УДК 007:004.056

[0000-0002-3121-4517] **Н. М. Баландіна**[1], *старший викладач кафедри кібербезпеки,*
e-mail: nataliabalandina2103@gmail.com
[0000-0002-8555-5712] **М. Д. Василенко**[1], *д.ф.-м.н., д.ю.н., професор,*
в.о. завідувача кафедри кібербезпеки,
e-mail: nvas08@ukr.net
[0000-0002-6082-981X] **В. М. Слатвінська**[1], *аспірантка кафедри господарського права та процесу,*
e-mail: slatvinskaya_valeriya@ukr.net
[0000-0002-0009-337X] **С. В. Сисоєнко**[2], *к.т.н., старший викладач кафедри*
інформаційної безпеки та комп'ютерної інженерії
e-mail: s.sysoienko@gmail.com
[1]Національний університет «Одеська юридична академія»
Фонтанська дорога, 23, м. Одеса, 65009, Україна
[2]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ПІДХІД ДО МОДЕЛЮВАННЯ ПОВЕДІНКОВИХ ПРОЯВІВ У СОЦІАЛЬНОМУ ІНЖИНІРИНГУ В ІНТЕРЕСАХ ЗАХИСТУ ІНФОРМАЦІЇ

Стаття покликана стимулювати інтерес до особливостей підходів до моделювання поведінки людини в інформаційному середовищі та соціальному інжинірингу з метою забезпечення безпеки інформації в інформаційному кіберсередовищі. Розглянуто проблеми побудови кількісної теорії людських систем. З огляду на те, що поведінка людини не піддається математичному моделюванню, жодна зі створених моделей не може бути застосована для здійснення поведінкового аналізу. Доведено потребу в новому методологічному підході до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу. Запропоновано синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

Ключові слова: *методологія, моделювання, інжиніринг, поведінка, захист інформації.*

Вступ. Інформатизація радикально змінила середовище суспільства, а зміни, що відбуваються, прямим чином стосуються людини та її місця в інформаційному світі. Людина змінюється відповідно до змін в інформаційно-технічних характеристиках суспільства, виступаючи суб'єктом інформаційної реальності, виходячи далеко за інформаційно-технічні параметри.

Інформатизація та інформаційне поле людського буття змінили поведінкові стандарти й ціннісні орієнтації особистості. Не викликає сумнівів, що перед тим, як почати якінебудь дії, необхідно провести певну роботу зі збирання та перероблення інформації, її осмислення й аналізу і, нарешті, відшукання найраціональнішого рішення. Для цього потрібна обробка великих обсягів інформації, що може виявитися не під силу людині без залучення спеціальних технічних засобів і знань. Від людини вимагається здатність до творчості, що збільшує попит на знання. Водночас в інформаційній небезпеці важливішим компонентом залишається саме людський чинник. Теоретична картина інформаційного суспільства поступово набуває зримих контурів: відбувається прогнозоване перетворення всього світового простору в єдину комп'ютеризовану й інформаційну спільноту людей та інформаційних машин, інформаційна діяльність яких викликає найбільше питань, тому що в результаті такої діяльності під загрозою опинилася сама людина, яка, на відміну від інших істот і технічних об'єктів, наділена розумом. Саме нові інформаційні технології відкривають перспективу для колосального посилення таких фундаментальних особливостей людини, як схильність до маніпуляції і переконання, когнітивні упередження, для їх застосування в не бачених раніше масштабах. Соціальна інженерія передбачає прояв непрофесіоналізму в екстремальних умовах використання та непрофесіоналізму персоналу для отримання доступу до інформації сторонніми особами. В сучасних умовах набули суттєвого розвитку інтелектуальні інформа-

DOI: 10.24025/2306-4412.4.2020.222064

ційні технології, на яких базується вирішення глобальної проблеми штучного інтелекту. Математичне моделювання фактично являє собою потужну методологію дослідження складних систем, включаючи і такі, на яких базуються й системи штучного інтелекту. Спираючись на можливості сучасних обчислювальних методів та інформаційних технологій, методологія забезпечує повніше й глибше дослідження об'єктів і процесів для отримання нових знань, які стають основою для забезпечення прийняття ефективних інноваційних рішень. На сьогодні існують певні типи моделей, які успішно застосовуються для розв'язання складних завдань у різних галузях людської діяльності. Однак водночас важко говорити про прояви поведінки людини, особливо в умовах соціального інжинірингу, і важко піддавати її математичному моделюванню. У зв'язку з цим постала необхідність у розробці нової методології побудови моделі людської поведінки у кіберсфері.

Аналіз останніх досліджень та публікацій. У статті [1] обговорено модель, коли визначається стан людини як системи з її характеристиками, правилами взаємодії підсистем і параметри, які визначають ступені спроможності для прийняття рішень. Це дає змогу змоделювати динаміку стану системи як результат взаємодії складових. Перевага методу полягає в тому, що зникає необхідність розв'язання складної системи рівнянь, замість цього розв'язок задається безпосередньо за допомогою предикатів. Особливості поведінки людини у стресових (екстремальних) ситуаціях завжди були у центрі уваги науковців. До сьогодні було виконано велику кількість емпіричних досліджень окремих аспектів стресу, складних ситуацій. Однак, попри поширеність виявлення стресу, багато аспектів залишаються недостатньо висвітленими. У роботі [2] проаналізовано реакції людини в умовах стресової ситуації та запропоновано сформувати окрему галузь «стресологію» як систему дослідження та управління стресами на виробництві. Встановлено, що на різних людей по-різному впливають подразники під час робочої зміни, оскільки не менш важливу роль відіграють зовнішні джерела стресу, тобто ті, що формуються поза межами виробництва, і суб'єктивне ставлення працівника до ситуації загалом. У праці [3] розглядаються прийоми, які застосовуються соціальними інженерами найбільш часто і успішно в спробах маніпулювання, йдеться, зокрема, про авторитетність, уміння розташувати до себе, взаємність, відповідальність, соціальну належність до авторизованих користувачів, обмежену кількість «безкоштовного сиру». У роботі [4] досліджуються підходи до поведінки соціального інженера, здатного витягувати контакти власника акаунта і відправляти шкідливий контент від його імені, користуючись репутацією та соціальними зв'язками, приписуваними викраденому акаунту. У [5] звернуто увагу на модель порушника інформаційної безпеки та циклічну модель забезпечення безпеки інформації. У [6] розглядається модель поведінки порушника, який здійснює несанкціонований доступ до будь-якої частини збереженої, оброблюваної та переданої інформації, яка потребує захисту. З огляду на те, що поведінка людини не піддається математичному моделюванню, нами вперше звернуто увагу на те, що є потреба в новому методологічному підході до побудови моделі поведінкових проявів у цифровому кіберсередовищі з метою захисту інформації в соціальному інжинірингу.

Метою статті є розробка методологічного підходу до побудови моделі поведінкових проявів у соціальному інжинірингу для захисту інформації.

Виклад основного матеріалу. Атаки соціальної інженерії являють собою значну загрозу кібербезпеці, піддаючи ризику окремих осіб та організації [7]. Соціальна інженерія використовує людську поведінку замість технічних заходів для дослідження систем, різних даних, речей, які можуть принести будь-яку користь [8].

Людська поведінка являє собою послідовність окремих дій, що мають на меті локальні цілі. А діяльність людей, як відомо, це сукупність їх окремих дій і рішень, що приймаються відповідно до цілей, які маються на меті. Внаслідок випадковості навколишнього середовища, випадковості дій людей та випадковості стану самих людей, всі їхні дії та діяльність мають імовірнісний характер. Тому математична теорія людських систем являє собою кількісне представлення дій та діяльності людей в умовах невизначеності.

Сферами застосування соціального інжинірингу є загальна дестабілізація роботи організації з метою зниження її впливу та можливістю подальшого повного руйнування організації: проникнення в мережу організації

DOI: 10.24025/2306-4412.4.2020.222064

для дестабілізації роботи основних вузлів мережі з якою-небудь метою; фінансові махінації в організаціях; фішинг та інші методи крадіжки паролів з метою доступу до персональних банківських даних; конкурентна розвідка: інформація про маркетингові плани організації; інформація про найбільш перспективних співробітників з метою їх подальшого «переманювання» до своєї організації; загальна інформація про організацію, її слабкі та сильні сторони з метою подальшого руйнування організації тим чи іншим способом; крадіжка клієнтських баз [9].

Загальновідомо, що «захист інформації – це комплекс заходів, проведених власником інформації, по огородженню своїх прав на володіння й розпорядження інформацією, створенню умов, що обмежують її поширення, що й виключають або істотно ускладнюють незаконний доступ до інформації з обмеженим доступом і її носіїв» [5]. Водночас досягти необхідного рівня захищеності можна тільки за рахунок певних принципів захисту інформації, до яких належать комплексне використання наявних методів і засобів захисту, безперервна реалізація заходів із захисту інформації, необхідність та достатність комплексу засобів і заходів, адекватність витрат на захист вартості можливої шкоди внаслідок реалізації загроз.

Традиційний підхід до захисту інформації передбачає застосування стандартних механізмів захисту: ідентифікацію та аутентифікацію, механізми обмеження доступу до інформації згідно з правами суб'єкта і криптографічні механізми [10]. Однак наразі слід переглянути наявний методологічний підхід.

Проблеми побудови кількісної теорії людських систем

Традиційні якісні методи управління суспільними процесами, що базуються на досвіді та інтуїції людей, потребують перегляду в бік більшого залучення кількісних методів, для розв'язання нагальних проблем сучасності. Це пов'язано з необхідністю прийняття швидких і адекватних рішень в умовах революційних змін, у житті суспільства, і, перш за все, в умовах глобалізації політики, економіки, проблем безпеки та комунікації між людьми.

Безвідносно того, в якій сфері діяльності людини приймаються зазначені рішення, центром усього цього процесу є деяка людська система (Human system). Це може бути індивід, група людей, колектив, організація і т.ін. Діяльність людських систем у будь-якій конкретній сфері зводиться до прагнення збільшення ймовірності її успіху, супроводжуючи все це мінімізацією необхідних ресурсів для її виконання.

Ця обставина створює необхідні передумови для побудови кількісної теорії людських систем, поведінка яких може бути описана фундаментальними законами абсолютно так само, як це робиться в теоретичній фізиці, математичній біології, математичній економіці та в інших галузях знань.

Вдалими прикладами побудови подібних кількісних теорій у соціальних і організаційних науках є кількісна соціодинаміка та динаміка систем. Головною метою досліджень обох цих наукових напрямів є залежності характеристик людських систем від часу, тобто, по суті, ці напрями сфокусовані на динамічній стороні поведінки людських систем.

Однак величезна кількість проблем, які пов'язані з діяльністю людських систем, не можуть бути представлені, описані та вирішені методами кількісної соціодинаміки (тобто статистичної фізики) або динаміки систем, оскільки ці проблеми інваріантні щодо часу.

Річ у тім, що суть реалізації будь-якої дії та діяльності людей – це знаходження компромісу між цілями й вартістю цієї діяльності, засобами виконання і тривалістю чергової дії в життєвому процесі, всілякими ризиками при її виконанні та якістю кінцевого результату.

Якщо ж параметри людей та параметри розв'язуваних ними завдань і проблем не залежать від часу або ця залежність слабка, то при дослідженні подібних завдань і проблем потреба у використанні динамічного підходу відпадає, бо варто робити статичні розрахунки. Зрозуміло, що життя людей – це послідовність дій, кожна з яких може характеризуватися величиною (або розміром, або масштабністю) W і труднощами виконання D.

Кожна дія людей характеризується також своєю сукупною складністю Cd, яка визначається її розміром і складністю за наступним виразом: $Cd = W \times D$ [11].

Люди, залежно від своїх здібностей та маючи різні рівні навичок і знань, можуть подолати складність дії Cd, частково або повністю, забезпечуючи водночас різні якості виконання.

Таким чином, люди, маючи продуктивність P (яка є відображенням їх навичок

DOI: 10.24025/2306-4412.4.2020.222064

і знань) і споживаючи зусилля *E,* можуть подолати деяку частину *Cs* складності *Cd,* яка визначається як $Cs = E \times P$.

Тобто, з одного боку, для забезпечення нормального перебігу життєвого процесу є потреба у діях людей, а з другого боку, тобто з боку людей, у вигляді відповіді на вимоги життя маємо їхні реальні дії, які є відображенням їх здібностей і вмінь.

Як було сказано вище, успішне виконання дій людьми має на увазі певний баланс, або рівновагу, між складністю дії *Cd* та здатністю людей *Cs* долати цю складність.

Найпростіший випадок зазначеного балансу – це рівність зазначених складнощів, тобто $Cs = Cd$, або $E \times P = W \times D$, що являє собою умову рівноваги життя і діяльності людей. Зусилля людей *E* визначається як [11]

$$E = N \times T,$$

де *N* – кількість людей, що беруть участь у дії (або діяльності), *T* – тривалість зусиль людей.

Таким чином, умова рівноваги діяльності людей набуде вигляду [11]

$$N \times T \times P = W \times D.$$

Сенс цієї рівності полягає в тому, що група людей, яка складається з *N* осіб, діючи з продуктивністю *P* протягом відрізка часу *T*, може здійснити дію, або діяльність, яка має величину *W* і труднощі *D*.

Це також означає, що, якщо розглядати діяльність людей як систему, то на високому рівні таку систему можна описати п’ятьма параметрами, або системними змінними *N, T, P, W і D*. Між цими параметрами, або системними змінними існують функціональні зв’язки фундаментального характеру. Наприклад, збільшення труднощі *D* деякої діяльності людей призводить до зменшення їх продуктивності *P*.

Також зменшення планової тривалості робіт *T* призводить до збільшення кількості виконавців *N*, що, в свою чергу, призводить до зменшення продуктивності людей *P* через збільшення часу контактів між людьми для комунікації і координації їх зусиль і т. д.

Зміна значення кожного із зазначених параметрів породжує ланцюжок нелінійних змін значень інших параметрів людської системи. Кожному набору чисельних значень зазначених параметрів відповідає певний стан системи, що просто означає, що умова рівноваги діяльності людей $N \times T \times P = W \times D$ являє собою типове рівняння стану (в сенсі відомих рівнянь стану у фізиці).

Чудовою особливістю цих рівнянь є те, що вони в неявному вигляді містять усі можливі функціональні зв’язки між параметрами відповідних систем (включаючи фізичні, біологічні та соціальні системи).

Для отримання функціональних зв’язків між параметрами досліджуваних систем, поряд з рівнянням стану, потрібні деякі додаткові умови у вигляді сталості значень частини параметрів або у вигляді інших обмежень.

Приклад практичного застосування – рівняння стану для планування діяльності заданої складності *Cd* (тобто для діяльності людей з $Cd = W \times D = Constant$).

З урахуванням цієї умови рівняння стану людської системи набуде вигляду

$$N \times T \times P = Cd = Constant$$ [11].

Таким чином, спільне рішення рівняння стану дає можливість вивести функціональні залежності між параметрами людської системи аналітичним шляхом.

Пошук оптимального методологічного підходу до захисту інформації в соціальному інжинірингу

Як відомо, «методологічні дослідницькі підходи» ґрунтуються на висновках світоглядних ідей, які в межах тієї чи іншої наукової парадигми визначають для науковця особливості виявлення, добору та систематизації досліджуваних фактів, а також їх інтерпретації й оцінки» [12].

Водночас реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, впровадження надійних механізмів захисту й забезпечення їх сталого функціонування та високої ефективності, провадження відповідних робіт тільки фахівцями високої кваліфікації в сфері захисту інформації [13].

Створення сучасних систем інформаційної безпеки на практиці може задовольнятися трьома формальними методами побудови моделей: кібернетичним підходом, системною динамікою і теоретично-множинним підходом [14]. Проте, на нашу думку, в умовах та інтересах захисту інформації відбувається певна взаємодія чинників впливу на отримання даних. Йдеться про виникнення нової багатоваріантності, що створює нову якість на новому рівні розвитку системи, що і реалізується

DOI: 10.24025/2306-4412.4.2020.222064

в інтересах захисту інформації. Водночас проблема невизначеності системи залишається. Однак принциповим залишається те, що відбувається синергія. Система характеризується синергійними процесами та має енергійну функцію.

Авторами детально розглядаються «синергія», «синергетика», «синтез», «синергетичний ефект» та синергетичний підхід у праві [15]. Вважаємо, що у кіберсфері під час процесу захисту даних можливо застосовувати комплексний підхід. Тож спробуємо сформулювати авторське бачення до методологічних підходів.

Пропонуємо застосувати *синергетично-криптографічний підхід* до побудови моделі в умовах соціального інжинірингу та захисту інформації. Свого часу в телекомунікаційних системах сформувався захист інформації, пов'язаний з криптологією, яка, в свою чергу, поділяється на два напрями: криптографію та криптоаналіз. Мета цих напрямів прямо протилежна. Якщо криптографія займається пошуком та дослідженнями математичних методів перетворення інформації, то криптоаналіз досліджує можливості розшифрування інформації без використання ключів. Криптографія включає такі напрями: симетричні криптосистеми, системи електронного підпису, криптосистеми з відкритим ключем та й, фактично, управління ключами. Реально криптографія дає можливість перетворювати інформацію таким чином, що після кодування її можна відновити тільки при наявності знань щодо ключа системи. Як інформація, що підлягає шифруванню та дешифруванню, розглядаються тексти, побудовані на деяких кінцевих множинах знаків, використаних для кодування інформації. Питання криптографічного розуміння про підходи моделювання та визначення їх особливостей виникли тому, що своїми можливостями їх можна розглядати як багатоваріантні.

Свого часу розробники глобальних комп'ютерних мереж, а також при створенні телекомунікаційних систем мали на увазі тільки технічний захист. Водночас не передбачалася багатоваріантність людського фактора. В той же час криптографічне розуміння, якщо не забезпечує запобігання людському фактору, то надає технічну реалізацію деяких ймовірностей щодо перетворень інформації таким чином, що її відновлення можливе лише за допомогою ключа, а сам процес відображається достатньо простою схемою (рисунок 1), на якій зображено відомі процеси шифрування і дешифрування даних. Однак у разі дії внутрішніх і зовнішніх факторів недостатньо одних криптографічних рішень, що й було спонуканням до створення та запровадження синергійно-криптографічного підходу до моделі поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації. Отже, в нашому випадку маємо справу з більш складними процесами, ніж ті, які були відомі раніше, звертаючи увагу на складність рішень, що пов'язано як з внутрішнім, так і зовнішнім людським фактором, який залишається до кінця не визначеним.

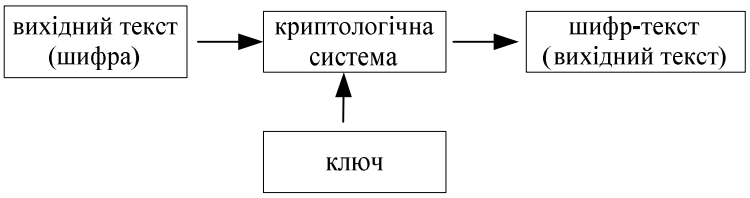

Рисунок 1 – Процес шифрування (дешифрування) даних [16]

Відзначимо ще раз результати нашої роботи щодо синергійної дії в зазначених системах, коли в результаті узгодженої спільної дії елементів виникає нова якість, яка не може бути досягнутою кожним окремим елементом [15]. У нашому контексті можна відзначити відому модель системи таємного зв'язку К. Шеннона, яка запропонована в його роботі «Теорія зв'язку в секретних системах», опублікованій у 1949 р. [16-17]. Прийнято вважати, що ця робота стала початком ери наукової криптографії. У цій роботі К. Шеннон, зокрема, розглядає поняття стійкості шифру в рамках відповідної моделі і вводить загальне поняття практичної стійкості шифрів. За К. Шенноном, криптографічна система є сі-

DOI: 10.24025/2306-4412.4.2020.222064

мейством обернених (рисунок 2) відображень безлічі можливих повідомлень у безліч криптограм. Кожне відображення T (k) є шифруванням. Вибір відображення проводиться за допомогою випадкового секретного параметра k, званого ключем. Ключ також дає змогу вибрати зворотне перетворення (розшифрування). Реально він використовується як параметр в обчисленнях при шифруванні і розшифруванні. Ключ обов'язково має бути доступним відправнику та одержувачу в необхідний момент. Така система секретного зв'язку має назву симетричної криптосистеми (симетрія користувачів щодо знання секрету). У цій системі питання про розподіл ключів фактично виноситься К. Шенноном за рамки моделі. Важливим моментом є модель противника, якому доступний для перехоплення шифр-текст і якому відомий алгоритм шифрування та його параметри, за винятком ключа (принцип відкритості, загальнодоступності системи).

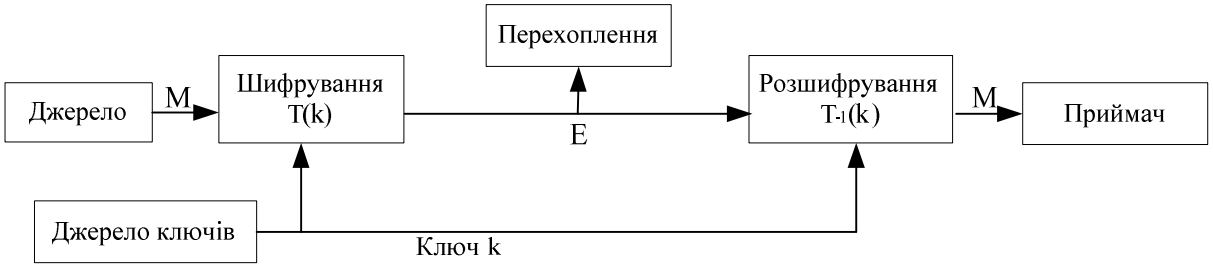

Рисунок 2 – Модель Шеннона секретного зв'язку [16]

Однак у рамках нашого дослідження ця модель може не спрацьовувати, а скоріше – зовсім не спрацює, бо за цей час сталося багато обмежень та з'явилися багатоваріантність і велика невизначеність, про які йшлося вище.

Крім того, принциповим є те, що функція захисту інформації покладена на звичайних користувачів мережі Internet. Підкреслимо, що захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних із тим, що інформація не є жорстко пов'язаною з носієм, може легко та швидко копіюватися і передаватися по каналах зв'язку [17].

Будь-які загрози витоку інформації – явища, тенденції та чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію інтересів власника даних та збереження цінності й достовірності інформації. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників. Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дають можливість вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних.

Поведінка порушників в інформаційному кіберсередовищі видозмінюється відповідно до рівня обізнаності щодо методів захисту інформації та залежить від поведінки власників інформації. Отже, відбувається взаємодія «порушників» (соціальних інженерів) та власників інформації – користувачів мережі Internet шляхом досягнення єдиної мети – отримання чи збереження інформації. Ця синергія відбувається за конкретних обставин та у певний час. В результаті відбувається поліпшення якісних показників методів захисту інформації.

На рисунку 3 структурно зображено розуміння синергійно-криптографічного підходу до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації.

DOI: 10.24025/2306-4412.4.2020.222064

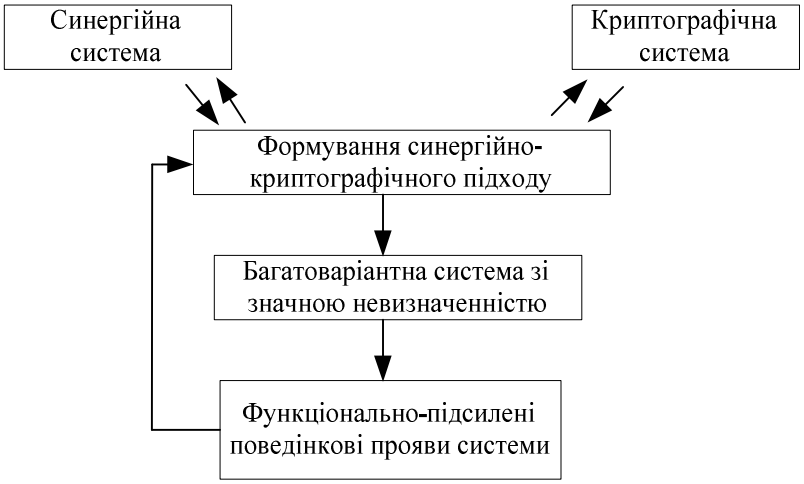

Рисунок 3 – Структурне відображення синергійно-криптографічного підходу до моделювання поведінкових проявів

Описати структурну побудову синергійно-криптографічного підходу можна наступним чином: в основі синергійної та криптографічної систем, які взаємовпливають на багатоваріантну систему зі значною невизначеністю, лежать функціонально-підсилені поведінкові прояви системи, які в сукупності приводять до формування синергійно-криптографічного ефекту та відповідного підходу. Водночас існують підсилювальні прояви системи на кінцевій стадії рішення з сильним зворотним зв'язком, що впливає на саму формуючу систему.

Таким чином, синергійно-криптографічний підхід до побудови моделі можна сформувати як складний, що має дві складові, одна з яких є багатоваріантною з невизначеності, друга – криптографічною, яка в умовах багатоваріантності неспроможна відображати кількісні характеристики при загальному посиленні системи з можливими збоями при захисті інформації. В результаті цього відбулося створення принципово нового підходу до розв'язування задач у системах соціального інжинірингу.

Висновки і перспективи подальшого розвитку. Досліджено кількісну теорію людських систем на прикладі систем кількісної соціодинаміки (динаміки систем) та виявлено проблеми при її побудові. Наукова новизна полягає в тому, що авторами вперше розроблено й обґрунтовано синергійно-криптографічний підхід для забезпечення моделювання поведінкових проявів у соціальному інжинірингу з метою вирішення задач захисту інформації.

Важливість отриманих результатів обумовлюється тим, що в умовах багатоваріантності, коли існують багатофакторні обмеження, виникає принципова невизначеність. Виникає складність у проведенні кількісного аналізу наявних методичних підходів. В умовах соціального інжинірингу поведінка людини не піддається математичному моделюванню. Представлений у роботі синергійно-криптографічний підхід дає можливість вивчати поведінку людини в соціальному інжинірингу з метою забезпечення безпеки інформації в інформаційному кіберсередовищі.

Перспективою подальших досліджень є проведення дослідження імовірнісної інтерпретації рівнянь стану людської системи та аналізу тривалості дій людей у соціальному інжинірингу в умовах захисту інформації. Крім того, доцільно провести аналіз ефективності застосування ймовірнісного підходу до обраної теми дослідження.

Список використаних джерел

[1] А. Л. Белкарян, и А. С. Акопов, "Моделирование поведения толпы на основе интеллектуальной динамики взаимодействующих агентов", *Бизнес-информатика*, № 1 (31), с. 69-77, 2015.

[2] Л. І. Мочурад, Н. І. Бойко, та М. В. Яцків, "Моделювання стресової ситуації людини в автоматизованих системах управління *технологічними* процесами", *Науковий вісник НЛТУ України*, т. 30, № 1, с. 152-157, 2020.
DOI: 10.36930/40300126

DOI: 10.24025/2306-4412.4.2020.222064

[3] Р. Чалдини, *Психология влияния*: учебник для вузов. Санкт-Петербург, Россия: Питер, 2008.

[4] A. Dalton et al. "Active defense against social engineering: The case for human language technology", in *Proc. First Int. Workshop on Social Threats in Online Conversations: Understanding and Management*, 2020, pp. 1-8.

[5] Г. М. Гулак, *Методологія захисту інформації. Аспекти кібербезпеки*: підручник. Київ, Україна: Вид-во НА СБ України, 2020.

[6] С. М. Сергеєв, "Модель поведінки порушника", на *XXXVII наук.-техн. конф. молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України*: зб. тез, (м. Київ, 15 трав. 2019 р.) / ІПМЕ ім. Г. Є. Пухова НАН України, 2019, с. 37-38.

[7] Adam Dalton, Alan Zemel, Amirreza Masoumzadeh et al., "Modeling social engineering risk using attitudes, actions, and intentions reflected in language use", in *Conf. FLAIRS-32*, FL, US Project: PANACEA, 2019, pp. 509-520. [Online]. Available: https://www.flairs-32.info/program#h.p_ngc7nAzybVbQ

[8] Neetu Bansla, Swati Kunwar, and Khushboo Gupta, "Social engineering: A technique for managing human behavior", *Journal of Information Technology and Sciences*, vol. 5, no. 1, pp. 18-22, 2019. DOI: 10.5281/zenodo.2580822

[9] М. В. Кузнецов, *Социальная инженерия и социальные хакеры*: учеб.-метод. пособие. Санкт-Петербург, Россия: БХВ-Петербург, 2010.

[10] О. В. Ямковий, та А. Б. Качинський, "Пошук аномалій в поведінці користування Інтернет-ресурсами за допомогою алгоритмів кластеризації машинного навчання", на *І наук.-практ. конф. Інформаційна безпека: сучасний стан, проблеми та перспективи*, (м. Київ, 20 верес. 2019 р.) / упоряд.: В. М. Фурашев, С. Ю. Петряєв, Нац. техн.. ун-т України "Київ. політехн. ін-т ім. Ігоря Сікорського". Київ: Політехніка, с. 69-74, 2019.

[11] П. Барсегян, *Елементи математичної теорії діяльності людських систем*, ч. 1. [Електронний ресурс]. Режим доступу: https://iarex.ru/insimgs/ d468ea43f597f6f.pdf

[12] Т. С. Перун, "Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні", дис.. канд.. юр. наук за спец. 12.00.07 "Адміністративне право і процес; фінансове право; інформаційне право", Нац. ун-т "Львівська політехніка", Львів, 2019.

[13] А. Дмитренко, та В. Мирошниченко, "Сутність потенційних та реальних загроз інформації", на *ІІІ Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів Захист інформації в інформаційно-комунікаційних системах*: зб. тез доп., (м. Львів, 28 листоп. 2019 р.). Львів, 2019, с. 4-6.

[14] Н. М. Баландіна, та М. Д. Василенко, "Деякі нотатки щодо математичних можливостей в моделюванні захисту інформації", на *ІІ Всеукр. наук.-практ. конф. Кібербезпека в сучасному світі* (м. Одеса, 20 листоп. 2020 р.) / за ред. О. В. Дикого; уклад.: Н. І. Логінова, В. Д. Бойко, та М. О. Флюнт. Одеса: Гельветика, 2020, с. 124-128.

[15] М. Д. Василенко, та В. М. Слатвінська, "Сила синергії у проявах правової науки: міждисциплінарне дослідження", *Наукові праці Національного університету "Одеська юридична академія"*, т. 24 / гол. ред. Ю. В. Цуркан-Сайфуліна; МОН України, НУ "ОЮА". Одеса: Гельветика, с. 18-26, 2019. DOI: 10.32837/npnuola.v24i0.650

[16] К. Шеннон, "Теория связи в секретных системах", в *Работы по теории информации и кибернетике.* Москва, Россия: Иностр. лит., 1963.

[17] *Введение в криптографию* / под общ. ред. В. В. Ященко, 3-е изд., доп. Москва, Россия: МЦНМО: "ЧеРо", 2000.

[18] О. В. Виноградов, "Актуальні питання захисту інформації в автоматизованих системах", на *Наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп., (м. Київ, 4 квіт. 2019 р.). [Електрон. вид.]. Київ: Нац. акад. СБУ, 2019, с. 286-287.

References

[1] A. L. Belkarian, and A. S. Akopov, "Modeling of crowd behavior based on intellectual dynamics of interacting agents", *Biznes-informatika*, no. 1 (31), pp. 69-77, 2015. [in Russian].

DOI: 10.24025/2306-4412.4.2020.222064

[2] L. I. Mochurad, N. I. Boyko, and M. V. Yatskiv, "Modelling of human stress situation in automated control systems of technological processes", *Naukovyi visnyk NLTU Ukrainy*, vol. 30, no. 1, pp. 152-157, 2020. DOI: 10.36930/ 40300126 [in Ukrainian].

[3] R. Cialdini, *Psychology of influence*: a textbook for universities. Saint Petersburg, Russia: Peter, 2008. [in Ukrainian].

[4] A. Dalton et al. "Active defense against social engineering: The case for human language technology", in *Proc. First Int. Workshop on Social Threats in Online Conversations: Understanding and Management*, 2020, pp. 1-8.

[5] G. M. Gulak, *Methodology of information protection. Aspects of cybersecurity*: a textbook. Kyiv, Ukraine: Vyd-vo NA SB Ukrainy, 2020. [in Ukrainian].

[6] S. M. Sergeev, "The model of violator's behavior", in *XXXVII Sci. and Tech. Conf. of young scientists and specialists of H. Ye. Pukhov Institute of modeling problems in the energy sector of the National Academy of Sciences of Ukraine*: abstracts, (Kyiv, May 15, 2019), 2019, pp. 37-38. [in Ukrainian].

[7] Adam Dalton, Alan Zemel, Amirreza Masoumzadeh et al., "Modeling social engineering risk using attitudes, actions, and intentions reflected in language use", in *Conf. FLAIRS-32*, FL, US Project: PANACEA, 2019, pp. 509-520. [Online]. Available: https://www.flairs-32.info/program#h.p_ngc7nAzybVbQ

[8] Neetu Bansla, Swati Kunwar, and Khushboo Gupta, "Social engineering: A technique for managing human behavior", *Journal of Information Technology and Sciences*, vol. 5, no. 1, pp. 18-22, 2019. DOI: 10.5281/zenodo.2580822

[9] M. V. Kuznetsov, *Social engineering and social hackers*: a textbook. Saint Petersburg, Russia: BKhV-Peterburg, 2010. [in Ukrainian].

[10] O. V. Yamkovy, and A. B. Kaczynski, "The search for anomalies in the behavior of Internet resources use with the help of machine learning clustering algorithms", in *First Sci. and Pract. Conf. Information Security: Current State, Problems and Prospects*, (Kyiv, Sept. 20, 2019) / V. M. Furashev, and S. Yu. Petryaev, Comp., National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". Kyiv: Politekhnika, 2019, pp. 69-74. [in Ukrainian].

[11] P. Barseghyan, *Elements of mathematical theory of human systems activities*, part 1. [Online] Available: https://iarex.ru/insimgs/d468ea43f597f6f.pdf.

[12] T. S. Perun, "Administrative and legal mechanism for ensuring information security in Ukraine", Ph.D. thesis in specialty 12.00.07 "Administrative law and process; Financial Law; Information Law", National University "Lviv Polytechnic", Lviv, 2019. [in Ukrainian].

[13] A. Dmytrenko, and V. Miroshnichenko, "The essence of potential and real threats to information", in *III All-Ukr. Sci. and Pract. Conf. of young scientists, students and cadets Information protection in information and communication systems*: abstracts, (Lviv, Nov. 28, 2019). Lviv, 2019, pp. 4-6. [in Ukrainian].

[14] N. M. Balandina, and M. D. Vasilenko, "Some notes on mathematical possibilities in information security modeling", in *II All-Ukr. Sci. and Pract. Conf. Cybersecurity in the modern world* (Odessa, Nov. 20, 2020) / A. V. Dykyy, Ed.; N. I. Loginova, V. D. Boyko, and M. O. Flunt, Comp. Odessa: Helvetika, 2020, pp. 124-128. [in Ukrainian].

[15] M. D. Vasilenko, and V. M. Slatvinska, "The power of synergy in the manifestations of legal science: An interdisciplinary study", *Naukovi pratsi Natsionalnoho universytetu "Odeska yurydychna akademiia"*, vol. 24 / Yu. V. Tsurkan-Sayfulina, Chief Ed.; Ministry of education and science of Ukraine, NU "UIA". Odessa: Helvetika, pp. 18-26, 2019. DOI: 10.32837/npnuola.v24i0.650 [in Ukrainian].

[16] K. Shannon, "The theory of communication in secret systems", in *Works on the theory of information and cybernetics*, Moscow, Russia: Inostr. lit., 1963. [in Russian].

[17] *Introduction to Cryptography* / under the general editorship of V. V. Yashchenko, 3rd ed., add. Moscow, Russia: MTsNMO: "CheRo", 2000. [in Russian].

[18] O. V. Vynohradov, "Actual issues of information protection in automated systems", in *Sci. and Pract. Conf. Actual problems of information security in automated systems*: abstracts, (Kyiv, Apr. 4, 2019). [Online]. Kyiv: Nats. akad. SBU, 2019, pp. 286-287. [in Ukrainian].

DOI: 10.24025/2306-4412.4.2020.222064

N. M. Balandina[1], *senior lecturer of the department of cybersecurity,*
e-mail: nataliabalandina2103@gmail.com
M. D. Vasilenko[1], *Dr.Phys.-Math.Sc., Doctor of Law, professor,*
acting head of the department of cybersecurity,
e-mail: nvas08@ukr.net
V. M. Slatvinska[1], *postgraduate student of the department of economic law and process,*
e-mail: slatvinskaya_valeriya@ukr.net
S. V. Sysoienko[2], *PhD, senior lecturer of the department of information security and computer engineering*
e-mail: s.sysoienko@gmail.com
[1]National university «Odessa Law Academy»
Fontanskaya doroga, 23, Odessa, 65009, Ukraine
[2]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

APPROACH TO MODELING OF BEHAVIORAL MANIFESTATIONS IN SOCIAL ENGINEERING IN THE INTERESTS OF INFORMATION PROTECTION

The article is devoted to the peculiarities of approaches to modeling of human behavior in the information environment and social engineering to ensure information security in the information cyber environment.

The meanings of the concepts "mathematical theory of human systems", "human activities" and "information protection" are considered. The areas of application of social engineering in the process of information protection are clarified. The attention is drawn to the existing traditional approach to ensuring the security of data storage in the information cyber environment.

Furthermore, the problems of constructing a quantitative theory of human systems are considered. It is proved that since human behavior is not amenable to mathematical modeling, none of the created models can be used for behavioral analysis.

Moreover, we emphasize that the authors for the first time have drawn attention to the fact that there is a need for a new methodological approach to building a model of human behavior in the digital sphere aimed at protecting information in social engineering.

A synergistic and cryptographic approach to constructing a model of behavioral manifestations in the context of social engineering and information security interests is proposed. The essence of the authors' methodological approach is manifested in the fact that as a result of the synergistic interaction of "violators" (social engineers) and information owners – internet users, aimed at achieving a single goal, the possession of information that occurs under specific circumstances and at a certain time, the quality indicators of information protection methods improve.

Finally, it is emphasized that to study human behavior in social engineering for further information protection, it is possible only by changing the methodological approach.

Keywords: *methodology, modeling, engineering, behavior, information protection.*

Стаття надійшла 20.11.2020
Прийнято 16.12.2020

DOI: 10.24025/2306-4412.4.2020.222064