УДК 519.81

ІНФОРМАЦІЙНА БЕЗПЕКА РЕФЛЕКСИВНИХ ІНДИВІДІВ

Х. Р. Чудо[1, а], С. А. Смирнов[1, б]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут*

Анотація

В роботі розглянуто основні поняття рефлексивного аналізу, інформаційної безпеки особистості та інформаційних операцій. Наведено класифікації рефлексивних індивідів та надано характеристику відповідних типів, описано стандартні сценарії проведення спеціальних інформаційних операцій; наведено основні методи протидії деструктивному інформаційному впливу; проведено моделювання власних сценаріїв за допомогою рефлексивного аналізу та визначено їх ефективність.

Ключові слова: рефлексивний аналіз, інформаційна безпека особистості, інформаційні операції, етичний статус

Вступ

Інформаційні операції не є новим явищем, вони практикувались принаймні з перших часів появи писемності. Найвідомішим прикладом і доказом цього є «Трактат про військове мистецтво» датований приблизно V ст. до н.е. Однак у ролі основних засобів військово-політичного протистояння вони постають саме у XX сторіччі, внаслідок глобалізації, значного розвитку інформаційних технологій, збільшення ролі ЗМІ. Нині СІО є одним із найбільш ефективних засобів досягнення зовнішніх та внутрішніх політичних цілей як у воєнний, так і у мирний час.

1. Класифікація рефлексивних індивідів

Основні поняття рефлексивного аналізу

Рефлексія – це здатність осмислювати себе, свої вчинки, бути «спостерігачем», з метою аналізу вчинків своїх, або особи, з якою ведеться комунікація.

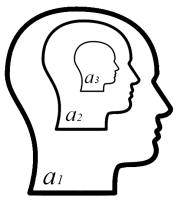

Рис. 1. Схема рефлексії індивіда

Основним об'єктом дослідження у рефлексивному аналізі є індивід, який має намір здійснити вибір, при цьому, цей індивід та усі рівні рефлексії аналізуються з боку незалежного спостерігача, який має об'єктивне бачення ситуації та може дати об'єктивну оцінку усім рівням рефлексії цього індивіда. Вибір при цьому є біполярним – добро (1) чи зло (0) [1]. Різним відношенням між добром та злом відповідають логічні операції додавання, множення та заперечення.

На рис. 1 змінні a_1, a_2, a_3 визначені на множині булевих елементів, де змінна

a_1 позначає тиск зовнішнього світу,

a_2 – оцінку індивідом цього тиску,

a_3 – інтенції індивіда, оцінку власних намірів.

За моделі рефлексії першого рангу, суб'єкт не усвідомлює себе, тому прийняття рішень залежить лише від тиску зовнішнього світу a_1:

$$\Phi(a_1) = \begin{cases} a_1, \\ \overline{a_1} \end{cases} \tag{1}$$

За сформованого образу себе у суб'єкта, отримаємо функцію для рефлексії індивіда другого рангу

$$\Phi(a_1, a_2) = a_2 \to a_1 = a_1 \vee \overline{a_2} = a_1^{a_2} \tag{2}$$

Найчастіше використовується модель третього рангу рефлексії, яка включає наміри індивіда:

$$\Phi(a_1, \Phi(a_2, a_3)) = \\ = (a_3 \to a_2) \to a_1 = a_1 \vee \overline{a_2} \wedge a_3 = a_1^{a_2^{a_3}} \tag{3}$$

Оскільки індивіди не існують ізольовано, необхідно розглянути схему взаємодії між двома рефлексивними суб'єктами з точки зору одного з них [2].

$$\Phi(A, B) = A^{A^{A*B} * B^{A*B}}, \tag{4}$$

де $A \in \{a, \overline{a}\}$, $B \in \{b, \overline{b}\}$,

$*$ – довільний тип відносин.

Взаємодія між індивідами відбувається за двома типами:

- конфронтація $(+)$
- компроміс $(\times)$

Етичний статус

Етичний статус індивіда – це характеристика, яка відображає частоту вибору позитивного полюсу ін-

[а] chudochristina@gmail.com
[б] s.smirnov@kpi.ua

Табл. 1. Типи індивідів за саморефлексією

Тип	Простак	Прагматик	Скептик	Мудрець
Форм.	$a^{\overline{a}^{\overline{a}}}$	a^{a^a}	$a^{\overline{a}^a}$	$a^{a^{\overline{a}}}$
a=0	1	1	1	1
a=1	0	0	0	1
Етичний статус	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1

Табл. 2. Типи індивідів за видом взаємодії

Вхідні значення		Тип взаємодії			
		Герой	Обиватель	Праведник	Лицемір
a	b	$a^{a^{a\times b}b}$	$a^{a^{a+b}+b}$	$a^{a^{a+b}\times b}$	$a^{a^{a\times b}+b}$
0	0	1	0	1	0
0	1	0	0	1	0
1	0	1	1	1	1
1	1	1	1	1	1
Етичний статус		$\frac{1}{2}$	1	$\frac{1}{2}$	

дивідом, тобто ступінь його спротиву спокусам зовнішнього тиску, за рівної ймовірності вхідних сигналів $\frac{1}{2}$ він визначається у межах від $\frac{1}{2}$ до 1. Він тісно пов'язаний з класифікацією індивідів та використовується для розрахунку ефективності змодельованих атак на інформаційну безпеку рефлексивного індивіда.

Класифікація індивідів

В рефлексивному аналізі виокремлюють по 4 типи індивідів за саморефлексією, відповідно до їх схильності піддавати сумніву образ себе й навколишнього світу, та типом взаємодії. Їх характеристики можна навести як вербально, так і формалізовано (таблиця 1,2).

Опис типів за саморефлексією:

- Прагматик – має коректний образ себе і не має сумнівів щодо цієї оцінки
- Скептик – має некоректний образ себе і сумніви щодо цієї оцінки
- Простак – має некоректний образ себе і не має сумнівів щодо цієї оцінки
- Мудрець – має коректний образ себе і сумніви щодо цієї оцінки

Як видно з таблиці 1, найвищим етичним статусом володіє тип Мудрець. Це явище пояснюється наявністю сумнівів у самооцінці суб'єкта, адже неправильно оцінивши вплив світу індивід помилково може обрати негативний полюс.

Відносно класифікації за видом взаємодії працює принцип максимуму етичного статусу образу себе. Тобто якщо у випадку, якщо індивід має змогу обирати вид взаємодії, він прагне максимізувати етичний статус образу себе. У таблиці 2 обчислено етичний статус кожного типу, найвищий з них має Праведник.

Комбінація цих двох класифікацій дозволяє більш детально змоделювати атаки на індивідів та обчислити їх ефективність.

2. Інформаційна безпека особистості

Інформаційна безпека особистості – це стан захищеності людської психіки і свідомості від деструктивних інформаційних впливів, спричинених маніпулюванням свідомістю, дезінформацією, підбурювання до завдання собі шкоди тощо [3]. Цей стан захищеності надає людині можливість сформувати й належно використовувати систему адекватного сприйняття реальності й самої себе, що в подальшому стає основою для подальшої соціалізації та благополуччя людини, в тому числі й цифрового, її цілісності як активної соціальної одиниці та наявності можливостей для саморозвитку в процесі комунікації з оточуючим світом.

У Законі України «Про національну безпеку» визначено, що забезпечення інформаційної безпеки є одним з фундаментальних національних інтересів України [4]. Оскільки людина, її права та свободи є головною цінністю будь-якої держави, особливо актуальним є питання забезпечення інформаційної безпеки особистості як невід'ємної частини національної безпеки.

2.1. Інформаційні операції

До переліку актуальних загроз національним інтересам і національній безпеці України в інформаційній сфері, визначених у Доктрині інформаційної безпеки України [5], входить проведення державою-агресором спеціальних інформаційних операцій різних спрямувань.

Табл. 3. Результати моделювання для жертви-Прагматика

	Тип B за саморефлексією			
Тип взаємодії	Простак	Скептик	Прагматик	Мудрець
Обиватель	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Герой	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Лицемір	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Праведник	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$

Табл. 4. Результати моделювання для жертви-Мудреця

	Тип B за саморефлексією			
Тип взаємодії	Простак	Скептик	Прагматик	Мудрець
Обиватель	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Герой	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$
Лицемір	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Праведник	1	1	1	1

Сутність спеціальних інформаційних операцій (СІО) полягає у проведенні спланованих дій в інформаційній сфері шляхом впливу на свідомість визначеної ворожої, дружньої або нейтральної аудиторії, її поведінку за допомогою використання організованої інформації та технологій для досягнення поставлених цілей.

Литвиненко О.В. виокремлює три основні типи інформаційних операцій за спрямуванням [6]:

- спрямовані проти суб'єктів, які ухвалюють рішення;
- спрямовані на компрометацію, завдання шкоди опонентам;
- спрямовані на політичну або економічну дестабілізацію.

У дослідженні феномену інформаційних операцій доволі часто використовують сценарний підхід, будь-який з сценаріїв СІО можна описати наступними етапами:

1) Етап планування.
   На цьому етапі відбувається оцінка доцільності здійснення операції, постановка завдань та цілей, визначення цільової авдиторії і формування у складі об'єкта впливу «п'ятої колони» – групи підтримки, вивчення настроїв в урядових колах, громадських політичних групах, широких народних масах, їх ставлення до внутрішнього стану країни.
2) Інформаційний привід.
   Вибір (або штучне створення) важливої події, яку можна використати з метою пропаганди або інформаційної операції.
3) Просування інформаційного приводу.
   Використання інформаційного приводу задля досягнень поставлених цілей, тобто по факту сама пропагандистська кампанія.
4) Етап закріплення.
   Плавний вихід з пропагандистської кампанії або ІО.

2.2. Методи проведення інформаційних операцій

Вплив СІО є найбільш ефективним у тій сфері, в якій жертва не має професійних знань, тому сприйняття поширеного зацікавленою стороною міфу викликає емоції, що базуються на ілюзії причетності людини до подій і це посилює деструктивність подібного впливу. У дослідженні для Ради Європи, дослідники Клер Уордл та Хосейн Дарахшан виокремили три групи, які можуть охарактеризувати деструктивну інформацію:

- дезінформація (disinformation) – неправдива або свідомо створена для заподіяння шкоди людині, соціальній групі, організації чи країні інформація;
- неправдива інформація (misinformation) – помилкова, але створена без наміру завдати шкоди, інформація;
- спотворена інформація (malinformation) – інформація, що ґрунтується на реальних фактах, використовується для заподіяння шкоди особі, організації або країні [7].

Загалом такі операції здійснюються шляхом розповсюдження інформаційного приводу наступними методами:

- дезінформування;
- легендування;
- дискредитація;
- пропаганда;
- маніпуляція;
- фейк;
- психологічний тиск;
- відволікання уваги;
- диверсифікація суспільної свідомості.

2.3. Методи протидії

Заходи протидії поширенню деструктивної інформації можна поділити наступним чином [8]:

- Організаційно-інституційні
  Здійснюються офіційними структурами різного рівня (міжнародними, національними, регіональними тощо) та окремими інституціями медіапростору. Цей напрям полягає у тому, що зацікавлені учасники медіапростору активно вживають спеціальних заходів щодо спростування дезінформації та убезпечення від неї на майбутнє.
- Правові
  Здійснюються на законодавчому рівні.
- Просвітницько-виховні.

З метою реалізації правових заходів протидії деструктивному інформаційному впливу, для забезпечення національних інтересів України в інформаційній сфері, було створено Центр протидії дезінформації при РНБО України та Центр стратегічних комунікацій та інформаційної безпеки при МКІП.

3. Моделювання атак

3.1. Опис використаної моделі

Моделювання атак на інформаційну безпеку особистості побудоване спираючись на класифікації рефлексивних суб'єктів за саморефлексією та видом взаємодії. Ролі рефлексивнх індивідів у моделі наступні: A – жертва, а B – нападаючий, ситуація розглядається з точки зору жертви. Обчислення проводяться за формулою, заснованій на (4):

$$\Phi(A,B) = a_1^{a_2^{a_3 * b_3} * b_2^{a_2 * b_2}}, \qquad (5)$$

де $A = \langle a_1, a_2, a_3 \rangle$, $B = \langle b_1, b_2, b_3 \rangle$.

У формулі (5) на місце $*$ підставляється вид взаємодії відповідно до обраного типу індивіда з класифікації за видом взаємодії, вектори A та B заповнюються відповідно до обраного типу за саморефлексією. З точки зору суб'єкта B, образ та образ образу ситуації буде коректним, а параметри точки зору суб'єкта A та його сприйняття взаємодії будуть змінюватися. Ефективність для кожної моделі розраховано методом обчислення етичного статусу атаки.

3.2. Результати моделювання

Результати проведеного моделювання для кожного типу суб'єкта-жертви наведені в таблицях 3, 4.

Етичний статус Скептика і Простака рівний $\frac{1}{2}$, незалежно від типу взаємодії та образу нападника. Таким чином запорукою ефективності атаки є тиск зовнішнього світу у бік негативного полюсу ($a_1 = 0$).

Зі значень етичного статусу у таблиці 3 видно, що найкращим типом взаємодії для жертви-Прагматика є Праведник, адже він сприяє підвищенню етичного статусу до $\frac{3}{4}$, в той час як в решті випадків він рівний $\frac{1}{2}$. Успішність атаки досягається при зовнішньому негативному впливові, однак для більшої ефективності підійдуть типи взаємовідносин Герой, Лицемір або Обиватель, адже у випадку типу взаємодії Праведник її ефективність падає до 25%.

З наведених у таблиці 4 обчислень можна зробити висновок, що ефективність атак на Мудреця є значно нижчою за решту типів, рівною 31, 25%. За будь-якого образу атакуючого, при взаємодії за типом Праведник, Мудрець завжди обиратиме добро, тобто матиме етичний статус рівний 1. За взаємодії ж по типу Герой, він матиме етичний статус $\frac{3}{4}$, тобто успішність атаки всього 25%. З цієї причини для успішного проведення атаки, необхідно діяти за типами Обиватель або Лицемір, аби досягти етичного статусу в $\frac{1}{2}$.

Висновки

Отже, в роботі було розглянуто основні поняття та категорії рефлексивного аналізу, які необхідні для досягнення поставлених задач. Наведено категоризацію основних типів індивідів за видом саморефлексії та взаємодії з партнером. У ході розгляду теоретичних основ інформаційної безпеки особистості було виділено її важливість в аспекті національної безпеки України. Проаналізовано класифікацію, типові сценарії та методи проведення спеціальних інформаційних операцій як основних загроз інформаційній безпеці особистості та наведено основні напрями протидії шкідливому інформаційному впливу у ході інформаційно-психологічних операцій. Змодельовані атаки на Мудреця та Прагматика показують зв'язок між зниженням ефективності атаки та наявністю у рефлексивного суб'єкта сумнівів щодо образу ситуації, намірів суб'єкта взаємодії та її характеру. У випадку атаки на Прагматика, її ефективність буде нижчою за атаки на типи Скептик та Простак, оскільки його етичний статус за взаємодії по типу Праведник буде рівним $\frac{3}{4}$, а у решті випадків – $\frac{1}{2}$. З цього випливає, що для успіху операції, спрямованої на Прагматика, необхідно забезпечити негативний тиск зовнішнього світу на жертву та конфлікт у взаємодії.

Перелік використаних джерел

1. Лефевр В. А. Алгебра совести. — М. : Когито-Центр, 2003.
2. Филимонов В. А. Алгебра логики и совести. — Издательство Омского государственного института сервиса, 2006.
3. Богуш В., Юдін О. Інформаційна безпека держави. — К. : Консум, 2005.
4. Про національну безпеку України. — 2018.
5. Про Доктрину інформаційної безпеки України. — 2016.
6. Литвиненко О. В. Інформаційні впливи та операції. — К. : Національний інститут стратегічних досліджень, 2003.
7. C. Wardle, D. Hossein. Information disorder: Toward an interdisciplinary framework for research and policymaking. — 2017.
8. Батиргареєва В. С. Основні напрями протидії поширенню дезінформації (на прикладі пандемії COVID-19). № 33. — 2020.