DOI https://doi.org/10.36059/978-966-397-621-1-65

Омецинська Н. В.,
кандидат технічних наук, доцент,
завідувачка кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Кисельов В. Б.,
доктор технічних наук, професор,
професор кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

ФІШИНГОВІ АТАКИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

У сучасних умовах цифровізації діяльності організацій та широкого впровадження інформаційних технологій значно зростає рівень кіберзагроз. Корпоративні інформаційні системи активно інтегрують електронні комунікації, хмарні сервіси та віддалений доступ, що створює додаткові вектори для здійснення атак. Однією з найбільш поширених і небезпечних загроз залишаються фішингові атаки, ефективність яких обумовлена використанням методів соціальної інженерії та орієнтацією на людський фактор.

Фішинг представляє собою вид кіберзлочинної діяльності, спрямований на отримання конфіденційної інформації шляхом введення користувача в оману. Основною метою таких атак є отримання облікових даних, фінансової інформації або несанкціонований доступ до корпоративних ресурсів. Особливістю фішингу є його здатність імітувати легітимні джерела інформації, що значно ускладнює його виявлення.

Реалізація фішингових атак здійснюється через різні канали комунікації, серед яких перше місце займає електронна пошта. Значного поширення також набувають атаки через підроблені вебресурси, соціальні мережі та мобільні повідомлення. Розвиток цифрових технологій сприяє ускладненню таких атак та підвищенню їх переконливості.

Фішингові атаки можуть відрізнятися за рівнем складності та спрямованістю. У сучасних умовах поряд із масовими розсилками все більшого поширення набувають цільові атаки, які орієнтовані на конкретних працівників або керівництво організацій. Такі атаки

враховують специфіку діяльності підприємства, структуру управління та особливості інформаційних потоків.

Механізми реалізації фішингових атак базуються на використанні підроблених доменів, створенні фальшивих вебсторінок, розсиланні електронних листів із шкідливими вкладеннями та застосуванні засобів обходу систем захисту. У сучасних умовах також спостерігається використання технологій штучного інтелекту для автоматизованого створення персоналізованих повідомлень, що значно підвищує ефективність атак.

Фішингові атаки можуть мати суттєві негативні наслідки для функціонування корпоративних інформаційних систем. Насамперед це стосується компрометації облікових записів користувачів, що відкриває можливість для подальшого несанкціонованого доступу до ресурсів організації. Крім того, можливий витік конфіденційної інформації, встановлення шкідливого програмного забезпечення та порушення безперервності бізнес-процесів.

Економічні наслідки таких інцидентів можуть проявлятися у фінансових втратах, зниженні довіри партнерів і клієнтів, а також у додаткових витратах на відновлення систем безпеки. У стратегічному вимірі фішингові атаки можуть впливати на стабільність функціонування організацій та їх конкурентоспроможність.

Важливою складовою проблеми фішингових атак є людський фактор, який часто виступає найбільш уразливою ланкою у системі інформаційної безпеки. Недостатній рівень обізнаності працівників щодо сучасних кіберзагроз, довіра до зовнішніх джерел інформації та відсутність навичок критичного аналізу отриманих повідомлень сприяють успішності атак.

Поведінкові аспекти користувачів відіграють ключову роль у процесі реалізації фішингових сценаріїв. Саме тому підвищення рівня цифрової грамотності персоналу є одним із пріоритетних напрямів забезпечення кібербезпеки.

Ефективна протидія фішинговим атакам передбачає застосування комплексного підходу, який поєднує технічні, організаційні та освітні заходи. Використання сучасних засобів фільтрації електронної пошти, систем моніторингу та багатофакторної аутентифікації дозволяє значно знизити ризик компрометації облікових даних. Водночас важливим є впровадження внутрішніх політик інформаційної безпеки та контроль доступу до ресурсів.

Не менш важливим є проведення регулярного навчання персоналу, спрямованого на формування навичок розпізнавання фішингових повідомлень. Використання імітаційних сценаріїв атак дозволяє оцінити рівень готовності працівників до протидії загрозам та виявити слабкі місця у системі захисту.

Подальший розвиток засобів протидії фішинговим атакам пов'язаний із впровадженням інтелектуальних систем аналізу поведінки користувачів, автоматизацією процесів виявлення загроз та інтеграцією механізмів кіберзахисту у загальну систему управління організацією. Особливого значення набуває використання технологій штучного інтелекту для своєчасного виявлення аномалій та реагування на інциденти.

Зростає також роль концепції кіберстійкості, яка передбачає здатність організації не лише запобігати атакам, але й ефективно відновлюватися після їх реалізації.

Фішингові атаки залишаються однією з ключових загроз для корпоративних інформаційних систем у сучасному цифровому середовищі. Їх ефективність зумовлена поєднанням технічних засобів та методів соціальної інженерії, а також значною залежністю від людського фактору.

Забезпечення належного рівня кібербезпеки потребує впровадження комплексних заходів, що охоплюють технічний захист, організаційні рішення та підвищення обізнаності персоналу. Подальші дослідження у цій сфері мають бути спрямовані на розробку інтелектуальних систем виявлення фішингових атак та підвищення рівня кіберстійкості організацій.

Список використаних джерел:

1. AI cybersecurity threats 2026: what experts predict. URL: https://techinformed.com/ai-cybersecurity-threats-2026-what-experts-predict/

2. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability. 2023.

3. Syracuse University iSchool: Al in Cybersecurity: How Al is Changing Threat Defense. URL: https://ischool.syracuse.edu/ai-in-cybersecurity/

4. Swimlane: Guide to Al in Cybersecurity: 7 Use Cases of Al Automation. URL: https://swimlane.com/blog/how-is-ai-used-in-cybersecurit