

УДК 621

Лізунов С. І.¹, Верещака М.П.², Філобок Є.В.²

¹ канд. техн. наук, доц НУ «Запорізька політехніка»

² асп. НУ «Запорізька політехніка»

РОЛЬ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У СУЧАСНИХ КІБЕРАТАКАХ ТА МЕТОДИ ПРОТИДІЇ

У сучасному цифровому світі технологічні рішення стають дедалі складнішими та витонченішими, а методи традиційного злому часто блокуються розвиненими системами захисту. Проте найслабшою ланкою в кібербезпеці залишається людина. Саме тому соціальна інженерія стала однією з найпоширеніших тактик серед кіберзлочинців.

Соціальна інженерія – це методика маніпулювання людьми для отримання конфіденційної інформації, несанкціонованого доступу до систем або примушення жертв до виконання дій, що шкодять їхній безпеці. Головна небезпека полягає в тому, що такі атаки не вимагають технічного втручання, а використовують людські слабкості: довірливість, страх (шантаж), образа (помста), підкуп або цікавість. Згідно з дослідженням компанії Verizon, у 2023 році близько 74% кіберзломів включали елементи соціальної інженерії [1].

З розвитком технологій методи соціальної інженерії також еволюціонують. Основними типами атак є:

Фішинг (Phishing) – масові атаки через електронну пошту, соціальні мережі або месенджери, які змушують жертву розкрити свої облікові дані або натиснути на шкідливе посилання.

Вішинг (Vishing) та смішинг (Smishing) – атаки через телефонні дзвінки та SMS-повідомлення. Зловмисники можуть представлятися працівниками банку, техпідтримки або навіть правоохоронних органів.

Бейтинг (Baiting) – використання "приманки", наприклад, заражених USB-накопичувачів або підроблених безкоштовних програм.

Пре-текстинг (Pretexting) – атаки, в яких злочинець вигадує правдоподібну історію, щоб отримати довіру жертви й змусити її розкрити важливу інформацію.

Атаки через соціальні мережі – створення підроблених акаунтів, маніпуляція довірою, використання персональних даних для цільових атак.

Один із найвідоміших випадків соціальної інженерії стався у липні 2020 року, коли група хакерів отримала доступ до внутрішньої системи Twitter [2]. Використовуючи методи вішингу, зловмисники переконали співробітників компанії передати свої облікові дані, що дозволило їм отримати контроль над акаунтами Ілона Маска, Барака Обами, Білла Гейтса та інших відомих осіб.

Хакери розмістили шахрайські повідомлення, пропонуючи людям перевести Bitcoin на певний гаманець, обіцяючи подвоєння коштів. У результаті атаки вони викрали понад 120 000 доларів США.

Атака на SolarWinds стала однією з найсерйозніших у сфері кібербезпеки за останнє десятиліття [3]. Зловмисники використали методи соціальної інженерії, щоб проникнути в ланцюг постачання компанії. Вони відправляли співробітникам підроблені електронні листи, які містили шкідливі посилання, що призводило до компрометації системи оновлення програмного забезпечення Orion. Ця атака вплинула на понад 18 000 організацій, включаючи урядові установи США та великі корпорації.

У вересні 2022 року Uber став жертвою атаки соціальної інженерії, коли хакер, використовуючи пре-текстинг, отримав доступ до внутрішньої мережі компанії [4]. Він видавав себе за працівника IT-відділу і зміг переконати одного зі співробітників передати йому код двофакторної автентифікації. Це дало хакеру можливість отримати доступ до внутрішніх ресурсів Uber, включаючи інструменти безпеки та фінансові дані.

У грудні 2022 року компанія LastPass, що спеціалізується на керуванні паролями, повідомила про витік даних клієнтів через атаку соціальної інженерії на одного з її співробітників [5]. Зловмисники змогли отримати доступ до зашифрованих резервних копій даних користувачів, що поставило під загрозу мільйони акаунтів по всьому світу.

Для зниження ризику атак необхідно поєднувати технологічні та поведінкові заходи безпеки:

Навчання та тренінги – регулярне проведення симуляцій фішингових атак серед співробітників та користувачів допомагає підвищити обізнаність і зменшити ризик маніпуляцій [6].

Багатофакторна автентифікація (MFA) – навіть якщо зловмисник отримає пароль жертви, йому буде значно складніше пройти додаткову перевірку (SMS-код, біометрія, тощо) [7].

Контроль доступу до критичних систем – принцип мінімальних привілеїв дозволяє уникнути ситуацій, коли компрометація одного облікового запису призводить до зламу всієї системи [8].

Використання ІІІ для аналізу поведінки користувачів – сучасні системи кібербезпеки можуть аналізувати дії користувачів і виявляти підозрілу активність, наприклад, спроби входу з незвичних пристроїв або локацій.

Фільтрація електронної пошти та веб-захист – блокування підозрілих повідомлень та посилань на рівні корпоративної безпеки значно зменшує можливість успішних атак.

Соціальна інженерія залишається одним із найнебезпечніших методів атак у кіберпросторі. Зловмисники продовжують використовувати психологічні прийоми, щоб обходити навіть найсучасніші системи безпеки.

Останні реальні випадки, такі як злам Uber, LastPass та атака на SolarWinds, підтверджують, що жодна компанія чи організація не застрахована від подібних загроз.

Ефективна боротьба із соціальною інженерією потребує комплексного підходу, що включає технічні заходи захисту, навчання користувачів та впровадження новітніх методів виявлення підозрілої активності. Використання штучного інтелекту для аналізу поведінки користувачів, багатофакторна автентифікація та регулярне оновлення політик безпеки є ключовими елементами стратегії протидії сучасним кібератакам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Verizon Data Breach Report 2023 [Електронний ресурс]. – Режим доступу: <https://www.verizon.com/business/resources/reports/dbir/>
2. Twitter Security Incident Report, 2020 [Електронний ресурс]. – Режим доступу: https://blog.x.com/en_us/topics/company/2020/an-update-on-our-security-incident
3. SolarWinds Attack Analysis, 2021 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a>
4. Uber Security Breach Report, 2022 [Електронний ресурс]. – Режим доступу: <https://www.uber.com/newsroom/security-update>
5. LastPass Data Breach Statement, 2023 [Електронний ресурс]. – Режим доступу: <https://blog.lastpass.com/posts/notice-of-security-incident>
6. Cybersecurity Awareness Training, 2023 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/cybersecurity-awareness-training>
7. NIST MFA Security Guidelines, 2023 [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final>
8. Zero Trust Architecture Guidelines, 2023 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>