УДК 341.32:681.3.06

КОВАЛЬЧУК А.Ю., *доктор юридичних наук, доцент*, начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4807-2436.

ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, старший науковий співробітник*, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0001-7496-9904.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВПЛИВИ ЯК ЗАСІБ МАНІПУЛЯЦІЇ СВІДОМІСТЮ, ЩО ЗАСТОСОВУЄТЬСЯ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПУВАННЯМИ

Анотація. *У статті визначено проблему недостатнього правового та організаційного забезпечення перешкоджанню діяльності організованим злочинним угрупованням у мережі Інтернет. Виділено проблему застосування методів інформаційно-психологічних впливів, що застосовуються організованими злочинними угрупованнями з метою розширення сфер впливу їх злочинної діяльності. Звертається увага на такі види кримінальних маніпуляцій свідомістю людини, що застосовуються для вчинення кіберсталкінгу, кібершахрайства та інших протиправних діянь. Вважається, що в Україні вкрай необхідно розвивати напрям дослідження – кібервіктимологію.*

Ключові слова: *інформаційна безпека, інформаційно-психологічна безпека, організована злочинність, кібервіктимологія.*

Summary*. The article identifies the problem of insufficient legal and organizational support for obstructing the activities of organized criminal groups on the Internet. The problem of application of methods of information and psychological influences used by organized criminal groups in order to expand the spheres of influence of their criminal activities is highlighted. Attention is drawn to the following types of criminal manipulation of human consciousness, which are used to commit cyberstalking, cyber fraud and other illegal acts. It is believed that in Ukraine it is extremely necessary to develop the field of research – cyber victimology.*

Keywords: *information security, information and psychological security, organized crime, cyber victimology.*

Постановка проблеми. Революційний за своїми темпами розвиток інформаційно-комунікаційних технологій призвів до суттєвої трансформації життєдіяльності людини. Як наслідок, людство опинилося як перед принципово новими можливостями, так і перед принципово новими викликами та загрозами особистій безпеці в інформаційному просторі. Технологічна революція змінила соціальний контекст буття людини, трансформувала цивілізаційний статус самого суспільства: з суспільства виробничого у суспільство інформації, суспільство знань. Соціальна комунікація, як особлива система, набула статусу соціально-технологічного всесвіту який не має меж і відповідно правил поведінки і співіснування у ньому. Такими змінами в існуванні суспільства безумовно скористалися й організовані злочинні угруповання, діяльність яких проникла в усі сфери життєдіяльності країни, охопила цілі галузі і регіони, завдаючи значної економічної шкоди, підриваючи авторитет держави, суспільної моралі

та моральності. Прагнення більшості організованих злочинних угруповань до широкого розмаху своєї діяльності та розширення сфер свого злочинного впливу на нові регіони, прагнення освоїти нові види злочинної діяльності – одна зі закономірностей організованої злочинної діяльності. Аналіз вітчизняних і зарубіжних джерел, з питань визначення та характеристики організованої злочинності показав, що це складний, багатогранний і, найголовніше, соціальний феномен, що динамічно розвивається і трансформується в умовах глобалізації. Слід зазначити, що нові кіберзлочини вчиняються з урахуванням поточного розвитку біотехнологічних, інформаційних, когнітивних, комунікативних, комп'ютерних, космічних, робототехнічних та інших інформаційно-телекомунікаційних технологій (наприклад, створюють і використовують шкідливе програмне забезпечення для незаконного одержання (майнінгу) криптовалют; розкрадання та використання для шахрайства баз біометричних даних громадян, облікових даних користувачів соціальних мереж та ін.; створення "ботнетів" із пристроїв "Інтернету речей"; створення шахрайських "Інтернет-магазинів" та рекламних сайтів Інтернет-торгівлі; впровадження "закладок" в апаратне та програмне забезпечення мобільних пристроїв тощо. Загальні збитки від кіберзлочинності і витрати на захист від кіберзлочинів збільшилися за два роки більш ніж на 50 % і в 2020 склали $1,1 трлн. або більше 1 % світового ВВП. У 2018 році збитки від кіберзлочинців становили $600 млрд. [1].

В останні роки в усьому світі зберігається тенденція щодо збільшення кількості кіберзлочинів, які спрямовані на отримання фінансового прибутку. Глобальні збитки від кіберзлочинності у 2025 році за прогнозами фахівців становитимуть до $10,5 трлн. щорічно [2]. Значну частину збитків становлять втрати через кібершахрайства. Серед методів, які активно використовують кібершахраї, слід зазначити соціальну інженерію – науку, яка вивчає людську поведінку та фактори, що на неї впливають. Соціальна інженерія є багатогранним і складним способом отримання конфіденційної інформації від користувачів із застосуванням методів переконання і технологічних засобів.

Методи прихованого впливу на поведінку людини вже використовують злочинні угруповання, створюючи розгалужені мережі клубів типу "Спейс" у багатьох державах, у тому числі в Україні. На членів цих клубів здійснюється спланований вплив із застосуванням навіювання, гучної музики та прийомів, що звужують свідомість і створюють стресові ситуації. Після такої обробки люди втрачають здатність розсудливо мислити й сліпо виконують чужу волю [3].

Результати аналізу наукових публікацій. Проблеми забезпечення інформаційної безпеки у кіберпросторі є предметом аналізу багатьох науковців, у фокусі їхньої уваги ціла низка питань, а саме: нормативно-правове регулювання інформаційної безпеки України, загрози інформаційній безпеці у нашій державі та у світі, технічні, психологічні, лінгвістичні інструменти й засоби маніпулювання, способи захисту від негативних впливів на свідомість мас [5; 6; 8 – 10]. Проте багато питань потребують свого розв'язання.

На сьогодні, нормативно-правовим фундаментом забезпечення інформаційно-психологічної безпеки, є низка статей Конституції України, крім того, основу галузевого законодавства складають п'ятнадцять базових законів і значний корпус пов'язаних нормативно-правових актів. За підрахунками фахівців, кількість тільки Законів України, в яких регулюються суспільні інформаційні відносини, перевищила 260 [4].

Метою статті є розгляд заходів інформаційно-психологічного впливу на свідомість громадян, що здійснюються організованими злочинними угрупуваннями з метою втягнення у злочинну діяльність, а також маніпуляцією свідомістю для примушення вчинити певні злочинні дії.

Виклад основного матеріалу. Інформаційна сфера, кіберпростір не стає виключенням для захоплення й використання його з метою розширення сфер впливу організованої злочинності. Важливо зазначити, що організована злочинність має величезні фінансові можливості, неконтрольовані ні державою, ні суспільством, а також власну систему внутрішнього управління, яка спрямована на отримання надприбутків за рахунок застосування різних засобів досягнення власних інтересів. Окрім того, сучасні інструменти комунікації дозволяють їх розширювати й удосконалювати свою злочинну діяльність прилаштовуючи новітні методики впливу на когнітивну систему людей з метою заволодіння їх ресурсами, а також розширення злочинних зв'язків. Пересічні громадяни не в змозі протистояти таким діям, більш того, подекуди вони навіть не можуть ідентифікувати загрози їх нормальному психологічному стану й не усвідомлюють настання негативних для них наслідків. Окрім того, на сьогодні українське законодавство насправді містить достатньо ***обмежений інструментарій для протидії шкідливому контенту в Інтернеті.*** Передумовою такому стану є непідготовленість українського суспільства до переходу від матеріального світу до інформаційного.

Діяльність організованих злочинних угруповань швидше прилаштовується до нових реалій буття суспільства, усе частіше застосовуються нові, новаторські способи задоволення власних інтересів. Окрім інформаційної зброї (наявної: дезінформації, суперечливий наратив тощо) нині створено багато нових засобів впливу на психіку людей і управління їхньою поведінкою. Сучасний розвиток науки й техніки набув такого рівня, коли створена реальна можливість масового поширення новітніх технологій, що дають змогу застосовувати засоби та методи для прямого й непрямого впливу на нервову систему людини з метою зміни її функціонування.

Тобто, ***першою*** й вихідною проблемою забезпечення інформаційно-психологічної безпеки є відсутність стандартів ідентифікації викликів (постійна розробка методів удосконалення й ефективного застосування "м'якої сили", соціальної інженерії), загроз (застосування психологічного, психоемоційного та ментального впливу), а також високий ступінь сингулярності у процесі управління ризиками, що супроводжують стан інформаційно-психологічної безпеки.

Другою вихідною проблемою вбачається – ідентифікація джерела загрози: уряд іншої держави, інтереси приватної особи, інтереси організованого злочинного угруповання.

Кримінальне маніпулювання здійснюється в комунікативному процесі під час взаємодії злочинця та жертви з використанням комплексу методів і прийомів, у тому числі сучасних психотехнологій. О.В. Кравченко визначає кримінальну маніпуляцію як процес цілеспрямованого використання різних специфічних способів і засобів зміни (модифікації) поведінки жертви злочину, її мети, бажань, намірів, відносин, установок, психічних станів та інших її психологічних характеристик в інтересах шахрая, які могли б не відбутися, якби потерпілий знав у достатньому обсязі дані, що характеризують ситуацію, зокрема те, які засоби застосовано щодо нього чи з якою метою їх використано [5].

Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Через це надійність комп'ютерної системи є не вищою, ніж надійність її оператора. Зловмисники проникають навіть у добре спроектовані, захищені комп'ютерні системи, скориставшись неуважністю довірливих користувачів або умисно вводячи їх в оману. Обман (повідомлення потерпілому неправдивих відомостей або приховування певних обставин) чи зловживання довірою (недобросовісне використання довіри потерпілого) під час шахрайства, зловмисник застосовує щоб викликати в потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього. Обов'язковою

ознакою шахрайства є добровільне передавання потерпілим майна чи права на нього. Обман під час шахрайства – це повідомлення явно помилкових даних або приховування, замовчування інформації про факти чи обставини, повідомити про які було необхідно, спрямовані на введення потерпілого в оману або на підтримання помилки особи з метою заволодіння чужим майном, і які призвели до такого стану потерпілого [6]. Ошуканство (outing & trickery) – отримання персональної інформації в міжособовій комунікації й передання її (текстів, фото, відео) в публічну зону Інтернету або поштою тим, кому вона не призначалася. Існують і інші заходи маніпуляцій, так наприклад соціотехніка. Під цим терміном позначаються шахрайські дії, що спрямовані на отримання інформації, яка дає змогу проникнути до певної системи та даних, що в ній знаходяться. Соціотехніка зазвичай є грою зловмисника на довірі людини. Захист від атак, заснованих на зворотній соціотехніці, є досить важким. У жертви немає підстав підозрювати зловмисника у чомусь, оскільки при таких атаках створюється враження, що ситуація знаходиться під її контролем. Претекстинг (від англ. pretexting) у Великій Британії також використовується термін blagging чи bohoing, полягає у застосуванні заздалегідь розробленого сценарію (приводу, чи претексту) спонукаючи вибрану жертву до розголошення інформації чи виконання дій, до яких у звичайних обставинах вона не вдалася б. Оскільки цей метод ґрунтується на спланованій схемі обману, то атаці передує збір інформації, необхідної шахраєві для того, аби видати себе за іншу особу (з'ясування дати народження, паспортних та інших ідентифікуючих даних, суми останнього рахунку тощо), щоб у жертви не виникало сумнівів у законності дій шахрая [7]. Кібергрумінг – це шахрайські дії, що пов'язані з отримання інтимних фото, або відео з метою подальшого шантажу, з метою отримання ще більш відвертих матеріалів, грошей, або з метою примушення до особистих зустрічей в офф-лайні.

Слід відзначити, що для застосування методів соціальної інженерії не потрібні технічні знання, але негативні наслідки можуть бути значні. Інфраструктура й мистецтво їх застосування постійно удосконалюються та набувають тенденцію до активізації. Враховуючи розширення масштабів діяльності організованої злочинності все більше застосовуються методи "м'якої сили". Прищеплення зовнішній аудиторії власних стандартів, специфічних цінностей через маніпулятивні засоби масової інформації, комплекс дипломатичних, когнітивних, культурно-освітніх ***інструментів несилового впливу*** дозволяє без застосування зброї справляти необхідний вплив на населення й політичні кола іноземних держав. Сам термін "м'яка сила" (softpower) у науковий обіг був введений американським політологом, професором Гарвардського університету, колишнім заступником міністра оборони США з питань міжнародної безпеки Джозефом С. Наємом-молодшим. За Дж. Наємом, "м'яка сила" (або "м'який" вплив, влада) – це здатність досягати бажаного шляхом приваблення та переконання інших до засвоєння ваших цілей [8]. Тобто не застосовується насильство у будь-якому прояві, психологічне, емоційне та ментальне. За допомогою "м'якої сили" можливе втілення у життя будь-яких власних інтересів без погроз чи прямого силового впливу [9].

Для досягнення злочинних цілей дедалі частіше використовуються ***штучний інтелект*** і ***bot-мережі.*** Застосування методів "м'якої сили", соціальної інженерії спрямоване ***не безпосередньо на комп'ютерну систему, а на її користувачів*** – "найслабшу ланку", і шляхом обходу інфраструктури, призначеної для захисту від шкідливого програмного забезпечення, він дозволяє досягти тих же результатів, що й інші види кібератак. Оскільки такі прийоми значно складніше виявити чи запобігти їм, цей напрям атак є набагато ефективнішим за інші. Основна тактика соціальної інженерії – за допомогою психологічних методів (наприклад, спілкуючись начебто від імені

сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо).

Висновки.

Сучасне суспільство у своїй сутності є технотронним, тобто залежним від техніки та високих технологій (інформаційно-комунікаційних, когнітивних, робототехнічних та ін.), активно використовуючи у повсякденному житті: комп'ютери, інформаційно-телекомунікаційні мережі, мобільні засоби зв'язку, Інтернет-речей та інші засоби створення, пошуку, збирання, зберігання, обробки, поширення інформації. В Україні вкрай необхідно розвивати напрям дослідження ***кібервіктимології як нової реальності існування суспільства.*** Розробка та обґрунтування кібервіктимології дозволить об'єднати методологічні підходи, узагальнити результати теоретичних і практичних розвідок, котрі пов'язані з виявленням і систематизацією видів кіберзлочинів, типів кіберзлочинців, чинників, джерел та наслідків найактуальніших кіберзагроз, ***соціально-психологічних механізмів кібервіктимізації***, ознак та особливостей становлення кібервіктимності й кібервіктимної поведінки осіб різних вікових груп, різного соціального статусу, осіб з різною професійною, конфесійною та іншою приналежністю тощо.

Використана література

1. Убытки от киберпреступности в мире выросли за два года на 50 % до $945 млрд. URL: https://forinsurer.com/news/20/12/10/38866

2. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. URL: https://cybersecurity ventures.com/cybercrime-damage-costs-10-trillion-by-2025

3. Сугестивні технології маніпулятивного впливу: навч. посіб. / В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш, О.Д. Бойко, В.В. Остроухов; за заг. ред. Є.Д. Скулиша. 2-ге вид. Київ: ЗАТ "ВІПОЛ", 2011. 248 с.

4. Дотримання інформаційних прав і свобод українських громадян: нормативно-правове забезпечення і регулятивні важелі: аналітична записка. URL: http://www.niss.gov.ua/articles/231

5. Кравченко О.В. Психологічні особливості шахрайства: автореф. дис. …канд. психол. наук: спец. 19.00.06. Харків, 2005. 20 с.

6. Смаглюк О. В. Шахрайство за кримінальним кодексом України 2001 року: автореф. дис. …канд. юрид. наук: спец 19.00.06. Київ, 2004. 20 с.

7. Претекстинг (Pretexting). URL:https://encyclopedia.kaspersky.ru/glossary/pretexting

8. Святковська Ю.Ю. "М'яка сила" як інструмент зовнішньої політики держави. URL: file:///C:/Users/demyd/Downloads/199792-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0 %D1%82%D1%82%D1%96-446276-1-10-20200330.pdf

9. Жмура Ольга. "М'яка сила" як інструмент зовнішньої політики Франції. Травневі студії 2021: *Історія, міжнародні відносини, філософія.* С. 108-111.

10. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. С. 14-27, 41-82.

11. Гавловський В.Д., Гуцалюк М.В. та ін. Основні об'єкти посягань організованих злочинних об'єднань. Сфера використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Психологічні особливості організованих злочинних об'єднань: наук.-практ. посіб.; за ред. Я.Ю. Кондратьєва, С.Д. Максименка, Б.В. Романюка. Київ: Національна академія внутрішніх справ України, 2002, С. 82-98.

12. Internet crime report 2021. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~