УДК 316.776.23] : [327.5:355.01(477: 470) «2022/1024»]
DOI https://doi.org/10.32782/2710-4656/2025.1.2/47

Бондаренко І. С.
Запорізький національний університет

КОНТРОВЕРСІЙНІСТЬ КОНЦЕПТУ «СОЦІАЛЬНИЙ ІНЖИНІРИНГ» В УМОВАХ СУСПІЛЬНО-ПОЛІТИЧНИХ ПОТРЯСІНЬ

Стаття присвячена вивченню концепцій соціального інжинірингу у сучасному науковому та комунікаційному дискурсах. Авторка ставить перед собою завдання провести логічні паралелі між медійною репрезентацією соціального інжинірингу та науковими його потрактуваннями. Орієнтуючись на світову методологічну практику інтерпретації поняття «соціальний інжиніринг», визначено основні маркери застосування терміна у різних прикладних площинах. У процесі дослідження авторка доходить висновку, що сталими категоріями тлумачення концепту є конструкти «маніпуляція», «кіберзлочин», «інформаційно-психологічна операція». Виявлено, що своєрідним «тригером» актуалізації поняття «соціальний інжиніринг» у науковому та медійному дискурсах постає російсько-українська війна. Журналісти, експерти у галузі кібербезпеки, науковці намагаються віднайти пояснення агресії російської федерації проти цивілізованого світу в історичних реєстрах її пропагандистських наративів. У статті визначено, що цифровий ландшафт інформаційної війни росії проти України будується на комбінації атак кібернетичного інжинірингу (фішинг, претекстинг, бейтинг) та дезінформації – розповсюдженні фейків, дипфейків, чуток в офіційних медіа та соціальних мережах. У процесі аналізу авторка звертається до моніторингового звіту найбільшої у світі розвідувально-аналітичної компанії Recorded Future (США), у якому відображається комунікаційна стратегія і тактика росії у проведенні ІПСО в інформаційному просторі країн Західної Європи та США протягом 2024 року. Визначено, що в історичних вимірах науки соціальний інжиніринг постає прикладною галуззю знань, спрямованою на технологічне конструювання соцієтальної моделі суспільства.

Ключові слова: *дезінформація, соціальний інжиніринг, пропаганда, соціально-комунікаційна технологія, інформаційний злочин, кібернетична війна, інформаційно-психологічна операція, фейк, дипфейк.*

Постановка проблеми. Російсько-українська війна як вияв безпрецедентної руйнації фізичних та екзистенційних «налаштувань» світового порядку спровокувала появу у глобальному комунікаційному просторі численних сценаріїв розвитку цивілізації та дизайну міжнародної безпеки. У гущині логічних та емоційних оцінок відбулася своєрідна «реанімація» концепту «соціальний інжиніринг». Останній, семантично кумулюючи почасти негативний досвід соціального конструювання індустріальної доби, якнайкраще транслює намагання учених, експертів, журналістів, з одного боку, пояснити складні системи пошуку миру, з іншого – вказати на історично передбачувану режисуру російської федерації у творені авторитарного / імперського світоустрою.

Аналіз останніх досліджень і публікацій. Сучасна наука про соціальні комунікації перебуває у стадії накопичення того методологічного ресурсу, який уможливить усебічне вивчення ролі СК у модерних управлінських парадигмах. Поготів, що історія розвитку соціальних комунікацій демонструє найбільш ефективні способи, засоби й техніки інформаційного впливу, до яких на різних етапах цивілізаційного поступу вдаються суб'єкти соціального інжинірингу. До таких СКТ належать інформаційно-психологічні операції, пропаганда, реклама, паблік рилейшнз, спічрайтинг, іміджмейкінг, які стали предметом пильної уваги науковців лише у XX ст. Наразі людство оперує новими цифровими технологіями, які не лише впливають на процеси формування громадської думки, а й модифікують межі географічного й соціального простору, змінюють особистісний статус самої людини. Попри інтенсивний розвиток ІТ-технологій та їх впливу на світову економіку, індивід залишається комунікаційно вразливою й інформаційно незахищеною істотою. Про це красномовно засвідчили панічні настрої населення України під час пандемії COVID-19 і передусім у період російсько-української війни.

Наразі соціальний інжиніринг постає об'єктом досліджень відразу у декількох наукових галузях – політології (М. Афанасьєва, І. Гербут,

К. Покровська, Ю. Ніколенко), журналістикознавстві (В. Різун, О. Холод, Н. Кунанець, В. Пасічник, А. Федонюк), інформаційному безпекознавстві / «security engineering» (А. Росс, М. Гіттон, Ф. Салахдін, В. Пахомов, О. Бондаренко), соціології (Т. Біршенк, М. Дерксен, М. Бірюкова, Є. Суїменко, В. Подшивалкіна; діяльність української школи соціальної інженерії 20–30-х рр. ХХ ст. ми неодноразово аналізували у своїх публікаціях), правознавстві (А. Окесола, А. Подгорецький), кожна з яких доповнює методологічний арсенал вивчення складної тканини соціального проєктування. У деяких україномовних джерелах це поняття взагалі ототожнюють з феноменом так званого «соціального гіпнозу» [2].

В останні роки термін «соціальний інжиніринг» набув найбільшого поширення у прикладній сфері – захисті комп'ютерних мереж, програм і баз даних. Причому він позначає низку кіберзлочинів – шахрайських схем несанкціонованого доступу до конфіденційної інформації, поширення дезінформації та ведення ІПСО.

Сучасна світова наука поряд з апофатичним контекстом тлумачення поняття «соціальний інжиніринг» демонструє компліментарні його концепції, сконцентровані на динамічні процеси розвитку суспільства. Так, німецький дослідник Т. Біршенк декларує появу нового напряму антропології – «глобального соціального інжинірингу» («global social engineering»). Учений вважає, що у зв'язку з інтернаціоналізацією світу назріло питання міждисциплінарного вирішення складних питань міграції населення, прав людини, соціальної відповідальності. На його думку, поняття «розвиток» є фундаментальним конструктом у соціально-політичному лексиконі сучасної епохи. «Смисловою локацією цього терміна постають інтерфейси політичної практики, нормативної оцінки та наукового аналізу […]. Точкою збігу диференційних площин концепту «розвиток» є ідея соціального інжинірингу, яка сформувала європейську модерність: переконання, що соціальні зміни можна контролювати, застосовуючи критерії розуму», – зауважує автор [6, с. 203]. Т. Біршенк вважає глобальний соціальний інжиніринг більш широкою прикладною галуззю, ніж антропологія розвитку.

Постановка завдання. Метою статті є вивчення основних підходів до феномену соціального інжинірингу, які склалися у сучасній світовій науці. Одним із завдань дослідження постає визначення магістральної наукової галузі, у якій стабільно використовується поняття соціального інжинірингу. Водночас авторка ставить перед собою ціль здійснити проекцію медійного статусу соціального інжинірингу на формування методологічних параметрів його репрезентації у мультидисциплінарному дискурсі.

Виклад основного матеріалу. Негативний контекст терміна «соціальний інжиніринг», на жаль, є сталою практикою його використання у науковому та медійному дискурсах. Про це красномовно свідчить назва матеріалу «Гангстерський уряд: «антисоціальний інжиніринг» комуністичної доби як основа падіння Росії у варварство», опублікованого у польському виданні «New Eastern Europe» наприкінці 2023 р. Чеський публіцист Д. Джун небезпідставно зауважує: «Росія – початковий інстигатор і виконавець катастрофічного глобального комуністичного експерименту – десятиліттями заохочувала негативну, антисоціальну поведінку та карала усе людське. Унаслідок цього інстинктивний страх тотального зла закарбувався у кожному аспекті російського життя. Без гіпербол, «зло» стало настільки нормалізованим і стимульованим, що сьогодні росіяни можуть здійснювати щоденні терористичні атаки проти України – бомбардувати заповнені дітьми театри, вокзали, автобусні зупинки, школи та багатоквартирні будинки, не відчуваючи якого-небудь морального дискомфорту» [8]. Автор статті називає «спеціальну воєнну операцію» фінальною маніфестацією комуністичного антисоціального інжинірингу.

Щоправда авторська конотація не закріплює негативного значення над самим терміном «соціальний інжиніринг», автоматично спростовуючи традиційні характеристики концепту як деструктивного суспільного проєкту. Утім, ретельний аналіз англійськомовного цифрового середовища дає підстави констатувати пряму кореляцію поняття «соціальний інжиніринг» з путінським режимом, зосібна, з новими тактиками ведення кібервійни.

Відтак мусимо визнати, що сучасні потрактування терміна здебільшого стосуються означення групи інформаційних злочинів, що здійснюються у цифровому просторі. Варто згадати публікацію розміщену на сайті компанії-розробниці програмного забезпечення KnowBe4 (США) під назвою «Putin Uses Psychiatrists For Social Engineering Attacks Against Individual Targets». У ній, зокрема, зауважується: «російські агенти створюють психологічний портрет своєї жертви через її або його сліди у соціальних мережах. Згодом, використовуючи цю інформацію, росіяни продукують персоналізовані комп'ютерні віруси або здійснюють атаку на соціальні мережі, спеціально розроблену для конкретної людини» [10].

Примітно, що в останніх дослідженнях російських учених підтверджується факт застосування атак індивідуальної дії у глобальному цифровому просторі. Так, у колективній статті під красномовною назвою «The role of social engineering in modern Russian society» (2022) автори категоризують специфічний різновид соціального інжинірингу «special social engineering» [11], що базується на персоніфікованому (цілеспрямованому) управлінні (маніпулюванні) людиною з використанням її психологічного портрету (страх, цікавість, жадібність, зверхність, щедрість, жалість, довірливість, лінощі) та персональних даних, відображених в особистих профілях соціальних мереж. Автори зазначають: «усі методи соціального інжинірингу базуються на конкретних параметрах людського характеру та є передумовою для прийняття певних управлінських рішень. Спеціальний соціальний інжиніринг має особливий фокус: зловживає отриманою інформацією (зазвичай незаконними засобами) і перетворює вразливі місця людини (клієнта) на користь третіх осіб» [11]. Показово, що російські учені фахово описують увесь алгоритм репутаційного знищення персони – навіювання, зомбування, вербування, маніпулювання свідомістю, не нехтуючи використанням кримінального соціолекту: «Людей спочатку лякають, потім «розігрівають», потім роблять певні «навідні підказки», потім пропонують «допомогу». Усі шахрайські ланцюжки так званого «спеціального соціального інжинірингу» є блокованими» [11].

Про застосування російською федерацією атак соціального інжинірингу проти цифрового простору України йдеться на платформі Dark Reading – онлайнспільноті професіоналів у сфері кібербезпеки «The Cybersecurity Community». Автори Dark Reading засвідчують численні факти хакерських атак країни-агресора на вітчизняні об'єкти критичної інфраструктури, державні установи та військовослужбовців. Н. Едді в одному з матеріалів зауважує: «Кіберкомпанії зосереджені на шпигунстві, дезорганізації та соціальному інжинірингу з метою послабити українську оборону та посіяти розбрат, а також на спробах скомпрометувати персональні дані та проникнути в захищені канали зв'язку. Пов'язані з росією кібератори, зосібна, передові групи постійних загроз (APT), як-от Gamaredon, значно посилили атаки після вторгнення росії в Україну у 2022 р.» [7].

Дослідники зауважують, що російсько-українська війна кардинально вплинула на цифровий ландшафт і диджитальну екосистему світу. Водночас безпрецедентна за своїми масштабами збройна агресія рф зумовила модифікацію самого театру воєнних дій, що відразу розгортається у декількох площинах – фізичних (реальних) і цифрових (віртуальних): кібератаки / кібервійна та кінетична війна; IT, хмарні сервіси, телекомунікації; цифрова геополітика та соціальна резилентність.

За словами ізраїльського дослідника І. Авіва, «головне розуміння кібервійни полягає в тому, що кібератаки на цифрову інфраструктуру України були лише частково ефективними, незважаючи на масову участь груп кіберзлочинців, які впроваджували адаптивне знищення даних і DDoS-атаки. Успіх кіберзахисту став результатом підтримки України союзниками та впровадженні ефективної національної стратегії кібербезпеки» [3].

У сучасному медійному дискурсі виокремлюємо ще один семантичний аспект концепту «соціальний інжиніринг» – його співставлення з російськими кампаніями дезінформації. Показовою у цьому розрізі є публікація на сайті видання «Forbes» під заголовком «Social Engineering and the Disinformation Threat in Cybersecurity» (2023). Д. Балабан, автор матеріалу, називає дезінформацію «найбільш обговорюваною темою у світі» [4], що має суттєвий вплив на світову історію. Колумніст апелює до доленосних фактів новітньої політики: агітаційної кампанії Vote Leave щодо виходу Великої Британії з Європейського Союзу (провокативний напис на червоному автобусі, символі кампанії, містив неправдиву інформацію «Ми віддаємо €C 350 мільйонів фунтів стерлінгів на тиждень, давайте будемо фінансувати нашу NHS»). Водночас автор згадує «істеричні звинувачення Дональда Трампа у «фейкових новинах» [4], військову риторику Путіна та дезінформаційну операцію «Russosphere», спрямовану на африканські країни з метою просування антизахідної, прокремлівської ідеології. За його словами, саме «росія здавна була майстром дезінформації, ба більше, деякі експерти вважають сучасну її дефініцію запозиченим перекладом слова «дезінформація», яке походить від назви відділу чорної пропаганди КДБ» [4].

Поряд з експресивними оцінками російських практик дезінформування Д. Балабан наводить логічні пояснення численних способів психологічного впливу на суспільну свідомість. Автор вбачає прямий зв'язок соціального інжинірингу та дезінформації; остання постає інструментом у процесі несанкціонованого доступу до персональних даних. Журналіст-розслідувач наводить три основні типи дезінформації, що використовуються під час соціоінженерних атак: відсутність

контексту («missing context»), оманливе редагування («deceptive editing») та зловмисну трансформація («malicious transformation»). Техніка «відсутність контексту» реалізовується зазвичай у соціальних мережах шляхом поширення оманливої інформації або повідомлень, позбавлених важливих деталей (приміром, зловмисники публікують зображення з підписами, що не відповідають змісту). Сценарій «оманливого редагування» передбачає маніпулювання візуальними медіа (фотографії, відео, ілюстрації, інфографіка), що відображають справжні новини або події, водночас спотворюючи реальність через вибіркову зміну основних компонентів; так створюється альтернативне повідомлення. Категорія «зловмисна трансформація» базується на використанні штучного інтелекту (ШІ) та дипфейків. Злочинці використовують ці методи соціального інжинірингу як у фінансовій сфері, так і в політиці, зосібна, під час виборчих перегонів. Закцентуємо, у наукових публікаціях вивчається ще один різновид соціального інжинірингу – електоральний.

Перетин дезінформації та соціального інжинірингу став об'єктом мультимодального вивчення у статті К. Белла, А. Егона та П. Брокліна «Social Engineering in The Age of Disinformation: A Multimodal Approach to Detection and Preven», розміщеній на онлайнплатформі Elsevier у 2024 р. Автори публікації маркують соціальний інжиніринг як «маніпулювання людьми з метою розголошення конфіденційної інформації або виконання дій, які загрожують різним рівням безпеки» [5]. Дослідники зауважують, що в атаках соціального інжинірингу зазвичай використовуються психологічні тактики й обман – фішинг, претекстинг («pretexting»), цькування / заманювання («baiting») та дезінформація. Комплексно вони продукують середовище, у якому дезінформація й неправдиві наративи можуть значно підвищити ефективність атак соціального інжинірингу.

К. Белл, А. Егон та П. Броклін висувають тезу про те, що задіяння арсеналу дезінформації у соціоінженерних атаках ускладнює цифровий ландшафт впливу на індивіда / соціальну групу / суспільство / людство. «Поява соціальних медіа та інших каналів онлайнкомунікації створила середовище, в якому активно множаться кампанії з дезінформації. Це негативно впливає на громадську думку, підбурює розбрат і підриває довіру до державних інституцій. Дезінформаційні кампанії зазвичай використовують різні тактики для досягнення цілей, приміром, створення фейкових новин, поширення теорій змови та маніпулювання суспільними настроями. Ці операції можуть організовуватися державними та недержавними акторами з політичних, економічних або соціальних мотивів. Вплив дезінформації виходить за межі індивідуальної дезінформації, впливає на довіру суспільства та цілісність публічного дискурсу», – до таких висновків приходять учені [5].

По суті, дослідники говорять про досить просту схему конвергенції соціального інжинірингу та дезінформації, у якій остання створює необхідне соціально-психологічне тло та робить суб'єкт / об'єкт більш вразливим для ураження серією соціоінженерних атак: фішинг – претекстинг – бейтинг. Фішинг працює зазвичай через електронні листи, які надсилаються буцімто від офіційних джерел; зловмисники змушують людей надати особисту інформацію або перейти за посиланнями. Претекстинг – тип атаки, яка базується на заздалегідь створених зловмисником приводах, з метою заманити жертву в уразливу ситуацію й обманом змусити її надати конфіденційну інформацію. Бейтинг – соціоінженерна атака, що ґрунтується на урахуванні компроментуючих характеристик конкретної особи – жадібності, цікавості, страху, надмірній довірливості. Зловмисники заманюють потенційних жертв за допомогою фальшивих обіцянок або стимулів, приміром, безкоштовними завантаженнями книги, музики, фільму або цінними призами.

Дезінформаційні кампанії, які зазвичай розгортаються в інформаційному просторі соціальної групи / корпорації / суспільства, спрямовані на поширення неправдивої інформації з метою маніпулювання громадською думкою. Магістральними техніками впливу постають фейкові новини, неправдиві наративи, теорії змов, режисура контроверсійних парадигм, дипфейки.

Слід визнати, в умовах російсько-української війни цифровий простір став справжнім полігоном інформаційно-психологічного протиборства. Державні та незалежні аналітичні центри протидії дезінформації щодня фіксують численні інформаційно-психологічні операції (ІПСО) супротивника, розраховані на різні цільові авдиторії. Так, за даними Центру стратегічних комунікацій та інформаційної безпеки, 25 грудня 2024 р. Україна зазнала масованої комбінованої атаки на критичну інфраструктуру з боку рф, що супроводжувалася потужним інформаційним прикриттям – 1,94 тис. повідомлень (лише за одну добу) з традиційними фейковими новинами «про враження «військових об'єктів», «баз НАТО», а також заяви про «помсту» за удари українських безпілотників» [1].

ІПСО ворога працює з громадською думкою багатовекторно, відразу комбінуючи різні тематичні блоки – від фейків про законодавче зобов'язання жінок з ім'ям Тетяна змінити його на Горпина до «інсайдів» про рішення уряду щодо мобілізації юнаків віком від 18 років. Цілком зрозуміло, що такі дезінформаційні кампанії працюють на посилення панічних настроїв і соціальної напруги у суспільстві, підрив довіри до українських бойових підрозділів, ЗСУ, дискредитацію влади всередині країни та на міжнародній арені.

У листопаді 2024 р. Insikt Group – аналітичний підрозділ компанії Recorded Future, що спеціалізується на вивченні загроз у сфері кібербезпеки, оприлюднив дослідження щодо комбінованої інформаційно-психологічної операції «Подрыв» / «Undercut» проти України, виконавцем якої постає російське Агентство соціального проєктування (рос. «Агенство социального проектирования»; на сайті Головного управління розвідки України вказано про санкційні юрисдикції США та Великобританії проти цієї організації). Insikt Group повідомила про використання рф штучного інтелекту (дипфейків) і тактик імперсональної атаки соціального інжинірингу з метою послаблення підтримки України державами Західної Європи. Зауважимо, «impersonation tactics» – цілеспрямована фішингова атака викрадення конфіденційних даних, за якої зловмисник видає себе за іншого. У моніторинговому звіті Insikt Group вказано: «Операція «Undercut» є частиною ширшої стратегії Росії, спрямованої на дестабілізацію західних альянсів і зображення української влади як неефективної та корумпованої. Орієнтуючись на аудиторію у Європі та США, «Агенство социального проектирования» прагне посилити антиукраїнські настрої, сподіваючись зменшити потік західної військової допомоги Україні» [9, с. 1].

Ключовими наративами ІПСО «Подрыв» / «Undercut» стали відразу декілька тез, які, транслюючи, здавалося б, різні суспільно-політичні теми, формували єдину стратегію – знищення репутації України на світовій арені й унеможливлення військової підтримки країнами Західної Європи і США. Головний наратив ІПСО «Подрыв» / «Undercut» – «корумпованість українських посадовців та недоцільність західної військової допомоги». Російська дезінформаційна кампанія звинувачувала / звинувачує українських лідерів у корупції, зловживанні іноземною допомогою, яка буцімто спрямовується для забезпечення розкішного способу життя. Поширюваний серед європейської авдиторії наратив має на меті підірвати громадську підтримку подальшої фінансової та військової допомоги Україні.

Резонування конфлікту між Ізраїлем і Газою – ще один компонент ІПСО «Подрыв» / «Undercut». Фахівці Insikt Group зауважують: «SDA намагається маніпулювати громадською думкою щодо конфлікту між Ізраїлем і Газою, звинувачуючи Захід в упередженості й махінації розвідувальними даними. Акцентуючи на суперечностях у світовій політиці, операція «Undercut» штучно створює подразнюючі чинники та поглиблює розкол. Це послаблює західні альянси та відволікає увагу від російської агресії» [9, с. 12].

«Напруга всередині ЄС і вибори у США» – постійний наратив російських ІПСО 2024 р. Пропаганда ворога постійно посилює існуючу політичну напруженість всередині Європейського Союзу, підтримуючи ультраправі наративи і критикуючи лідерів ЄС. Окремою темою дезінформаційних меседжів стали вибори в США, у яких військова допомога Україні поставала зоною конфлікту американського суспільства. Представляючи майбутнє України як залежне від результатів виборів у США, російські ІПСО максимізують занепокоєння щодо політичної стабільності на Заході.

Водночас фахівці Recorded Future дійшли висновку, що в ході реалізації ІПСО «Undercut» використовувалися технології ШІ для обробки відео й зображень, більшість з яких імітували надійні медіаджерела. Закадровий голос, згенерований штучним інтелектом, і реалістичні зображення підсилювали антиукраїнські наративи. Використовуючи логотипи й позивні авторитетних масмедіа, «Агенство социального проектирования» підвищувало правдоподібність дезінформації, вводячи в оману авдиторію та підриваючи довіру до незалежних медіа. Загалом акаунти «Агенства социального проектирования» публікують вузькоспеціалізований контент на різних платформах під трендовими хештегами, аби охопити різну цільову авдиторію. У процесі моніторингу операції «Undercut» було виявлено низку відеороликів зі схожими наративними сценаріями, у яких тринадцять українських посадовців звинувачувалися у корупції, використанні іноземної військової допомоги та державного фінансування для придбання розкішних маєтків у Європі та Карибському басейні. Звичайно, вміст таких матеріалів варіювався залежно від регіону поширення, включаючи пости англійською, німецькою, французькою, польською та турецькою мовами.

Висновки. Наша стратегія вивчення формування концепту «соціальний інжиніринг» у сві-

товій науці і дискурсі соціальних комунікацій вказує на відсутність методологічної бази вказаного напряму. Ба більше, у сучасній філософії цей термін метафорично використовується на позначення суспільних експериментів низки тоталітарних країн XX–XXI ст. – нацистської Німеччини, СРСР, Італії, Китаю, Туреччини періоду правління молодотурків, путінської росії. Водночас західноєвропейські учені пов'язують вказаний конструкт з ефективними суспільно-економічними реформами, що відбулися у деяких державах напередодні або після Другої світової війни. Нами була визначена методологічна повторюваність актуалізації конструкту «соціальний інжиніринг» саме в період глобальних суспільно-політичних зрушень. Науковці звертаються до аналізу цього поняття, намагаючись пояснити й систематизувати складні технологічні трансформації світу. Наразі термін «соціальний інжиніринг» активно використовується у сфері кібернетичної безпеки, позначаючи комбіновані атаки на електронні бази даних, а також маніпулятивний вплив керованих інформаційно-психологічних операцій на масову свідомість суспільства. Водночас у сучасній науці концепт «соціальний інжиніринг» демонструє варіативність методологічних підходів, що може стати предметом подальших досліджень.

Список літератури:

1. Ракетний удар РФ по Україні на Різдво: інформаційна складова. Центр стратегічних комунікацій та інформаційної безпеки. URL : https://spravdi.gov.ua/raketnyj-udar-rf-po-ukrayini-na-rizdvo-informaczijna-skladova/ (дата звернення: 11.01.2025).

2. Сучасний гіпноз, або Соціальний інжиніринг. *На Урок: Освітній проєкт*. URL : https://naurok.com.ua/socialniy-inzhiniring-439081.html (дата звернення: 14.01.2025).

3. Aviv I. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*. 2023. Vol. 43. DOI : https://doi.org/10.1016/j.ijcip.2023.100637 (дата звернення: 08.01.2025).

4. Balaban D. Social Engineering and the Disinformation Threat in Cybersecurity. *Forbes*. 2023. Jun. 16. URL: https://www.forbes.com/sites/davidbalaban/2023/06/16/social-engineering-and-the-disinformation-threat-in-cybersecurity/ (дата звернення: 09.01.2025).

5. Bell C., Broklyn P., Egon A. Social Engineering in the Age of Disinformation: a Multimodal Approach to Detection and Prevent. Social Science Research Network. 2024. July, 12. DOI: http://dx.doi.org/10.2139/ssrn.4904945.

6. Bierschenk T. Anthropology and development in Germany. *Anthropologie & développement. Hors-Série*. 2021. № 4. Pp. 201–226. DOI : https://doi.org/10.4000/anthropodev.1247 (дата звернення: 08.01.2025).

7. Eddy N. Ukraine-Russia Cyber Battles Tip Over Into the Real World. *Dark Reading*. 2024. October, 3. URL: https://www.darkreading.com/cyberattacks-data-breaches/ukraine-russia-cyber-battles-tip-over-into-real-world (дата звернення: 08.01.2025).

8. Jun D. Gangster Government: the communist-era «anti-social engineering» at the heart of Russia's descent into barbarity. *New Eastern Europe*. 2023. October 31. URL: https://neweasterneurope.eu/2023/10/31/gangster-government-the-communist-era-anti-social-engineering-at-the-heart-of-russias-descent-into-barbarity (дата звернення: 07.01.2025).

9. "Operation Undercut" Shows Multifaceted Nature of SDA's Influence Operations. *THREAT ANALYSIS. Recorded Future.* 2024. November, 26. 24 p. URL : https://go.recordedfuture.com/hubfs/reports/TA-RU-2024-1126.pdf (дата звернення: 11.01.2025).

10. Putin Uses Psychiatrists For Social Engineering Attacks Against Individual Targets. *KnowBe4*. 2024. October 30. URL: https://blog.knowbe4.com/putin-uses-psychiatrists-for-social-engineering-attacks-against-individual-targets (дата звернення: 07.01.2025).

11. Stozhko K.P., Stozhko D.K., Shilovtsev A.V., Nekrasov S.N. and Makarova T.N. The role of social engineering in modern Russian society. *BIO Web Conf.: International Scientific and Practical Conference "From Modernization to Advanced Development: Ensuring Competitiveness and Scientific Leadership of the Agro-Industrial Complex" (IDSISA 2022)*. 2022. Vol. 58. DOI : https://doi.org/10.1051/bioconf/20225106008 (дата звернення: 08.01.2025).

Bondarenko I. S. THE CONTROVERSY OF THE CONCEPT OF SOCIAL ENGINEERING IN THE CONDITIONS OF SOCIO-POLITICAL CHANGES

The article is devoted to the study of the concepts of social engineering in modern scientific and communication discourses. The author aims to draw logical parallels between the media representation of social engineering and its scientific interpretations. Focusing on the global methodological practice of interpreting the concept

of social engineering, the author identifies the main markers of the term's application in various applied areas. In the course of the study, the author comes to the conclusion that the constructions manipulation, cybercrime, information and psychological operation are the stable categories of interpretation of the concept. It is found that the Russia-Ukraine war is a kind of trigger for the actualization of the concept of social engineering in scientific and media discourses. Journalists, cybersecurity experts, and scholars are trying to find an explanation for the Russian Federation's aggression against the civilized world in the historical records of its propaganda narratives. The article determines that the digital landscape of Russia's information war against Ukraine is based on a combination of cyber engineering attacks (phishing, pretexting, baiting) and disinformation – the spread of fakes, deepfake, rumors in official media and social networks. In the course of the analysis, the author refers to the monitoring report of the world's largest intelligence and analytical company Recorded Future (USA), which reflects Russia's communication strategy and tactics in conducting PSYOP in the information space of Western Europe and the United States in 2024. In the historical dimensions of science, social engineering appears as an applied field of knowledge aimed at the technological construction of a societal model of society.

Key words: *disinformation, social engineering, propaganda, social and communication technology, information crime, cyber warfare, information and psychological operation, fake, deepfake.*