2. Кібербезпека: правові та психологічні аспекти // Пєтков В. В. // Київ: КНТ, 2021 р. // ст. 63–70 // URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf
3. Поради з кібербезпеки для громадян // Міністерство цифрової трансформації України // офіційний сайт // URL: https://thedigital.gov.ua/

Чистоклєтова Анна Денисівна
Студентка н.гр. 302 СПС ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

МЕТОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ У КІБЕРЗЛОЧИННОСТІ

Сучасний цифровий простір став не лише каналом передачі інформації, але й полем інтенсивної психологічної експлуатації: кіберзлочинці дедалі частіше змушують жертв приймати рішення, що шкодять їх інтересам.

Актуальність теми випливає з росту кількості фішингових атак, компрометацій акаунтів та витоку персональних даних [3]. Сучасні кібератаки дедалі частіше використовують соціальну інженерію, маніпуляцію увагою та емоціями жертв для досягнення фінансової, інформаційної або ж репутаційної вигоди, що зумовлює високий ризик системних втрат, як на рівні окремих користувачів, так і організацій. Та незважаючи на прогрес у технічних засобах захисту, їхня ефективність значною мірою залежить від розуміння та протидії психологічним механізмам, що маніпулюють увагою, емоційним станом жертви та спираються на соціальні правила поведінки.

У загальному вигляді під *кіберзлочинами* міжнародна спільнота розуміє: незаконний доступ, нелегальне перехоплення, втручання у дані або систему, зловживання пристроями, пов’язані з комп’ютерами, підробки та шахрайство, всі види забезпечення обігу та використання дитячої порнографії за допомогою комп’ютерної мережі, а також порушення авторських прав. Їх особливість полягає в середовищі здійснення – кіберпросторі, де «віртуальні» об’єкти психологічно сприймаються як більш доступні та менш захищені. Значущим криміногенним фактором також є анонімність користувачів, що дозволяє приховати особу, тим самим вводячи в оману інших та виступати під чужим іменем.

У поєднанні з дистанцією та відсутністю негайного соціального контролю, це послаблює моральні бар'єри, підсилює відчуття безкарності та створює сприятливі умови для вчинення злочинів [1].

Виходячи з описаних характеристик кіберпростору, можна виокремити низку конкретних психологічних методів впливу, які активно використовуються зловмисниками. Дані прийоми спрямовані на захоплення уваги, створення емоційного тиску та мобілізацію автоматичних реакцій жертви. Їхня мета – спонукання до конкретної дії (натискання посилання, введення даних, відкриття файлу або здійснення переказу), які в умовах спокійного, усвідомленого прийняття рішень жертва, швидше за все, не виконала б.

Відволікання уваги. Метод, що передбачає інсценування контакту від імені служби технічної підтримки. Під час телефонної розмови зловмисник інформує про нібито виявлене шкідливе ПЗ і наполягає на негайній інсталяції «інструмента для нейтралізації», який фактично є шкідливим. Щоб унеможливити критичне осмислення ситуації, шахрай застосовує спеціалізовану термінологію, демонструє сфабриковані вікна системних помилок і здійснює постійний психологічний тиск, апелюючи до терміновості [5].

Емоційна експлуатація. Зловмисники систематично використовують емоційні тригери – страх, жадібність, співчуття або почуття провини – щоб спонукати адресата до імпульсивних дій. Поширеною практикою є надсилання образливих або провокативних повідомлень від неідентифікованих профілів; зацікавлені користувачі переходять на сторінку відправника для з'ясування обставин. Часто такий профіль є закритим і містить лише одне гіперпосилання, розміщене угорі: воно викликає цікавість і підштовхує до переходу. Це посилання, як правило, є фішинговим і створює ризик несанкціонованого доступу до облікових записів у Telegram, Instagram чи інших сервісах [3].

Соціальна інженерія. Методика заснована на створенні ілюзії легітимності за допомогою підроблених документів, вебресурсів або електронних листів. Наприклад, фішингові повідомлення, що нібито надходять від банків, містять посилання на фальшиві сайти, а фейкові інвестиційні платформи супроводжуються підробленими ліцензіями й сертифікатами. Така тактика дозволяє отримувати персональні та фінансові дані жертв або схилити їх до здійснення платежів, оманливо спираючись на довіру, створену фіктивними атрибутами легітимності.

Створення ілюзії вигоди. Розсилка повідомлень про виграш значної суми або цінного подарунка супроводжується вимогою попередньої оплати «комісії» чи «податку» невеликого розміру. Обіцянка швидкого та легкого збагачення призводить до переказу коштів, після чого контакт з шахраями переривається.

Маніпулювання довірою. Кіберзлочинець, поінформований про близькі зв'язки жертви, може імітувати знайому особу – використовуючи схожий голос у дзвінку або надсилаючи повідомлення з підробленого профілю.

Апелювання до спільних спогадів або відомих лише вузькому колу деталей створює ілюзію достовірності; у такому контексті жертва часто без сумніву переказує кошти або надає конфіденційну інформацію [4].

Таким чином, психологічні методи впливу в кіберзлочинності призводять до суттєвих наслідків для жертв: прямі фінансові втрати, компрометація персональних і корпоративних даних, втрата доступу до акаунтів та довгострокові репутаційні й емоційні збитки. Часто пошкодження має каскадний характер – один скомпрометований обліковий запис полегшує подальші атаки. Отже, ефективний захист вимагає поєднання технічних заходів з організаційними процедурами й регулярним навчанням користувачів, що знижує імпульсивність рішень і підвищує стійкість до соціально-інженерних атак.

Список використаних джерел:

1. Деревягін О. О., Пашнєв Д. В., Новицький А. О. Окремі підходи до визначення сучасного портрету професійного кібершахрая. *Вісник Кримінологічної асоціації України*. 2025. Т. 34, № 1. С. 236–248. URL: https://doi.org/10.32631/vca.2025.1.17
2. Кравцова м. о. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ. Харків, 2016. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/8da73c50-5c7d-4ae4-85b4-30fa7107489f/content.
3. Коваленко Д. Як шахраї використовують психологію для маніпуляцій. Гречка. 2024. URL:https://gre4ka.info/novyny/yak-shahrayi-vykorystovuyut-psyhologiyu-dlya-manipulyaczij/
4. 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/dysertacziya-ira-chajka.pdf
5. Самодін А. В. Особливості розслідування шахрайств. Київ. 2006. 35 с. URL: https://www.navs.edu.ua/files/kafedru/ksm/shahraystvo.doc