ПРИКЛАДНІ ПРОБЛЕМИ ЮРИДИЧНОЇ ПСИХОЛОГІЇ

УДК 159.98: 343.985 doi: https://doi.org/10.33270/03212801.34

Козицька О. Г. – кандидат юридичних наук, доцент кафедри кримінального права та процесу Хмельницького університету управління та права імені Леоніда Юзькова, м. Хмельницький
ORCID: https://orcid.org/0000-0002-3045-8181

Використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень

Метою *статті є дослідження особливостей використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень, а також окреслення кола основних тактичних завдань, які можуть бути виконані за допомогою застосування окремих прийомів соціальної інженерії.* ***Методологія****. Основним методом, який використано під час підготовки статті, був діалектико-матеріалістичний метод наукового пізнання соціально-правових явищ. Крім того, застосовано загальнонаукові та спеціальні методи, зокрема: історико-правовий – для дослідження стану наукових досліджень проблем соціальної інженерії; порівняльно-правовий – під час аналізу думок науковців стосовно досліджуваної проблематики, наукової категорії «соціальна інженерія», інших визначень і підходів; догматичний – для тлумачення юридичних категорій, поглиблення й уточнення понятійного апарату; функціональний – для виокремлення кола тактичних завдань, які можуть бути реалізовані за допомогою методу соціальної інженерії.* ***Наукова новизна.*** *Уперше запропоновано розглядати соціальну інженерію як метод кіберрозвідки, що охоплює сукупність прийомів, які ґрунтуються на здійсненні психологічного впливу суб'єкта соціальної інженерії (слідчого, оперативного працівника) на об'єкт (особу, яка взаємодіє з кіберпростором шляхом використання електронно-цифрових приладів), з метою виконання окремих тактичних завдань у процесі виявлення, розкриття та розслідування кримінальних правопорушень.* ***Висновки.*** *Метод соціальної інженерії доцільно використовувати в процесі виявлення, розкриття, розслідування кримінальних правопорушень, а також розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання, і безвісно відсутніх осіб, з метою реалізації таких тактичних завдань, як ідентифікація особи за цифровим об'єктом; отримання криміналістично значущої інформації (переважно орієнтуючого характеру) про особу, яка вчинила кримінальне правопорушення або готується до цього; спонукання особи до вчинення певних дій або ж до утримання від їх вчинення. Основні прийоми соціальної інженерії ґрунтуються на здійсненні психологічного впливу на об'єкт соціальної інженерії. Подальшими науковими розвідками в цьому напрямі є дослідження окремих прийомів соціальної інженерії, які можна використовувати під час виявлення, розкриття, розслідування кримінальних правопорушень.*

Ключові слова: соціальна інженерія; кіберрозвідка; тактичне завдання; психологічний вплив; кримінальне правопорушення; кіберпростір.

Вступ

Сучасна тенденція розвитку злочинності засвідчує появу нових видів кримінальних правопорушень, місцем або знаряддям вчинення яких є кіберпростір, а також використання інформаційно-комунікаційних технологій під час підготовки та вчинення й інших видів протиправних діянь. Зазначене зумовлює необхідність удосконалення засобів, прийомів і методів пошуку, збирання, аналізу та використання криміналістично значущої інформації в процесі виявлення, розкриття, розслідування і профілактики кримінальних правопорушень. Одним із таких методів є соціальна інженерія, вивченню теоретичних та практичних аспектів застосування якого присвячено наше дослідження.

Загалом проблеми пошуку та збирання інформації з використанням інформаційно-комунікаційних технологій в процесі розкриття та розслідування злочинів висвітлено в працях таких вітчизняних науковців, як С. В. Албул, С. М. Князєв, О. Є. Користін, Ю. Ю. Орлов, М. А. Погорецький, В. Д. Хахановський, Ю. М. Чорноус та ін. Досліджували соціотехнічні аспекти інформаційної та кібербезпеки й соціальної інженерії як метод розвідки в інформаційно-телекомунікаційних системах В. Л. Бурячок, В. Б. Толубко, С. В. Толюпа, В. О. Хорошко. Не оминули увагою вивчення різноманітних напрямів використання соціальної інженерії в різних сферах суспільного життя й іноземні вчені, зокрема: О. В. Веселов, М. В. Кузнєцов, І. В. Сімдянов, S. Abraham, R. Anderson, M. Fincher, K. Hanagy, K. Popper та ін. Слід виокремити дисертаційне дослідження «Експериментальна соціальна інженерія. Розслідування та профілактика» нідерландського науковця J.-W. Bullee (Bullee, 2017), у якому схарактеризовано основні прийоми соціальної інженерії. Водночас особливості застосування соціальної інженерії як методу кіберрозвідки в правоохоронній та слідчій діяльності в науковій літературі майже не розглядали.

Мета і завдання дослідження

Мета статті полягає в дослідженні особливостей використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень.

З огляду на мету, необхідно було виконати такі завдання:

– проаналізувати основні підходи науковців щодо визначення поняття «соціальна інженерія»;

– дослідити сутнісну характеристику соціальної інженерії як методу кіберрозвідки;

– окреслити коло тактичних завдань, які можуть бути виконані за допомогою соціальної інженерії;

– визначити особливості здійснення психологічного впливу під час застосування прийомів соціальної інженерії.

Виклад основного матеріалу

Попри те, що вперше термін «соціальна інженерія» було використано в роботі R. Pound «Введення у філософію права» ще 1922 року (Pound, 1922), дотепер єдиний підхід щодо його розуміння не сформовано.

У широкому значенні соціальну інженерію розглянуто у філософії, соціології, педагогіці й теорії управління, його визначають як науку, науковий підхід або ж вид діяльності.

Зокрема, О. В. Веселов вважає, що соціальна інженерія – це міждисциплінарна наука і практична діяльність людей щодо регулювання суспільних відносин шляхом організації та розвитку соціальних систем різного рівня складності (Veselov, 2012, p. 8); Є. І. Суіменко зазначає, що соціальна інженерія є порівняно новою наукою, яка претендує на сукупність тих специфічних знань, які направляють, упорядковують й оптимізують процес створення, модернізації та відтворення нових («штучних») соціальних реальностей (Suimenko, 2000, p. 83). Також соціальну інженерію розглядають як форму управлінської діяльності, що полягає в науковій організації управління соціальними системами штучного типу, тобто приведення їх у відповідність з дією об'єктивних соціальних законів, виражених і обґрунтованих у наукових уявленнях і концепціях (Melnychenko, 2008, p. 41), як низку взаємопов'язаних, послідовних процедур, спрямованих на оцінку стану соціального об'єкта з метою виявлення шляхів і методів його модернізації (Urzha, 2017) або як цілеспрямовану діяльність суб'єктів державного управління на формування сталого розвитку території, побудову взаємодії між населенням та суб'єктами державного управління, подолання соціальної ліні (Drahomyretska, 2015).

У вузькому значенні соціальну інженерію розглядають як прийом, метод, чи спосіб отримання доступу до інформації або спонукання особи до вчинення певних дій. Такий підхід до визначення соціальної інженерії здебільшого використовують у теорії інформаційної безпеки та юридичних науках, зокрема в криміналістиці й теорії оперативно-розшукової діяльності.

Розглянемо декілька визначень, запропонованих науковцями. Зокрема, соціальна інженерія – це:

– метод несанкціонованого доступу до інформації чи систем збереження інформації без використання технічних засобів, ґрунтований на визначеній сукупності прийомів, методів і технологій прикладних соціальних наук (використовуються слабкі сторони людини та людський фактор), що дає змогу створити такий простір, умови й обставини, завдяки яким бажаного результату атаки на ціль досягають максимально ефективно (Okulovskaia, & Filippov, 2018, p. 39);

– один із найбільш перспективних методів кіберрозвідки, що полягає в одержанні неавторизованим користувачем (хакером, порушником) несанкціонованого доступу до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена й паролі, а також іншої конфіденційної інформації про об'єкт атаки – людину (або групу людей), використовуючи її (їх) слабкість або некомпетентність, непрофесіоналізм чи недбалість та керуючи її (їх) діями (Buriachok, V.L., Korchenko, & Buriachok, L.V., 2012, p. 7);

– систему способів впливу та контролю людей, що спонукає їх вчиняти певні дії, її застосовують з метою отримання персональних даних особи, а також іншої конфіденційної інформації для досягнення злочинного результату (Starostenko, 2020, p. 81);

– атаку, що здійснюють шляхом маніпулювання та обману з метою отримання конфіденційної інформації або доступу до інформаційних ресурсів (Fan, Lwakatare, & Rong, 2017, p. 1);

– використання соціальних масок, культурних і психологічних хитрощів з метою примушування користувача комп'ютера до надання злочинцям (хакерам) допомоги в незаконному втручанні та використанні комп'ютерних систем і мереж (Abraham, & Chengalur-Smith, 2010) тощо.

Проаналізувавши викладене вище, можемо дійти висновку, що значна кількість учених поділяє думку, що прийоми й техніки соціальної інженерії використовують здебільшого для досягнення протиправної мети і є способом вчинення кримінальних правопорушень. Водночас заслуговує на увагу позиція тих авторів, які розглядають можливість застосовування соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень.

До прикладу, Н. І. Старостенко пропонує ввести в курс «Криміналістика» системне знання про техніки соціальної інженерії, що застосовують під час вчинення злочинів, яке має охоплювати:

поняття соціальної інженерії, її види, ознаки технік, методи і способи їх виявлення, фіксування та використання в розкритті й розслідуванні злочинів (Starostenko, 2020, p. 82).

Учені Ю. М. Онищенко, К. Е. Петров та І. В. Кобзев розглядають можливість використання прийомів соціальної інженерії для попередження злочинів у кіберпросторі, зокрема шляхом створення сайтів-пасток. Учені виокремлюють три прийоми, які можуть бути використані оперативними працівниками:

а) встановлення IP-адреси користувача й подальше встановлення його особи. Суттю цього методу є створення сайту будь-якої тематики й виду з розміщенням на ньому програмного коду лічильника відвідувачів з можливістю фіксації IP-адреси та часу відвідування кожним користувачем мережі Інтернет;

б) залучення потенційних злочинців до спілкування на спеціально створеному тематичному ресурсі з метою отримання від них оперативної інформації;

в) дослідження актуальних методик хакерських атак. Цей метод полягає у створенні локальної мережі-приманки, тобто одного з різновидів пастки. Наживкою є захищений ресурс, призначення якого – виступати об'єктом зондування атак і зломів з боку хакерів (Onyshchenko, Petrov, & Kobzev, 2017, p. 66).

На нашу думку, перелік тактичних завдань, які можуть виконувати в процесі розкриття та розслідування кримінальних правопорушень за допомогою використання методу соціальної інженерії, є значно ширшим. Однак перед тим, як перейти до його детального розгляду, з'ясуємо сутність соціальної інженерії з позицій криміналістики й теорії оперативно-розшукової діяльності. Отже:

1) соціальна інженерія є одним з методів кіберрозвідки (кіберрозвідка полягає в гласному й негласному пошуку, збиранні, аналізі, оцінці та використанні інформації, яка розміщена в кіберпросторі, з метою виявлення, розкриття та розслідування кримінальних правопорушень, розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання та безвісно відсутніх осіб (Kozytska, 2020, p. 108);

2) метод соціальної інженерії охоплює сукупність прийомів (фішинг, вішинг, претекстінг тощо), застосування яких можливе лише щодо особи, яка взаємодіє з кіберпростором шляхом використання електронно-цифрових приладів (комп'ютера, планшета, мобільного телефону тощо);

3) прийоми соціальної інженерії ґрунтуються на здійсненні психологічного впливу суб'єкта соціальної інженерії (слідчого, оперативного працівника) на об'єкт;

4) результатом застосування методу соціальної інженерії є отримання інформації, яку особа бажала залишити в таємниці від слідчого або оперативного працівника, або виконання цією особою певних дій (наприклад, поява в обумовленому місці) чи утримання від їх виконання (наприклад, відмова від вчинення кримінального правопорушення);

5) мета застосування соціальної інженерії має бути виключно суспільно корисною – виявлення, припинення, профілактика, розкриття та розслідування кримінальних правопорушень, розшук осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання, і безвісно відсутніх осіб;

6) застосування окремих прийомів соціальної інженерії можливе лише за умови дотримання прав і свобод людини та громадянина.

Основними тактичними завданнями, які можуть бути виконані за допомогою методу соціальної інженерії, є:

а) ідентифікація особи за цифровим об'єктом (встановлення належності сторінки в соціальній мережі конкретній особі; встановлення фактичного користувача абонентського номеру мобільного зв'язку; встановлення анкетних даних особи, яка розмістила протиправний контент у мережі Інтернет, телеграм-каналі тощо (наприклад, оголошення про продаж зброї, порнографічні матеріали);

б) отримання криміналістично значущої інформації (переважно орієнтуючого характеру) про особу, яка вчинила кримінальне правопорушення або готується до його вчинення (актуальні номери телефонів, адреса фактичного проживання, транспортні засоби, якими користується, місця, які відвідує з протиправною метою, наприклад, для вживання наркотичних засобів);

в) спонукання особи до вчинення певних дій або ж до утримання від їх вчинення (наприклад, спонукання особи, яку розшукують, з'явитися у визначеному місці або написати повідомлення чи зателефонувати з власного номеру телефону; переконання особи в недоцільності продажу викраденого майна, яке знаходиться в її незаконному володінні).

Використання методу соціальної інженерії для виконання зазначених вище тактичних завдань допускається виключно з метою виявлення, розкриття, розслідування кримінальних правопорушень, а також розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання та безвісно відсутніх осіб.

Загалом метод соціальної інженерії охоплює низку різноманітних прийомів, до яких можна віднести фішинг, вішинг, претекстінг, зворотну

соціальну інженерію тощо. Детальне вивчення таких прийомів становить предмет окремого дослідження, однак слід зауважити, що всі вони ґрунтуються на здійсненні психологічного впливу суб'єкта соціальної інженерії (слідчого, оперативного працівника) на об'єкт – особу, яка взаємодіє з кіберпростором.

Психологічний вплив є обов'язковим суттєвим елементом криміналістичної (слідчої) тактики, постійним джерелом формування тактичних рекомендацій та неодмінним структурним компонентом тактичних прийомів й операцій процесуального й допоміжного (оперативного) характеру, становить комплекс прийомів, застосовуваних у процесі передавання, опрацювання та використання інформації, які викликають відповідну реакцію, що дає змогу діагностувати психічний стан особи, контролювати перебіг її думок, ставлення до фактів для зміни її поведінки (Sokyran, 2019, p. 15).

Нідерландський дослідник J.-W. Bullee (Bullee, 2017) зазначає, що успішність застосування прийомів соціальної інженерії зумовлена використанням під час здійснення психологічного впливу таких прагнень і рис особистості, як: повага до авторитетів, прагнення людей підпорядковуватися вимогам авторитетних осіб (якщо людина не може самостійно прийняти рішення, вона прагне перекласти відповідальність за його прийняття на групу осіб або іншу авторитетну особу); конформізм, соціальне доказування – імітація особою поведінки інших людей (прагнення наслідувати поведінку інших залежить від чисельності групи осіб, яка діє відповідно; вдячність, взаємність (людина починає відчувати себе в боргу, отримавши навіть незначний подарунок, а отже, прагне віддячити); прагнення дотримуватися наданих обіцянок; симпатія (людина відчуває сильнішу симпатію до того, у кого схожі погляди, інтереси, переконання); прагнення володіти тим, що становить дефіцит (люди сприймають дефіцитний товар, послуги, інформацію як більш цінні; що менше товару є в наявності, то бажанішим він стає для людини) (Bond, & Smith, 1996, p. 5-6).

Крім того, під час застосування прийомів соціальної інженерії враховують такі принципи й ефекти:

– принцип першочерговості, що ґрунтується на специфіці психіки, яка влаштована так, що сприймає інформацію, яка надійшла першою, як достовірну;

– ефект правдоподібності – людина схильна вірити інформації, що не суперечить її внутрішньому «Я»;

– ефект «інформаційного штурму», який полягає в тому, що індивід перебуває в потоці непотрібної та некорисної інформації, у якому втрачається суть основного інформаційного повідомлення;

– емоційне забарвлення – що більш емоційно забарвлена інформація, то менш критично її сприймають;

– несподіване одкровення або раптова чесність – після нетривалої бесіди повідомляють нібито секретні й важливі відомості, унаслідок чого в людини виникає довіра до співрозмовника;

– удавана байдужість або псевдонеуважність – якщо людина відчуває, що її слова сприймають байдуже, вона прагне переконати співрозмовника у своїй значущості для нього (Voitko, Katsalap, & Rakhimov, 2019, p. 123-124).

Під час застосування методу соціальної інженерії обов'язковим є дотримання прав і свобод людини й громадянина, у зв'язку з чим обрані прийоми психологічного впливу не повинні принижувати честь, гідність особи чи мати дискримінаційний характер. Крім того, слушно зазначає Ю. М. Чорноус, застосування тактичних прийомів має передбачати ретельну підготовку, що охоплює перевірку їх відповідності правовим і морально-етичним нормам; оцінку можливого тактичного ризику та його виправданість; прогнозування поведінки учасників; визначення заходів на випадок невідкладності дій та виходу ситуації з-під контролю; використання отриманих результатів (Chornous, 2020, p. 17). Хоча науковець мала на увазі підготовку до застосування тактичних прийомів під час проведення слідчих (розшукових) дій, на нашу думку, цілком доречно дотримуватися зазначених вимог і в процесі підготовки до застосування прийомів соціальної інженерії.

Наукова новизна

Наукова новизна здійсненого дослідження полягає в тому, що вперше запропоновано соціальною інженерією вважати метод кіберрозвідки, що охоплює сукупність прийомів, ґрунтованих на здійсненні психологічного впливу суб'єкта соціальної інженерії (слідчого, оперативного працівника) на об'єкт (особу, яка взаємодіє з кіберпростором шляхом використання електронно-цифрових приладів), з метою виконання окремих тактичних завдань у процесі виявлення, розкриття та розслідування кримінальних правопорушень. Крім того, визначено основні тактичні завдання, які можуть бути реалізовані за допомогою методу соціальної інженерії. Увагу акцентовано на особливостях здійснення психологічного впливу суб'єкта соціальної інженерії (слідчого, оперативного працівника) на об'єкт (особу) з метою отримання інформації або виконання цією особою певних дій чи утримання від їх виконання.

Висновки

Резюмуючи, зазначимо, що соціальна інженерія є одним з методів кіберрозвідки, який охоплює низку прийомів, які ґрунтовані на здійсненні психологічного впливу. Застосування прийомів соціальної інженерії можливе лише стосовно особи, яка взаємодіє з кіберпростором шляхом використання електронних приладів, для отримання інформації, яку особа бажала залишити в таємниці від слідчого або оперативного працівника, або виконання цією особою певних дій чи утримання від їх виконання. Допускається використання методу соціальної інженерії виключно із суспільно корисною метою – під час виявлення, припинення, профілактики, розкриття та розслідування кримінальних правопорушень, розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання, і безвісно відсутніх осіб та за умови неухильного дотримання прав і свобод людини й громадянина.

До основних тактичних завдань, які можуть бути виконані за допомогою методу соціальної інженерії, належать: ідентифікація особи за цифровим об'єктом; отримання криміналістично значущої інформації (переважно орієнтуючого характеру) про особу, яка вчинила кримінальне правопорушення або готується до його вчинення; спонукання особи до вчинення певних дій або ж до утримання від їх вчинення.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics and implication. *Technjljgy in Society, 32(3),* 183-196. doi: 10.1016/j.techsoc.2010.07.001.

Bond, R., & Smith, P.B. (1996). Culture and conformity: A meta-analysis of studies using asch's (1952b, 1956) line judgment task. *Psychological Bulletin, 119(1),* 111-137. doi: 10.1037/0033-2909.119.1.111.

Bullee, J.-W. (2017). Experimental Social Engineering Investigation & Prevention. *Doctor's thesis.* Enschede, The Niderland. doi: 10.3990/1.9789036543972.

Buriachok, V.L., Korchenko, O.H. & Buriachok, L.V. (2012). Sotsialna inzheneriia yak metod rozvidky informatsiino-telekomunikatsiinykh system [Social engineering as a method of intelligence of information and telecommunication systems]. *Zakhyst Informatsii, Information protection, 4,* 5-12. doi :10.18372/2410-7840.14.3471 [in Ukrainian].

Chornous, Yu.M. (2020). Psykholohichni osnovy realizatsii taktychnykh pryiomiv [Psychological Basics of Tactical Techniques Application]. *Yurydychna psykholohiia, Legal psychology, 1(26).* 13-21. doi: https://doi.org/10.33270/03202601.13 [in Ukrainian].

Drahomyretska, N.M. (2015). Suchasne zarubizhne rozuminnia sotsialnoi inzhenerii ta yii mozhlyvosti v derzhavnomu upravlinni [Modern foreign understanding of social engineering and its possibilities in public administration]. *Teoriia ta praktyka derzhavnoho upravlinnia i mistsevoho samovriaduvannia, Theory and practice of public administration and local self-government. 2.* Retrieved from http://el-zbirn-du.at.ua/2015_2/32.pdf [in Ukrainian].

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security, 1,* 1-11. doi: 10.5815/ijcnis.2017.01.01.

Kozytska, O.H. (2020). Kiberrozvidka yak novitnii napriam operatyvno-rozshukovoi diialnosti [Cyberintelligence as the newest direction of operative-search activity]. *Naukovii protses ta naukovi pidkhody: metodyka ta realizatsiia doslidzhen, Scientific process and scientific approaches: methods and implementation of research:* Proceedings of the International Scientific Conference (Vol. 1), (pp. 107-109). Odesa: MTsND. doi: 10.36074/23.10.2020.v1.13 [in Ukrainian].

Melnychenko, A.A. (2001). Problema spivvidnoshennia sotsialnoi inzhenerii ta sotsialnoho upravlinnia: filosofska refleksiia [The problem of the relationship between social engineering and social management: philosophical reflection]. *Visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho, Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky", 1(22),* 40-43. Retrieved from https://ela.kpi.ua/handle/123456789/8747 [in Ukrainian].

Okulovskaia, A.G., & Filippov, I.E. (2018). Sotsialnaia inzneneriia: opredelenie, tekhniki ataki, sposoby zashchity [Social engineering: definition, attack techniques, methods of defense]. *Innovatsionnoe razvitie nauki i obrazovaniia, Innovative development of science and education:* Proceedings of the 3rd International Scientific and Practical Conference (pp. 38-42). Penza: MTsNS [in Russian].

Onyshchenko, Yu.N., Petrov, K.E., & Kobzev, I.V. (2017). Protydiia zlochynam, shcho vchyniaiutsia za dopomohoiu metodiv sotsialnoi inzhenerii v Interneti [Counteraction crimes committed by the methods of social engineering in the Internet]. *Pravo i Bezpeka, Law and Security, 1,* 63-68 [in Ukrainian].

Pound, R. (1922). *An Introduction to the Philosophy of Law*. London: New Haven; Yale University Press. Retrieved from https://oll-resources.s3.us-east2.amazonaws.com/oll3/store/titles/2222/Pound_1502_EBk_v6.0.pdf.

Sokyran, F.M. (2019). Zastosuvannia psykholohichnoho vplyvu v kryminalnomu sudochynstvi [The application of psychological impact in criminal proceedings]. *Kryminalistychnyi Visnyk, Forensic Bulletin, 32(2),* 15-21. doi: 10.37025/1992-4437/2019-32-2-15 [in Ukrainian].

Starostenko, N.I. (2020). Kriminalisticheskiy aspekt tekhnik sotsialnoy inznenerii pri sovershenii prestupleniy [The forensic aspect of social engineering techniques in the commission of crimes]. *Vestnik Krasnodarskogo universiteta MVD Rossii, Bulletin of Krasnodar University of the Ministry of Internal Affairs of Russia, 1(47),* 80-83 [in Russian].

Suimenko, E.I. (2000). Sotsialnaia inzneneriia: k voprosu v nauchnom statuse [Social engineering: a question in scientific status]. *Sotsiolohichna nauka i osvita v Ukraini, Sociological Science and Education in Ukraine, 1,* 82-97 [in Russian].

Urzha, O.A. (2017). Sotsialnaia inzneneriia kak metodologiia upravlencheskoy deiatelnosti [Social engineering as a methodology of management activities]. *Sotsiologicheskie issledovaniia, Sociological research, 10,* 87-96. doi: https://doi.org/10.7868/S0132162517100099 [in Russian].

Veselov, A.V. (2012). Sotsialnaia inzneneriia: suschnost i paradigmalnaia metodologiia [Social engineering: essence and paradigm methodology]. *Extended abstract of candidate's thesis*. Moscow [in Russian].

Voitko, O.V., Katsalap, V.O., & Rakhimov, V.V. (2019). Analiz osoblyvostei manipuliatsii yak instrumentu psykholohichnoho vplyvu na svidomist [Analysis of the peculiarities of manipulation as a tool of psychological influence on consciousness]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, Modern information technologies in the sphere of security and defence, 2(35),* 121-126. doi: 10.33099/2311-7249/2019-35-2-121-126 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Abraham S., Chengalur-Smith I. An overview of social engineering malware: Trends, tactics and implication. *Techniljgy in Society.* 2010. No. 32 (3). P. 183–196. doi: 10.1016/j.techsoc.2010.07.001.

Bond R., Smith P. B. Culture and conformity: A meta-analysis of studies using asch's (1952b, 1956) line judgment task. *Psychological Bulletin*. 1996. No. 119 (1). P. 111–137. doi: 10.1037/0033-2909.119.1.111.

Bullee J.-W. Experimental Social Engineering: Investigation and Prevention : dissirtation to obtain the degree or doctor at the University of Twente. Enschede, The Niderland, 2017. 178 p. doi: 10.3990/1.9789036543972.

Бурячок В. Л., Корченко О. Г., Бурячок Л. В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем. *Захист інформації.* 2012. № 4. С. 5–12. doi :10.18372/2410-7840.14.3471.

Чорноус Ю. М. Психологічні основи реалізації тактичних прийомів. *Юридична психологія.* 2020. № 1 (26). С. 13–21. doi: https://doi.org/10.33270/03202601.13.

Драгомирецька Н. М. Сучасне зарубіжне розуміння соціальної інженерії та її можливості в державному управлінні. *Теорія та практика державного управління і місцевого самоврядування*. 2015. № 2. URL: http://el-zbirn-du.at.ua/2015_2/32.pdf.

Fan W., Lwakatare K., Rong R. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*. 2017. No. 1. P. 1–11. doi: 10.5815/ijcnis.2017.01.01.

Козицька О. Г. Кіберрозвідка як новітній напрям оперативно-розшукової діяльності. *Науковий процес та наукові підходи: методика та реалізація досліджень* : матеріали Міжнар. наук. конф. (Одеса, 23 жовт. 2020 р.). Одеса : МЦНД, 2020. Т. 1. С. 107–109. doi: 10.36074/23.10.2020.v1.13.

Мельниченко А. А. Проблема співвідношення соціальної інженерії та соціального управління: філософська рефлексія. *Вісник Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського.* 2008. № 1 (22). С. 40–43. (Серія «Філософія. Психологія. Педагогіка»). URL: https://ela.kpi.ua/handle/123456789/8747.

Окуловская А. Г., Филиппов И. Е. Социальная инженерия: определение, техники атаки, способы защиты. *Инновационное развитие науки и образования* : сб. ст. III Междунар. науч.-практ. конф. Пенза : МЦНС, 2018. С. 38–42.

Онищенко Ю. М., Петров К. Е., Кобзев І. В. Протидія злочинам, що вчиняються за допомогою методів соціальної інженерії в Інтернеті. *Право і безпека.* 2017. № 1 (64). С. 63–68.

Pound R. An Introduction to the Philosophy of Law. London : New Haven ; Yale University Press, 1922. URL: https://oll-resources.s3.us-east2.amazonaws.com/oll3/store/titles/2222/Pound_1502_EBk_v6.0.pdf.

Сокиран Ф. М. Застосування психологічного впливу в кримінальному судочинстві. *Криміналістичний вісник.* 2019. № 32 (2). С. 15–21. doi: 10.37025/1992-4437/2019-32-2-15.

Старостенко Н. И. Криминалистический аспект техник социальной инженерии при совершении преступлений. *Вестник Краснодарского университета МВД России*. 2020. № 1 (47). С. 80–83.

Суименко Е. И. Социальная инженерия: к вопросу в научном статусе. *Соціологічна наука і освіта в Україні.* 2000. Вип. 1. С. 82–97.

Уржа О. А. Социальная инженерия как методология управленческой деятельности. *Социологические исследования*. 2017. № 10. С. 87–96. doi: https://doi.org/10.7868/S0132162517100099.

Веселов А. В. Социальная инженерия: сущность и парадигмальная методология : автореф. дис. ... канд. филос. наук : 09.00.11. М., 2012. 31 с.

Войтко О. В., Кацалап В. О., Рахімов В. В. Аналіз особливостей маніпуляції, як інструменту психологічного впливу на свідомість. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 2 (35). С. 121–126. doi: 10.33099/2311-7249/2019-35-2-121-126.

Стаття надійшла до редколегії 15.01.2021

Kozytska O. – Ph.D in Law, Associate Professor of the Department of Criminal Law and Procedure of the Leonid Uzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine
ORCID: https://orcid.org/0000-0002-3045-8181

The Use of Social Engineering in the Process of Identification, Detection and Investigation of Criminal Offenses

*The **purpose** of the article is to study the features of the use of the method of social engineering in the process of identification, detection and investigation of criminal offenses, as well as determining the range of basic tactical tasks that can be solved using certain techniques of social engineering. **Methodology.** The main method used in the preparation of the article was the dialectical-materialistic method of scientific knowledge of social and legal phenomena. In addition, general scientific and special methods were used, in particular, historical and legal methods – when considering the state of scientific research on the problems of social engineering; comparative legal – when analyzing the opinions of scientists regarding the problem under study, the scientific category «social engineering», other definitions and approaches; dogmatic – for the interpretation of legal categories, deepening and clarifying the conceptual apparatus; functional – in order to highlight the range of tactical tasks that can be solved using the method of social engineering. **Scientific novelty.** For the first time, the author proposed to consider social engineering as a method of cyber intelligence, which includes a set of techniques based on the implementation of the psychological impact of the subject of social engineering (investigator, operative worker) on an object (a person who interacts with cyberspace through the use of electronic digital devices), in order to solve certain tactical tasks in the process of identifying, solving and investigating criminal offenses. **Conclusions.** The method of social engineering is advisable to use in the process of identification, detection and investigation criminal offenses, as well as for searching for persons hiding from the pre-trial investigation authorities, investigating judge, court or evading criminal punishment and missing persons, in order to solve such tactical tasks as personal identification by a digital object; obtaining forensically significant information (mainly orienting nature) about a person who has committed a criminal offense or is preparing to commit it; persuading a person to perform certain actions or to refrain from performing them. The basic techniques of social engineering are based on the implementation of psychological impact on the object of social engineering. Subsequent scientific research in this direction is the study of individual techniques of social engineering that can be used in the process of identifying, disclosing, and investigating of criminal offenses.*

Keywords: social engineering; cyber intelligence; tactical task; psychological influence; criminal offense; cyberspace.