

Отже, роль штучного інтелекту в оптимізації бізнес-процесів є ключовою для сучасних підприємств. Ефективна інтеграція ШІ дає змогу автоматизувати рутинні завдання, підвищити продуктивність, знизити операційні витрати та забезпечити конкурентну перевагу на глобальному ринку, створюючи умови для інноваційного розвитку та стабільного зростання компанії.

Список використаних джерел

1. Автоматизація бізнес-процесів зі штучним інтелектом. *Techno Logic*. URL: <https://techno-logic.com.ua/avtomatyzacziya-biznes-proczesiv-z-shtuchnym-intelektom/> (дата звернення: 29.03.2025).
2. Штучний інтелект – це musthave для оптимізації бізнес-процесів і посилення кібербезпеки компанії. *Kness energy*. URL: <https://kness.energy/news/shtuchnij-intelekt-ce-musthave-dlya-optimizacii-biznes-procesiv-i-posilennya-kiberbezpeki-kompanii/> (дата звернення: 29.03.2025).



УДК 343.37:159.947.5

Степанюк Дарина Василівна

(наук. керівник – д-р філол. наук, професор Шкіцька І. Ю.)

Західноукраїнський національний університет, м. Тернопіль

МАНІПУЛЯТИВНІ ПРИЙОМИ ШАХРАЙСЬКОЇ ПОВЕДІНКИ

Анотація. У тезах представлено дослідження психологічних прийомів маніпулювання, що застосовуються суб'єктами шахрайської діяльності для досягнення власних цілей. Проаналізовано найбільш поширені методи впливу на потерпілих, зокрема емоційну експлуатацію, соціальну інженерію, маніпулювання довірою, конструювання ілюзорних ситуацій і відволікання уваги. Окрему увагу приділено новітнім формам кіберзлочинності, що демонструють активний розвиток у цифровому середовищі.

Ключові слова: шахрайство, маніпулювання, психологічні прийоми, кіберзлочин.

В умовах дедалі більшої складності інформаційних потоків і соціальних взаємодій у сучасному суспільстві шахрайство стає надзвичайно актуальною проблемою. Шахраї використовують різноманітні психологічні методи, щоб маніпулювати потенційними жертвами. Це призводить до того, що люди ухвалюють рішення, які не відповідають їхнім інтересам, часто не розуміючи справжніх причин такого вибору.

Актуальність дослідження маніпулятивної поведінки шахраїв обумовлена збільшенням кількості злочинів, пов'язаних із психологічним впливом на людину. В умовах швидкого розвитку інформаційних технологій, а також у контексті зростаючої соціальної вразливості окремих груп населення злочинці дедалі частіше використовують витончені методи психологічного маніпулювання для досягнення власних протиправних цілей.

Головною метою таких дій є отримання контролю над поведінкою людини, що досягається шляхом введення її в оману або нав'язування хибної картини реальності. З огляду на це важливим є системне дослідження механізмів, що забезпечують ефективність таких впливів. Питання зловмисної маніпулятивної пове-

дінки привертали увагу таких дослідників: І. Боденчук [1], О. Брисковська [2], Д. Коваленко [3], О. Кравченко [4], А. Самодін [5], Ю. Чайка [6], С. Чернявський [7] та ін.

Із розвитком цифрового простору вдосконалюються й інструменти шахрайства: зловмисники вигадують нові види кіберзлочинів, включно з фішингом, шахрайськими схемами, поширенням шкідливої інформації. Наслідки таких впливів можуть бути вкрай серйозними – від втрати особистих і фінансових даних до психологічних травм, тому дослідження механізмів маніпуляцій і принципів шахрайської поведінки є важливим для створення ефективної системи боротьби із цифровими загрозами.

Мета розвідки – виявлення й систематизація головних прийомів маніпулятивної поведінки зловмисників у віртуальному просторі.

Суб'єкти шахрайської діяльності застосовують широкий спектр психологічних прийомів для маніпулювання потенційними потерпілими. Серед найбільш поширених прийомів маніпулятивної поведінки кіберзлочинців треба виокремити такі:

Емоційна експлуатація. Шахраї часто використовують емоційні тригери, як-от страх, жадібність, співчуття або почуття провини, з метою спонукання особи до імпульсивних дій. Популярності серед зловмисників набула модель маніпулятивної поведінки, що ґрунтується на провокуванні емоційної реакції особи через надсилання повідомлень образливого змісту від неідентифікованого відправника. Зазвичай значна частина реципієнтів здійснює перехід на профіль відправника з метою ідентифікації особи та з'ясування обставин. Сторінка зазначеного користувача є закритим профілем, що містить єдине гіперпосилання угорі профілю. Його метою є викликання цікавості та спонукання до переходу. Зазначене гіперпосилання є фішинговим та несе потенційну загрозу несанкціонованого доступу до облікових записів у Telegram, Instagram або інших онлайн-сервісів [3].

Соціальна інженерія. Кіберзлочинці використовують підроблені документи, вебсайти або електронні листи, щоб створити ілюзію легітимності, маніпулюючи людьми. Наприклад, вони можуть надсилати фішингові електронні листи від імені банків із посиланнями на підроблені вебсайти або створювати фальшиві інвестиційні платформи з підробленими ліцензіями та сертифікатами. Ця тактика дає їм змогу викрадати особисті дані, фінансову інформацію або переконувати жертв здійснити платежі, використовуючи довіру, викликану фальшивими документами.

Маніпулювання довірою. Зловмисник, знаючи про близькі стосунки людини з певною особою, видає себе за неї, використовуючи схожий голос або надсилаючи повідомлення з підробленого профілю. Він може розповісти про термінову ситуацію, у якій опинився, і попросити про фінансову допомогу, посилаючись на спільні спогади або деталі, відомі лише близьким друзям. Жертва, довіряючи «знайомому», без вагань переказує гроші, не підозрюючи про шахрайство [6].

Створення ілюзії. Зловмисники здійснюють розсилання електронних повідомлень, що містять неправдиву інформацію про отримання значних грошових виграшів або цінних матеріальних призів. Умовою отримання зазначених благ є

здійснення попереднього платежу у вигляді комісійного збору або податкового відрахування відносно невеликого розміру. Шляхом обіцянки швидкого та легкого збагачення шахраї спонукають адресата до переказу грошових коштів, після чого припиняють будь-який подальший контакт.

Відволікання уваги. Суб'єкт кіберзлочинної діяльності, вдаючись до представлення співробітником служби технічної підтримки легітимної організації, ініціює телефонний контакт із потенційною жертвою. Під час розмови зловмисник повідомляє про наявність шкідливого програмного забезпечення на персональному комп'ютері особи. Наполягаючи на терміновій інсталяції спеціалізованого «інструменту для нейтралізації вірусів», кіберзлочинець фактично встановлює шкідливе програмне забезпечення. З метою запобігання критичному осмисленню ситуації з боку потерпілого шахрай використовує складну технічну термінологію, демонструє сфабриковані вікна системних помилок на комп'ютері жертви та чинить постійний психологічний тиск, наголошуючи на невідкладній необхідності «вирішення проблеми» [5].

Отже, маніпулювання є складним явищем, яке ґрунтується на використанні різноманітних психологічних прийомів. Удаючись до методів, гри на емоціях, соціальної інженерії, маніпулювання довірою, створення ілюзій та відволікання уваги, кіберзловмисники здатні ефективно впливати на рішення та поведінку своїх жертв. Розуміння цих прийомів є критично важливим для розроблення ефективних стратегій захисту від шахрайства. Підвищення обізнаності громадськості, навчання критичному мисленню та пошук технологічних рішень для виявлення та запобігання маніпуляціям можуть допомогти зменшити кількість жертв і мінімізувати негативні наслідки шахрайських дій.

Список використаних джерел

1. Боденчук Б., Савицька Д. Психологія обману: як працюють шахрайські схеми. *Суспільне*. 2024. URL: <https://suspilne.media/ternopil/653010-psihologia-obmanu-ak-pracuut-sahrajski-shemi/> (дата звернення: 07.04.2025).
2. Брисковська О. М. Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет. *Науковий вісник Національної академії внутрішніх справ*. 2020. С. 70–78 (дата звернення: 07.04.2025).
3. Коваленко Д. Як шахраї використовують психологію для маніпуляцій. *Гречка*. 2024. URL: <https://gre4ka.info/novyny/yak-shahrayi-vykorystovuyut-psyhologiyu-dlya-manipulyaczij/> (дата звернення: 07.04.2025).
4. Кравченко О. В. Психологічні особливості шахрайства: автореф. дис. ... канд. психол. наук: спец. 19.00.06 / Нац. ун-т внутр. справ. Харків, 2005. 21 с.
5. Самодін А. В. Особливості розслідування шахрайств. Київ. 2006. 35 с. URL: <https://www.navs.edu.ua/files/kafedru/ksm/shahraystvo.doc> (дата звернення: 07.04.2025).
6. Чайка Ю. А. Індивідуальна злочинна поведінка особи, яка вчиняє шахрайство як об'єкт наукових досліджень. Кропивницький: Донецький державний університет внутрішніх справ України. 2023. 296 с. URL: <https://dnuvs.ukr.education/wp-content/uploads/2023/04/dyser-tacziya-iga-chajka.pdf> (дата звернення: 07.04.2025).
7. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства: автореф. дис. ... д-ра юрид. наук: спец. 12.00.09 / Нац. акад. внутрішніх справ. Київ, 2010. 34 с.

