УДК 004.77:007 **DOI:** 10.31673/2412-9070.2024.031217

В. А. САВЧЕНКО, доктор техн. наук, професор, ORCID: 0000-0002-3014-131X,
Державний університет інформаційно-комунікаційних технологій, Київ

ДОСЛІДЖЕННЯ ПОТЕНЦІЙНОГО ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПРОЦЕСИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Цифрова трансформація відбиває процес переходу суспільства та бізнесу до нових технологій із метою поліпшення діяльності та забезпечення нових можливостей. Цей процес охоплює впровадження штучного інтелекту, Інтернету речей, хмарних сервісів та багатьох інших технологій для покращення результатів діяльності. Такий перехід обіцяє нам низку переваг, серед яких: гнучкість та оперативність цифрових процесів через тотальну комп'ютеризацію; підвищення ефективності виробничих процесів завдяки Інтернету речей, хмарним обчисленням та автоматизації; покращення взаємодії з клієнтами на основі штучного інтелекту. Це далеко не повний перелік технологій цифрової трансформації. Але скільки б технологій не з'явилося в майбутньому, всі вони разом із перевагами створюють нові виклики кібербезпеці, зокрема і ті, які базуються на методах соціальної інженерії.

У статті досліджено відомі випадки кібератак із використанням соціальної інженерії. Показано, що ані малі, ані великі компанії не захищені від соціальної інженерії. Досліджено базову модель соціальної інженерії, яка ґрунтується на схильності людей до передавання всієї інформації і здійснення нелогічних дій. Проаналізовано технології соціальної інженерії: претекстинг, фішинг, дорожнє яблуко, плечовий серфінг, послуга за послугу. Оцінено потенційні загрози від методів соціальної інженерії для таких систем: SCADA, хмарних обчислень, Інтернету речей, дронів, великих даних, блокчейну, штучного інтелекту та соціальних мереж. Визначено ключові засоби протидії соціальній інженерії в епоху цифрової трансформації. Зроблено висновки щодо впливу соціальної інженерії в майбутньому.

Ключові слова: цифрова трансформація; соціальна інженерія; фішинг; претекстинг; Інтернет речей; хмарні обчислення; SCADA.

ВСТУП

Із ростом використання технологій та переходом до цифрового суспільства відбуваються позитивні зміни в різних сферах нашого життя: від підвищення продуктивності до спрощення повсякденних завдань. Проте разом із цими перевагами ми стикаємося з новими загрозами кібербезпеці, зокрема з використанням соціальної інженерії. Тому, сьогодні актуальним є запитання: Чи будемо ми більш захищеними в майбутньому від атак із використанням соціальної інженерії?

Постановка проблеми. Цифрова трансформація відображає процес переходу суспільства та бізнесу до нових технологій для поліпшення діяльності та забезпечення нових можливостей (рис. 1). Цей процес включає в себе впровадження штучного інтелекту, Інтернету речей (IoT), хмарних сервісів та багатьох інших технологій для покращення результатів діяльності. Завдяки цьому можна здобути низку переваг, серед яких: гнучкість та оперативність цифрових процесів через тотальну комп'ютеризацію; підвищення ефективності виробничих процесів за допомогою Інтернету речей, хмарних обчислень та автоматизації; покращення взаємодії з клієнтами на основі штучного інтелекту. Це далеко не повний перелік технологій цифрової трансформації. Але скільки б технологій не з'явилося в майбутньому, всі вони разом із перевагами створюють нові виклики кібербезпеці, зокрема і ті, які базуються на методах соціальної інженерії.

Аналіз публікацій. У статті [1] наведено статистику з кількості підключень, дозволів на використання адреси електронної пошти і паролю, а також дозволу на автоматичне передавання службових даних браузером (кукі). Статистичні дані оброблені за допомогою спеціально написаних алгоритмів. Запропоновані підходи до вирішення проблеми соціотехнічних атак можуть бути використані та впроваджені для експлуатації на будь-яких об'єктах інформаційної діяльності. Результати експериментів показали, що обізнаність користувачів навіть технічних спеціальностей недостатня, тому потрібно приділяти окрему увагу до розроблення методик підвищення рівня компетентності користувачів та зменшення кількості потенційних атак на об'єкти інформаційної діяльності.

У [2] розглядаються основні методи, які використовують зловмисники під час проведення фішингових атак із використанням електронної пошти, ознаки того, що користувач став жертвою соціальних інженерів, та наведено рекомендації, як можна підвищити стійкість корпоративного середовища до подібних атак за допомогою організаційних методів.

У публікації [3] обговорюються чотири домени соціальної інженерії (голосовий дзвінок, електронна пошта, особисте спілкування та текстове повідомлення). Пояснюються психологічні концепції, які використовуються в соціальній інженерії. Наприклад, чому люди стають жертвами та як право-

Рис. 1. Технології цифрової трансформації та їх переваги

порушники зловживають недоліками людського мислення. Дослідження авторів ілюструє проблематику соціальної інженерії, зокрема, яка група є найбільш вразливою до соціальної інженерії та якою мірою можна протидіяти атаці. Автори обговорюють деякі труднощі в дослідженні соціальної інженерії та визначають напрями майбутніх досліджень.

У статті [4] показано, що соціальна інженерія складається з методів, які застосовуються для маніпулювання людьми, щоб змусити їх виконувати дії або розголошувати конфіденційну інформацію. Для досягнення цього соціальний інженер обманом змушує когось надати доступ до інформації або порушити звичайні процедури безпеки. Це загрожує не лише компаніям, організаціям та урядам, а й окремим особам. Хоча новітні технології ускладнили деякі шахрайські дії, вони створили нові можливості для адаптивних шахраїв, і тому найефективнішу технологію безпеки може подолати розумний соціальний інженер.

Отже, можна дійти висновку, що сьогодні важко сказати, як саме бурхливий розвиток процесів цифрової трансформації буде захищений від втручання з використанням методів соціальної інженерії.

Тому, метою цієї публікації є розгляд питання впливу методів соціальної інженерії на процеси цифрової трансформації.

ОСНОВНА ЧАСТИНА

Соціальна інженерія — це маніпулятивні та обманні методи, які використовуються для отримання конфіденційної інформації, доступу до систем чи контролю над людьми через використання психологічних та соціальних механізмів. Такі атаки базуються на використанні людських емоцій та довіри. Майже кожен із нас хоча б раз у житті був жертвою соціальної інженерії. Практично щодня нам надходять електронні листи, повідомлення в соціальних мережах, телефонні дзвінки з пропозицією взяти участь у розіграші цінного подарунка, отримати спадок чи грошові кошти лише за невеличку послугу — передати облікові дані наших фінансових рахунків.

Хакер може надіслати електронний лист, який має цілком достовірний вигляд, але насправді це трюк, щоб змусити вас натиснути на посилання. Потім це посилання встановить шкідливе програмне забезпечення на ваш комп'ютер. Або хтось може зателефонувати вам, видаючи себе за представника банку, і спробувати змусити вас надати йому пароль свого облікового запису. Якщо ви розкриєте таку інформацію, її може бути використано для викрадення ваших даних, грошей або навіть вашої особи.

Ось кілька прикладів кібератак із використанням соціальної інженерії (табл. 1). Як бачимо, ані малі, ані великі компанії, такі як, наприклад, Google, Facebook, Toyota, Twitter, Microsoft не захищені від соціальної інженерії. Збитки цих компаній можуть сягати десятків і сотень мільйонів доларів. При цьому у більшості випадків ключовим методом впливу були фішингові листи [5].

Одна з найбільш відомих кібератак, в якій було використано методи соціальної інженерії, сталася у 2012 році в Ірані. Тоді вірус Stuxnet було інфільтровано до системи керування заводом зі збагачення урану в Натанзі. Вірус було підкинуто завантаженням ураженого музичного файлу через працівника, який був шанувальником національних пісень. Флешку з цим файлом працівник при-

Таблиця 1

Приклади атак соціальної інженерії [5]

Компанії	Дата	Деталі/Пошкодження	Метод/Інструменти порушення
Saudi Aramco	2021	Хакери стверджували, що вони мають майже 1 терабайт даних Aramco, і вимагали викуп у розмірі 50 млн дол. США	Фішингова електронна пошта
Microsoft	2021	Кілька користувачів MS Office стали жертвами фішингової електронної афери. Кожного з них було ошукано на суму від 100 до 199 дол. США	Компрометація бізнес-електронної пошти (BEC), фішингова електронна пошта
Marriott	2018-2020	В обох випадках хакери отримали доступ до мільйонів записів гостей. Ці записи включали імена гостей, адреси, контактні номери та зашифровану інформацію про кредитні картки	Фішингова електронна пошта, скомпрометовані облікові дані двох співробітників Marriott, троян віддаленого доступу (RAT), інструмент Mimikatz для використання недоліків системи безпеки
Twitter	2020	Хакери зламали 130 акаунтів у Twitter. Кожен обліковий запис мав щонайменше 1 млн підписників. Хакери використовували 45 дуже впливових облікових записів для просування шахрайства з біткойнами	SE-атака за допомогою фейкових акаунтів, цільовий фішинг
Shark Tank	2020	Постачальник послуг хостингу Shark Tank втратив 400 000 дол. США в результаті неспромоги відфільтрувати шахрайські електронні листи	Фішингова електронна пошта
Toyota	2019	Корпорація Toyota Boshoku втратила 37 млн дол. після того, як стала жертвою атаки BEC	Фішингова електронна пошта (наприклад, BEC)
Energy firm (базується у Великобританії)	2019	Головного виконавчого директора (CEO) хакери ошукали на 243 000 дол. США	Фішингова імітація за допомогою засобу Deepfake
Google і Facebook	2015-2013	Фішингові електронні листи коштували Google і Facebook понад 100 млн дол. США	Цільовий фішинг

ніс на робоче місце, де і слухав улюблену музику. Комп'ютерний хробак Stuxnet швидко поширився у внутрішній мережі керування системою SCADA і змінив умови роботи центрифуг так, що їх оператори тривалий час не помічали жодних відхилень, тоді як центрифуги фізично виходили з ладу внаслідок абсолютної неконтрольованості процесу.

Найзначніша кібератака з використанням соціальної інженерії в Україні сталася в грудні 2015 року. Тоді нападники отримали доступ до корпоративної мережі енергетичних компаній кількох областей через зараження троянською програмою Black Energy. Заражений документ Word надсилався в приєднаному до листа файлі. Коли співробітники клікали по файлу, з'являлося вікно із запитом про дозвіл увімкнути виконання програми-макроса, який відкривав «чорний хід» для хакерів. У такий спосіб під час зламу було використано штатну функціональність програми Microsoft Word, що і призвело до аварійної ситуації. У результаті атаки було вимкнено приблизно 30 підстанцій, майже 230 тисяч мешканців залишались без світла протягом однієї-шести годин.

Поєднання методів технічного зламу з методами соціальної інженерії дало назву таким атакам, як APT-атаки (Advanced Persistent Threat), що стало новим явищем та істотною проблемою для фахівців кібербезпеки.

Модель соціальної інженерії (рис. 2) базується на схильності людей до передавання всієї інформації і здійснення нелогічних дій. Здебільшого в компанії всі співробітники мають різні права доступу до інформації. Звичайні співробітники не повинні мати доступу до інформації, яка може завдати шкоди компанії. Але, у разі якихось проблем, персонал із різними рівнями доступу може передати проблему на наступний щабель, і там вже вирішують, чи уповноважені вони розв'язувати ситуацію. Якщо відповіді немає, питання передається далі і т. д.

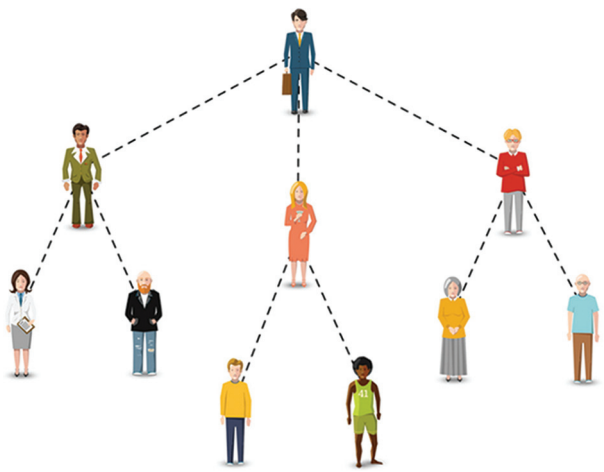

Рис. 2. Модель соціальної інженерії

Уразливість системи полягає в тому, що можна представитися одним із людей вищого рівня. Важко уявити ситуацію, що рядовий співробітник буде з'ясовувати вірогідність того, хто телефонував, якщо це представник вищого керівництва. Емоції, зокрема страх — це невід'ємна частина людської натури і тому можна знайти лазівки навіть у самій строгій структурі.

Існує два основних методи соціальної інженерії — прямий і зворотний.

Пряма соціальна інженерія. Спочатку зловмисник збирає інформацію про жертву та цільову систему. Потім встановлює стосунки (зв'язки) з ціллю. Після цього зловмисник дістається до цільової системи і вчиняє подальші дії. Наприклад, зловмисник протягом місяця щодня набирає працівника з Call-центру і видає себе за співробітника компанії. Активні розмови дають змогу з'ясувати будь-які незначні дрібниці про компанію. Далі зловмисник може попросити про невелику допомогу, яку зазвичай буде виконано.

Зворотна соціальна інженерія. У разі зі зворотною методикою передавання потрібних даних зловмиснику здійснюється добровільно самим користувачем. Наприклад, якщо на стіні біля робочого місця користувача замість номера техпідтримки зазначити власний контакт, то для працівника можна влаштувати невелику проблему. Майже одразу ж вам надійде дзвінок від засмученого працівника, який буде готовий розказати все, бо покладається на компетентність співробітника служби підтримки.

Технології соціальної інженерії

Щоб здобути інформацію, шахраї насамперед використовують такі слабкості людини, як страх, цікавість, неуважність, недосвідченість. Далі коротко розглянемо техніки, за допомогою яких зловмисники здійснюють атаки.

Претекстинг. Суть цього методу полягає в тому, що жертва виконує дії, до яких її підштовхують зловмисники за розробленим раніше сценарієм. Це може бути розкриття облікових даних або завантаження шкідливого програмного забезпечення. Шахрай може видавати себе за іншу особу, наприклад, спілкуючись як працівник банку.

Фішинг. Фішинг може різнитися за способом спілкування: письмовий, розмовний або їх поєднання. Листування — найчастіший вид фішингу. В його основі відправлення жертві листа чи SMS-сповіщення на пошту зі шкідливим програмним забезпеченням або підробленим сайтом із формою введення даних. Для того, щоб користувач напевно відкрив повідомлення та перейшов за посиланням, зловмисник підробляє його під звернення від банків, державних установ, служби безпеки, поліції тощо. Телефонний фішинг ще небезпечніший за листування, бо в цьому разі шахрай вимагає термінових дій, коли жертва не має часу на роздуми. А коли людина поспішає, вона частіше робить помилки. Теми телефонного фішингу, як правило, пов'язані з потребою у невідкладному вирішенні: рідні потрапили в аварію; чоловіка затримала поліція; необхідність лікування тощо. Також бувають випадки, коли жертві спочатку надсилають листа, а потім додатково дзвонять, щоб вона напевно його відкрила та отримала «троянського коня».

Дорожнє яблуко. Цей метод полягає в тому, що жертві підкладається фізичний носій (флешка), який активує вірус-вимагача або вірус-шпигуна. Носій має гарний вигляд, офіційні логотипи, щоб привернути увагу. Його ніби хтось губить у публічних місцях: у кафе, коворкінгу, на автостоянці, у спортклубі, приміщенні для перевдягання/куріння робітників тощо. І коли людина вставляє знахідку в персональний/робочий пристрій, то отримує неприємності, зокрема блокування програм, зміни в базах даних, крадіжку паролів.

Плечовий серфінг. Цей метод не дуже простий і передбачає спостерігання за жертвою в публічних місцях. І хоча кожен впевнений, що зможе вчасно помітити людину, яка за ним стежить, це не завжди так, оскільки зловмисники можуть працювати в команді: один із них відвертатиме увагу користувача, а другий буде стояти за спиною. У такий спосіб зловмисники можуть не тільки побачити PIN-код картки (який людина вводить у банкоматі або на касі в супермаркеті), а ще й розгледіти код-повідомлення для двофакторної автентифікації на екрані телефона/ноутбука.

Послуга за послугу. Такий метод атаки передбачає створення для користувача зовнішніх ознак серйозної проблеми. Це можуть бути питання, пов'язані з банківськими рахунками, страхуванням, справністю техніки, доступом до мережі тощо. Коли людина стикається з такою «проблемою», вона звертається до зловмисника, який каже, що питання вирішується легко, треба тільки надати якісь дані або встановити програму.

Отже, як бачимо, проблема соціальної інженерії стає щороку більш актуальною, а кількість її методів лише збільшується.

Потенційні загрози від методів соціальної інженерії

SCADA. Зловмисники, націлені на мережі SCADA, можуть використовувати різні шляхи проникнення до контрольованої зони системи: переконфігурація фаєрволів, небезпечний віддалений доступ, інфіковані власні пристрої та носії працівників, зламаний безпроводовий доступ, інфіковані штатні пристрої, які були передані недовіреним особам тощо. Соціальна інженерія дає

можливість зловмисникам дізнатися більше про саму систему SCADA, як вона працює та чи зможуть вони створити бекдор для використання в майбутньому.

Хмарні обчислення. Зараз хмарні служби є однією з головних цілей фішингових зловмисників. За статистикою, приблизно 33% інцидентів у хмарі пов'язані з методами соціальної інженерії через користувачів, і лише 11% — від хмарних провайдерів. У загальнодоступній хмарній службі URL-адреса або домен відомі всім, і домен може отримати доступ із будь-якого місця, тому зловмисник може здійснювати зловмисні атаки на цільові служби. Як наслідок зловмисник здатен отримати доступ до сервісів хмарних обчислень.

Інтернет речей. Багато пристроїв IoT, зокрема маршрутизатори, давачі та принтери мають віддалений доступ. Хакери можуть використовувати їх, щоб отримати доступ до мережі вашої компанії, навіть не ступаючи у вашу будівлю. Наприклад, зловмисник через ваших працівників отримує доступ до пристроїв IoT або знаходить пристрої з обліковими даними з усталеним налаштуванням і може використовувати їх як точки доступу до мережі, до якої він підключений.

Дрони. Не зважаючи на те, що системи керування та канали комунікації дронів достатньо добре захищені, недобросовісні працівники можуть робити бекдори на ваших дронах, комунікаціях або серверах і частково чи повністю здійснювати віддалене керування ними. Мережне застосування груп дронів призведе до істотних наслідків.

Великі дані. Вплив соціальної інженерії на Big Data не має важливих технологічних особливостей, але може мати значні наслідки. Приклад із компанією eBay у 2014 році, коли хакери отримали доступ до внутрішньої мережі компанії, скориставшись обліковими даними трьох її співробітників і мали бекдор-доступ протягом майже року. У цей період вони одержали персональні дані майже 150 млн споживачів.

Блокчейн. Технологія блокчейн, яка забезпечує криптовалюту, є високоанонімною і тому надзвичайно важливо для користувачів захистити свій приватний ключ автентифікації від розголошення неавторизованим сторонам. У зв'язку з анонімністю системи обов'язки IT-безпеки криптобізнесу покладаються на приватну відповідальність самих користувачів. У разі будь-яких зловживань правоохоронним органам буде майже неможливо відстежити вкрадені кошти.

Штучний інтелект. Можливості штучного інтелекту (ШІ) у поєднанні із соціальною інженерією майже безмежні. ШІ може зробити претекстинг більш вірогідним. Наприклад, генеративний ШІ можна використовувати для імітації стилів написання довірених організацій або окремих осіб, щоб спроби фішингу мали більш вірогідний вигляд. Суб'єкт загрози, оснащений ШІ, може скерувати його на систематичне дослідження організації на наявність слабких місць. Завдяки штучному інтелекту один хакер може становити таку саму загрозу, як і команда хакерів.

Водночас, хоча ШІ може спростити хакерство, але він також може оптимізувати захист кібербезпеки організації. ШІ настільки хороший чи шкідливий, наскільки люди його використовують.

Соціальні мережі. Соціальні мережі є одним із найбільш складних та небезпечних явищ в аспекті соціальної інженерії. Соціальні мережі сьогодні стали найсприятливішим середовищем для розвитку методів соціальної інженерії. Через можливість спілкування всіх з усіма вони чинять чи не найбільший вплив на людей у порівнянні з раніше розглянутими технологіями. Соціальні мережі дають можливість швидко здобути потрібну інформацію про абсолютно невідомих людей. А чим більше відомо про користувачів, тим легше застосувати техніку переконання, щоб запропонувати їм саме те, що їм подобається або чого вони бояться.

Засоби протидії соціальній інженерії в епоху цифрової трансформації

Абсолютна більшість авторів [5–11] вважає, що тренування та підготовка персоналу в поєднанні з відповідними політиками безпеки та комунікації в компанії — це основні дієві механізми протидії соціальній інженерії (табл. 2). Далі можна відзначити низку технічних засобів, які також впливають на безпеку: фаєрволи, криптографія, керування паролями тощо. Лише поєднання всіх цих заходів дасть можливість побудувати безпечне середовище сучасної компанії.

Таблиця 2

Засоби протидії соціальній інженерії

Засоби	Соціальні			Технічні			Організаційні		Загалом
	Тренувальні	Політики безпеки	Політики комунікацій	Firewalls	Шифрування	Фірмове обладнання	Керування паролями	Повідомлення про інциденти	
Кількість залучених експертів	15	11	7	7	4	3	3	2	52
%	29	21	13	13	8	6	6	4	100

ВИСНОВКИ

1. Поява нових технологій і розширення спектра цифрової трансформації призведе до того, що в майбутньому слід очікувати ще більших проблем щодо кібербезпеки, зокрема із застосуванням соціальної інженерії.

2. Соціальна інженерія не зникне сама по собі, оскільки вона базується на ключових проблемах людського спілкування, на використанні людських емоцій та довіри, а також на схильності людей до передавання всієї інформації і здійснення нелогічних дій.

3. За умов цифрової трансформації навчання та підготовка персоналу в поєднанні з відповідними політиками безпеки та комунікації в компанії — це основні дієві механізми протидії соціальній інженерії.

Список використаної літератури

1. **Соколов В. Ю., Курбанмурадов Д. М.** *Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності // Кібербезпека: освіта, наука, техніка. № 1(1). С. 6–16. URL: https://arxiv.org/ftp/arxiv/papers/1904/1904.01692.pdf*

2. **Якименко Ю. М., Рабчун Д. І., Запорожченко М. М.** *Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти // Кібербезпека: освіта, наука, техніка. 2021 № 1(13). С. 6–16.*

3. **Bullée J.-W., Junger M.** *Social Engineering. 2021. 10.1007/978-3-319-78440-3_38.*

4. **Sadiku Matthew, Shadare Adebowale, Musa Sarhan.** *Social Engineering: An Introducction // The Journal of Scientific and Engineering Research. 2016. № 3. P. 64–66.*

5. **Siddiqi M. A., Pak W., Siddiqi M. A.** *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures // Appl. Sci. 2022. № 12. P. 6042. URL: https://doi.org/ 10.3390/app12126042*

6. **Human** *factor, a critical weak point in the information security of an organization's Internet of things / K. Hughes-Larteya, M. Li, F. E. Botchey, Z. Qin // Heliyon. 2021. № 7. P. 6522–6535.*

7. **Parthy P. P., Rajendran G.** *Identification and prevention of social engineering attacks on an enterprise // Proceedings of the International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019.*

8. **Review** *and insight on the behavioral aspects of cybersecurity / R. A. M. Lahcen, B. Caulkins, R. Mohapatra, M. Kumar // Cybersecurity. 2020. № 3. P. 10.*

9. **Campbell C. C.** *Solutions for counteracting human deception in social engineering attacks // Inf. Technol. People. 2019. № 32. P. 1130–1152.*

10. **Washo A. H.** *An interdisciplinary view of social engineering: A call to action for research // Comput. Hum. Behav. Rep. 2021. № 4. P. 100126.*

11. **Measuring** *awareness of social engineering in the educational sector in the kingdom of Saudi Arabia / M. H. Alsulami, F. D. Alharbi, H. M. Almutairi [et al.] // Information. 2021. № 12. P. 208.*

V. Savchenko

RESEARCH OF THE POTENTIAL IMPACT OF SOCIAL ENGINEERING ON DIGITAL TRANSFORMATION PROCESSES

Digital transformation reflects the process of transition of society and business to new technologies in order to improve operations and provide new opportunities. This process includes the introduction of artificial intelligence, the Internet of Things, cloud services, and many other technologies to improve business results. Such a transition promises us a number of advantages, including: flexibility and efficiency of digital processes due to total computerization; increasing the efficiency of production processes due to the Internet of Things, cloud computing and automation; improving interaction with customers based on artificial intelligence. This is far from a complete list of Digital Transformation technologies. But no matter how many technologies appear in the future, all of them, along with their advantages, create new challenges for cyber security, including those based on social engineering methods. Social engineering is manipulative and deceptive methods used to obtain confidential information, access systems, or gain control over people through the use of psychological and social mechanisms. The article examines known cases of cyberattacks using social engineering. It is shown that neither small nor large companies are immune from social engineering. The basic model of social engineering, which is based on the tendency of people to transfer all information and perform illogical actions, was studied. Social engineering technologies were analyzed: Pretexting, Phishing, Road apple, Shoulder surfing, Service for service. Potential threats from social engineering methods for systems: SCADA, Cloud Computing, Internet of Things, Drones, Big Data, Blockchain, Artificial Intelligence and Social Networks are assessed. The key means of countering social engineering in the era of digital transformation have been identified. Conclusions are made regarding the impact of social engineering in the future.

Keywords: digital transformation; social engineering; phishing; pretexting; Internet of Things; cloud computing; SCADA.