Постійна освіта персоналу, використання передових технологій та систем аналізу є ключовими елементами успішної стратегії виявлення та аналізу загроз в інформаційних системах.

Список літератури

1. Юдін О.К., Матвійчук-Юдіна О.В., Супрун О.М. Інформаційно-психологічна війна та технології соціального інжинірингу. Science-Based Technologies, 2021. №2 (50). С. 130–139. DOI: https://doi.org/10.18372/2310-5461.50.15684.

2. Буров О. Вплив кіберзлочинності на цифрову економіку. *Теорія і практика інтелектуальної власності*, 2021. № 5. С. 69–78.

3. Лунгол О.М., Агішева А.В. Технології створення та застосування систем захисту інформаційно-комунікаційних систем. *The 2nd International scientific and practical conference «Topical aspects of modern scientific research»*. October 26-28, 2023. CPN Publishing Group, Tokyo, Japan. 2023. P. 255–260.