РОЗДІЛ ІІ
Суспільні комунікації

УДК 327.7:316.4
Олена Бондаренко,
кандидат психологічних наук,
доцент кафедри міжнародної інформації та країнознавства,
Хмельницький національний університет,
Хмельницький, Україна
elenaivbond@gmail.com
https://orcid.org/0000-0002-7783-7146

КОГНІТИВНЕ МОДЕЛЮВАННЯ РОЗВИТКУ ЗАГРОЗ ПРИВАТНОСТІ ОСОБИСТОСТІ ТА БЕЗПЕЦІ КРАЇНИ

У статті здійснено когнітивне моделювання розвитку загроз приватності особистості та безпеці країни. Для моделювання обрано такі фактори: «Приватність особистості», «Безпека розвитку країни», «Розробка систем захисту», «Онлайн-присутність», «Кібер-атаки», «Втрати від кіберзлочинів», «Витрати на захист», «Сталий розвиток». Результати показали, що всі фактори в системі є дестабілізаційними й чутливими до змін. Найбільш чутливим є фактор «Онлайн-присутність». Такий характер системи свідчить про те, що будь-які зміни можуть дестабілізувати систему, привести до змін усі інші фактори. При цьому система сама сприятиме таким змінам, оскільки є нестійкою. Отже, уся система забезпечення захисту приватності особистості та безпеки країни потребує постійної уваги й моніторингу змін усіх факторів. Фактори «Приватність особистості» та «Безпека розвитку країни» є взаємозалежними, оскільки демонструють майже однаковий вплив на них усіх інших факторів системи. Так, ці фактори підсилюватимуться при зростанні факторів «Розробка систем захисту», «Онлайн-присутність», «Витрати на захист» і «Сталий розвиток». Зростання рівня захисту приватності особистості сприятиме зростанню рівня безпеки країни й навпаки. При цьому «Приватність особистості» сильніше впливає на зміцнення рівня безпеки країни, порівняно з впливом безпеки держави на захист приватності особистості при її присутності в мережі Інтернет. Лише два фактори – «Кібер-атаки» та «Втрати від кіберзлочинів» зменшуватимуть рівень захисту приватності й безпеки країни при їх зростанні. Рівень захисту приватності є більш чутливим до впливу на неї з боку кібератак, порівняно з чутливістю рівня безпеки країни. На рівень безпеки розвитку держави найбільше впливає рівень захисту приватності особистості, і цей вплив на 14 % більш потужний, порівняно з протилежним впливом факторів. Аналіз засвідчив, що основним пріоритетом під час розвитку мережевих технологій, упровадженні ІКТ у всі сфери суспільного життя та розвитку інформаційної економіки повинно бути забезпечення захисту приватності

особистості, її персональних даних. Забезпечення безпеки розвитку країни потребуватиме більшого рівня розвитку систем захисту, порівняно із захистом приватності особистості, при цьому на 4 % менше впливатиме на сталий розвиток.
Ключові слова: *кібербезпека; приватність особи; персональні дані; кіберзлочин.*

1. ВСТУП

Постановка наукової проблеми та її значення. У сучасному світі спостерігаємо інтенсивний процес розвитку, поширення й упровадження різних інформаційно-комунікаційних технологій у всі сфери діяльності людини, суспільства та держави. Рівень розвитку національної інформаційної інфраструктури впливає на оборонний і політичний потенціали держав та є одним із ключових чинників зростання й підвищення конкурентоспроможності на світовій арені. Якість сучасного життя людини також пов'язують із проникненням інформаційно-комунікативних технологій. Однак розвиток ІКТ породжує поряд із позитивними явищами й негативні, такі як інформаційні загрози. Саме унікальні особливості інформаційних технологій полегшують їх використання з деструктивною метою.

Багато країн світу потребують прискорення розвитку важливих індикаторів у сфері кібербезпеки, підвищенні ефективності кіберпростору. Розв'язання проблеми вимагає впровадження комплексу організаційно-технічних заходів і процедур у системі світового кіберпростору з урахуванням негативних чинників вразливості механізмів безпеки. Забезпечення міжнародної безпеки у світовому кіберпросторі вимагає не лише зусиль окремих країн світу, але й розробки та реалізації максимально ефективних міжнародних інструментів. Тому всі економічні й політичні ресурси з протидії загрозам повинні розглядатися спільними зусиллями Міжнародного співтовариства, оскільки стосуються не тільки кожної країни окремо, але й кожної людини. Отже, забезпечення кібербезпеки стає глобальною проблемою людства.

Активне використання персональних даних органами державної влади, комерційними та громадськими організаціями суттєво посилює ризик несанкціонованого вторгнення сторонніх осіб у приватне життя, створює загрозу порушення права на недоторканність приватного життя. Приватність стала одним із найбільш важливих питань у галузі прав людини новітнього часу. Однак проблема контролю за можливостями правопорушень із персональними даними залишається нерозв'язаною. Тому визначення тенденцій глобальних загроз у міжнародному інформаційному просторі й аналіз сучасного стану розвитку загроз приватності особи в умовах зростання злочинності в інформаційній сфері є актуальними для розробки та здійснення превентивних заходів проти кібератак і кіберзлочинів.

Мета й методологічна база дослідження – проведення когнітивного моделювання розвитку загроз приватності особистості та безпеки країни за методикою, запропонованою О. В. Малигіним [1].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Виклад основного матеріалу й обґрунтування результатів дослідження. Когнітивне моделювання розроблено на основі проведеного аналізу загроз безпеці розвитку країн і забезпеченню приватності особи крізь призму кіберзлочинності в інформаційній сфері [2–3].

Попереднім дослідженням світових тенденцій виявлено [2], що злочинність в інформаційній сфері чинить суттєві перешкоди для розвитку країн. Серед найбільш небезпечних напрямів кіберзлочинності – атаки на інфраструктуру, руйнування роботи підприємств, державних установ, кібершпигунство, а також прямі економічні збитки через шахрайства, здирництва, компрометацію даних тощо. Як показав прогноз, кількість уразливостей і ризиків кібербезпеки у світі зростає, тому потрібне посилення міжнародної політики та розробки механізмів протидії кіберзлочинності. Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері [3] засвідчив, що зі зростанням розвитку ІКТ і мережевих технологій, зростає також рівень загроз від злочинності в інформаційній сфері. Крадіжки особистих даних є найбільш поширеним злочином проти приватності особи, а особиста інформація стала цінним товаром для кіберзлочинців. На рівень захисту приватності особи найбільше впливає рівень компрометованих даних, тобто тих, які втрачені, розкриті або викрадені внаслідок дій кіберзлочинців. Прогнозування показало, що обсяг компрометованих даних знижуватиметься.

Тому для когнітивного моделювання обрано такі фактори, як «Приватність особистості», «Безпека розвитку країни», «Розробка систем захисту», «Онлайн-присутність», «Кібер-атаки», «Втрати від кіберзлочинів», «Витрати на захист», «Сталий розвиток». Обрані фактори для когнітивної моделі мають таке тлумачення:

Фактор «Приватність особистості» передбачає рівень захищеності особистості під час її присутності он-лайн, захищеність її особистих даних, облікових записів у фінансових, державних установах. Теоретично високий рівень приватності не потребує систем захисту та не приводить до втрат від кіберзлочинів, робить непотрібними або безперспективними кібератаки, але насправді такий рівень недосяжний, тому потрібні витрати на захист. Зрозуміло, що захищена особа є основою захищеності країни й навпаки.

Фактор «Безпека розвитку країни» відрізняється від фактора приватності лише масштабом потрібних заходів для її досягнення. Безпека країни сприяє сталому розвитку й збільшує можливість присутності організацій, підприємств, державних установ бути присутніми в мережі Інтернет та використовувати сучасні комунікаційні канали для своєї діяльності.

Фактор «Розробка систем захисту» включає всі технічні й програмні заходи захисту від кібератак. Крім того, сюди входять підготовка персоналу та система організаційних заходів щодо належного функціонування інформаційної системи підприємства, організації чи установи. Чим більше і якісніше розроблені системи захисту, тим більш захищена приватність, безпечніше працює інформаційна інфраструктура країни, прискорюється сталий розвиток і

зростає рівень присутності он-лайн. Водночас розробка систем захисту потребує певних витрат із боку суспільства, як фінансових, так і людських, натомість платою за це є зменшення рівня кібератак і втрат від них.

Фактор «Онлайн-присутність» означає активне представлення особистості або організації, підприємства чи установи в мережі Інтернет, використання соціальних мереж, виконання фінансових транзакцій тощо. За присутність он-лайн доводиться платити зменшенням рівня приватності та безпеки країни. Присутність он-лайн стимулює сталий розвиток, розробку систем захисту й коштів на них, а також збільшення кібератак та пов'язаних із цим утрат.

Фактор «Кібератаки» уключають усі види кіберзлочинів, як-от шахрайство, фішинг, здирництво, викрадення особових даних, шпигунство, напади на інформаційну інфраструктуру. Кібератаки вповільнюють сталий розвиток країни та змушують обмежувати присутність он-лайн і спрямовані проти захисту приватності особистості й безпеки країни. З іншого боку, їх зростання вимагає більших розробок систем захисту та витрат на захист, оскільки без цього зростають утрати від кіберзлочинів.

Фактор «Втрати від кіберзлочинів» уключають як фінансові, так і репутаційні втрати. Так, наприклад, оприлюднення інтимних фото особи не завжди призводить до фінансових збитків, однак завжди – до репутаційних утрат. Зрозуміло, що зростання таких утрат змушує обмежувати свій рівень присутності он-лайн, порушує рівень приватності особистості та безпеки країни й водночас зменшує рівень сталого розвитку.

Фактор «Витрати на захист» уключають витрати коштів, часу та людських ресурсів, однак вони окуповуються зменшенням кількості кібератак і втрат від них та сприяють підвищенню рівня захищеності приватності й безпеки країни. Зрозуміло, що зростання витрат уповільнює темпи зростання сталого розвитку країни.

Фактор «Сталий розвиток» – це комплексний фактор, який уключає зростання рівня життя населення, підвищення соціальних стандартів, захищеності суспільства, розвиток усіх сфер його діяльності. Цей фактор сприяє розвитку всіх вищеназваних факторів за винятком кількості кібератак, які можуть бути суттєво зменшені, оскільки потреби у фінансових крадіжках (основного мотиву кіберзлочинців) будуть меншими через високий рівень життя всього населення.

Оскільки треба проаналізувати рівень приватності особистості й безпеку країни в умовах кіберзлочинності, то в цій моделі представлено два цільові фактори – «Приватність особистості» та «Безпека розвитку країни». Решта факторів виступають керівними.

Для оцінки впливу скористаємося такою системою переходу від лінгвістичних змінних до числових значень, що відповідає шкалі Чедока: якщо маємо дуже сильний вплив, беремо значення 0,9, значний вплив – 0,7, істотний вплив – 0,5, помірний – 0,3, слабкий – 0,1, проміжні значення, що перебувають

між приведеними лінгвістичними змінними – 0,8; 0,6; 0,4; 0,2. Негативне значення для впливу одного фактора на інший обираємо у випадку, якщо зростання (посилення) одного фактора приводить до спадання (послаблення) іншого. Результати проведеного аналізу взаємодії факторів з урахуванням напрямів їх зміни наведено в когнітивній карті (див. рис. 1).

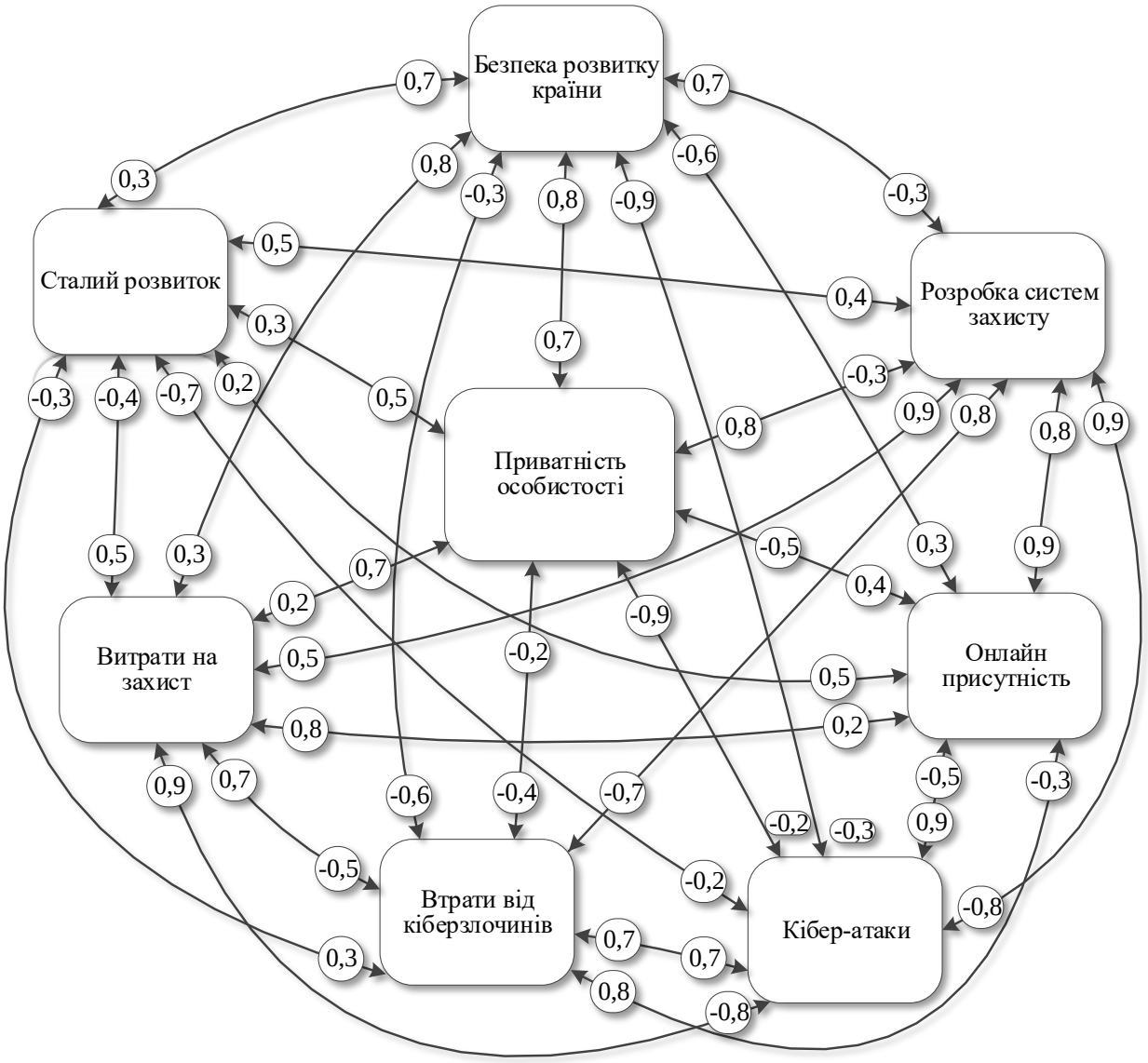

Рис. 1. *Когнітивна карта моделі розвитку загроз приватності особистості та безпеці країни*

Для проведення моделювання потрібно врахувати комплексну взаємодію факторів системи між собою. Усі необхідні розрахунки проведено за методикою когнітивного аналізу, запропонованою О. В. Малигіним [1] та розробленою ним програмою «Когнітивний аналіз». Результати розрахунків значень узагальнених контурів зворотного зв'язку для обраних факторів системи показали, що вони більші за 1. Тому отриману матрицю нормалізовано. Для нормалізації зменшили масштаб отриманих результатів, розділивши всі значення матриці на стале число – 59. Результати нормалізованої матриці зведено в табл. 1.

Таблиця 1

Нормалізовані результати розрахунків когнітивної моделі розвитку загроз приватності особистості та безпеці країни

Фактор	Приватність особистості	Безпека розвитку країни	Розробка систем захисту	Онлайн-присутність	Кібератаки	Утрати від кіберзлочинів	Витрати на захист	Сталий розвиток
Приватність особистості	0,31	0,11	0,08	-0,08	-0,09	-0,1	-0,02	0,08
Безпека розвитку країни	0,1	0,3	0,08	-0,09	-0,08	-0,08	-0,03	0,07
Розробка систем захисту	0,15	0,15	0,37	0,32	-0,05	-0,02	0,27	0,08
Онлайн-присутність	0,38	0,39	0,06	0,67	-0,19	-0,22	0,16	0,3
Кібератаки	-0,09	-0,1	-0,07	0,15	0,31	0,13	0,03	-0,02
Утрати від кіберзлочинів	-0,04	-0,04	-0,03	0,2	0,04	0,23	0,04	0,01
Витрати на захист	0,09	0,09	0,16	0,04	-0,03	-0,02	0,18	0,13
Сталий розвиток	0,24	0,25	0,09	-0,05	-0,15	-0,21	0,04	0,34

Отримані в результаті розрахунків значення узагальнених коефіцієнтів зворотного зв’язку відображено на рис. 2.

За результатами моделювання, представленими на рис. 2, видно, що всі фактори в системі є дестабілізаційними, а отже, і чутливими до змін. Найбільш чутливим фактором є «Он-лайн присутність». Такий характер системи свідчить про те, що будь-які зміни в той чи інший бік (збільшення або зменшення) може дестабілізувати систему, привести до змін всі інші фактори. При цьому система сама сприятиме таким змінам, оскільки є нестійкою. Отже, зростання, наприклад, он-лайн присутності призведе до зростання як кібератак, так і розробок систем захисту, витрат на них, утрат від кіберзлочинів.

Отриманий результат дає підстави зробити висновок: уся система забезпечення захисту приватності особистості та безпеки країни потребує постійної уваги й моніторингу змін усіх факторів. Цей висновок підтверджується й останніми законодавчими ініціативами. Наприклад, у 2018 р. набули чинності глобальні нормативно-правові акти про захист даних, як-от «Генеральний регламент щодо захисту даних в ЄС» (European General Data Protection Regulation, GDPR) і поправки до закону про нерозповсюдження конфіденційної інформації Австралії (Australia's Privacy Amendment Act).

Рис. 2. *Значення узагальнених коефіцієнтів зворотного зв'язку когнітивної моделі розвитку загроз приватності особистості та безпеці країни*

Отримані значення дають уявлення лише про характер поведінки системи, тому проаналізуємо вплив керівних факторів системи на цільові «Приватність особистості» й «Безпека розвитку країни». Результати обчислень представлено на рис. 3.

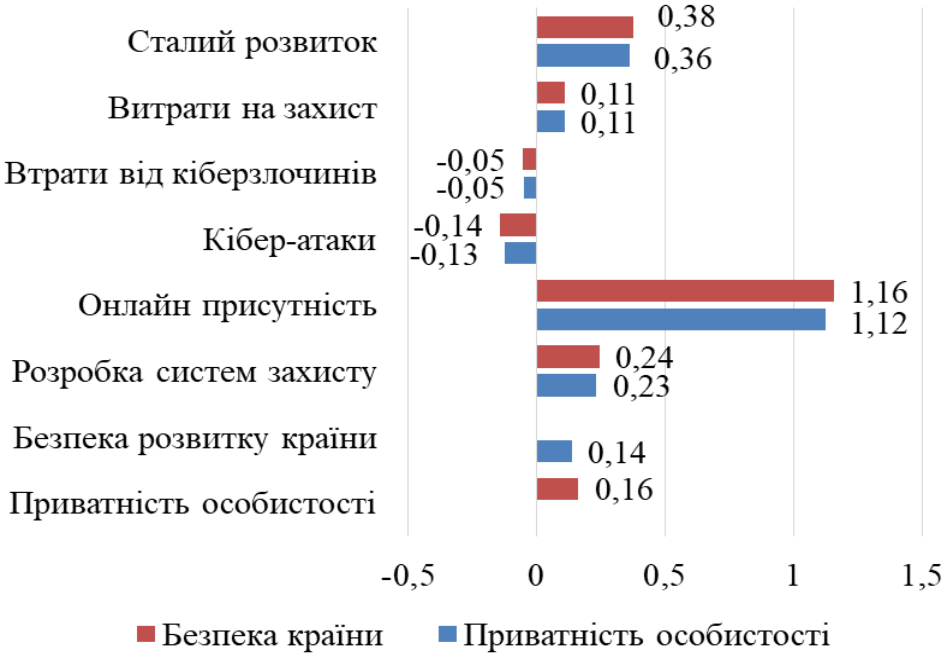

Рис. 3. *Приведені коефіцієнти впливу факторів системи на цільові фактори «Приватність особистості» та «Безпека розвитку країни»*

Результати моделювання свідчать, що фактори «Приватність особистості» та «Безпека розвитку країни» є взаємозалежними, оскільки демонструють

майже однаковий вплив на них усіх інших факторів системи. Так, ці фактори підсилюватимуться за зростання факторів «Розробка систем захисту», «Онлайн-присутність», «Витрати на захист» та «Сталий розвиток».

Крім того, зростання рівня захисту приватності особистості сприятиме зростанню рівня безпеки країни й, навпаки, підвищення рівня безпеки країни сприятиме зростанню рівня захисту приватності. При цьому «Приватність особистості» сильніше впливає на зміцнення рівня безпеки країни, порівняно з впливом її безпеки на захист приватності особистості за її присутності в мережі Інтернет.

Лише два фактори – «Кібератаки» та «Утрати від кіберзлочинів» – зменшуватимуть рівень захисту приватності й безпеки країни за їх зростання. Рівень захисту приватності більш чутливий до впливу на неї з боку кібератак, порівняно з чутливістю рівня безпеки.

З іншого боку, цільові фактори «Приватність особистості» та «Безпека розвитку країни» впливають на всі інші фактори системи розвитку загроз приватності особистості й безпеці країн (див. рис. 4).

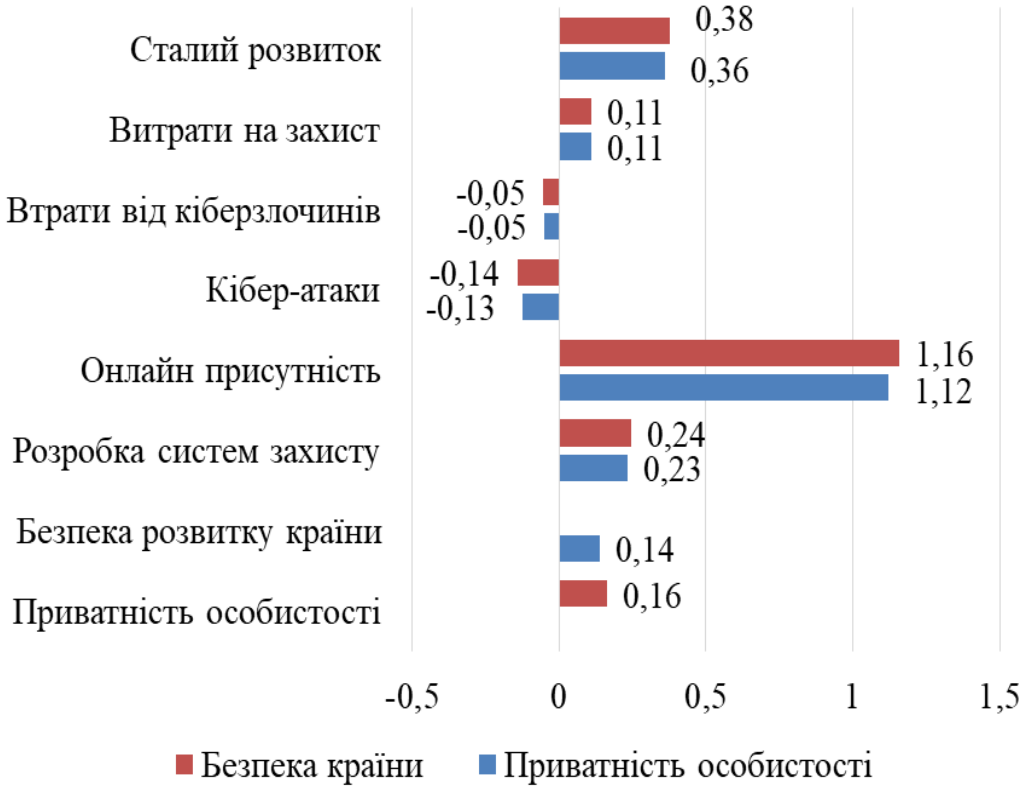

Рис. 4. *Коефіцієнти впливу цільових факторів «Приватність особистості» та «Безпека розвитку країни» на керівні фактори системи*

Результати моделювання свідчать, що на рівень безпеки розвитку країни найбільше впливає рівень захисту приватності особистості й цей вплив на 14 % більш потужний, порівняно з впливом фактора «Безпека розвитку країни» на фактор «Приватність особистості».

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ДОСЛІДЖЕНЬ

Отже, можемо зробити висновок, що основним пріоритетом під час розвитку мережевих технологій, упровадження ІКТ у всі сфери суспільного життя та розвитку інформаційної економіки повинно бути забезпечення захисту приватності особистості, її персональних даних. Моделювання також показало, що забезпечення безпеки розвитку країни потребуватиме більшого рівня розвитку систем захисту, порівняно із захистом приватності особистості, при цьому на 4 % менше впливатиме на сталий розвиток.

Зауважимо, що, за результатами моделювання, посилення рівня захисту приватності особистості більш суттєво зменшить рівень утрат від кіберзлочинності (на 17 %) і кількість кібератак (на 18 %), порівняно з аналогічним підсиленням рівня безпеки розвитку країни. Негативним наслідком підсилення рівня захисту приватності особистості та безпеки держави буде зменшення рівня онлайн-присутності. У реальному житті така суперечність, як розширення використання інформаційних технологій, розвиток інформаційної економіки за необхідності зменшення рівня присутності он-лайн, розв'язується створенням захищеного середовища, доступ до якого обмежений, що й зовні виглядатиме як обмеження присутності он-лайн. Так, наприклад, у соціальних мережах створюються пабліки, які не доступні он-лайн будь-кому, а доступ мають лише ті користувачі, яким дозволений такий доступ. Тобто особа не є присутньою в усьому інформаційному просторі. Аналогічно створюються корпоративні середовища на підприємствах щодо обміну інформацією, листування тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малигін, О. В., Бондаренко, О. І. (2017). Когнітивне моделювання міжнародних відносин: особливості та удосконалення методики досліджень. *Науковий вісник Східноєвропейського національного університету ім. Лесі Українки. Серія: Міжнародні відносини.* Луцьк: Вежа-Друк. Вип. 6 (355), С. 64–69. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/7866/3/Nvvnum_2017_6_13.pdf

2. Бондаренко, О. І. (2018). Аналіз загроз безпеці розвитку країн крізь призму кіберзлочинності. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки:* наук. журн. Луцьк, № 2 (375), С. 54–64. URL: http://elar.khnu.km.ua/jspui/handle/123456789/7111

3. Бондаренко, О. І., Малигін, О. В. (2018). Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки:* наук. журн. Луцьк, № 1 (374), С. 43–52. URL: http://elar.khnu.km.ua/jspui/handle/123456789/6566

THE COGNITIVE MODELING OF THE DEVELOPMENT OF THREATS TO PERSONAL PRIVACY AND STATE SECURITY

In the article the cognitive modelling of the development of threats to personal privacy and state security is presented. The following factors were chosen for the modelling: «The Personal Privacy», «The Security of State Development», «The Development of Security

Systems», «The Online Presence», «Cyber-Attacks», «Losses from Cybercrime», «Security Costs», «The Sustainable Development». The results showed that all factors in the system are destabilizing and sensitive to changes. The «The Online Presence» factor is the most sensitive. This nature of the system indicates that any changes can destabilize the system, causing changes of all other factors. Besides the system itself will be conductive to such changes as it is unstable. Therefore, the whole system of the personal privacy and state security protection needs constant attention and monitoring of all factors' changes. «The Personal Privacy» and «The Security of State Development» factors are interdependent, because all other factors of the system show almost the same impact on them. Thus, these factors will strengthen with the growth of «The Development of Security Systems», «The Online Presence», «Security costs» and «The Sustainable Development» factors. The increase of the personal privacy protection level will contribute to the increase of state security level and vice versa. At the same time «The Personal Privacy» has a stronger impact on the state security reinforcement in comparison to the impact of the state security on the personal privacy protection on the Internet. Only two factors, «Cyber-Attacks» and «Losses from Cybercrime», will decrease the protection level of privacy and state security, if they grow. The level of privacy protection is more sensitive to cyber-attacks than the state security level is. The level of personal privacy protection has the strongest impact on the state development security level. This impact is 14 % more powerful than the reversed impact. According to the analysis, the protection of personal privacy and personal data should be the main priority in the process of network technologies development, implementation of information and communication technologies in all spheres of public life and information economy development. The state development security protection will require a greater level of security systems' development than the protection of personal privacy. And it will have 4% less impact on sustainable development.

Key words: cybersecurity; cyber-extortion; crime in the information sphere; attacks with ransom demand; economic damage.

REFERENCES

1. Malyhin, O. V., Bondarenko, O. I. (2017). Kohnityvne modeliuvannia mizhnarodnykh vidnosyn: osoblyvosti ta udoskonalennia metodyky doslidzhen. *Naukovyi visnyk Skhidnoievropeiskoho natsionalnoho universytetu im. Lesi Ukrainky. Seriia: Mizhnarodni vidnosyny.* Lutsk: Vezha-Druk, Vyp. 6 (355), P. 64–69. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/7866/3/Nvvnum_2017_6_13.pdf

2. Bondarenko, O. I. (2018). Analiz zahroz bezpetsi rozvytku krain kriz pryzmu kiberzlochynnosti. *Naukovyi visnyk Skhidnoievropeiskoho natsionalnoho universytetu imeni Lesi Ukrainky:* nauk. zhurn. Lutsk, № 2 (375). P. 54–64. URL: http://elar.khnu.km.ua/jspui/handle/123456789/7111

3. Bondarenko, O. I., Malyhin, O. V. (2018). Analiz zahroz zabezpechenniu pryvatnosti osoby kriz pryzmu zlochynnosti v informatsiinii sferi. *Naukovyi visnyk Skhidnoievropeiskoho natsionalnoho universytetu imeni Lesi Ukrainky:* nauk. zhurn. Lutsk, № 1 (374), P. 43–52. URL: http://elar.khnu.km.ua/jspui/handle/123456789/6566

Матеріал надійшов до редакції 08.10.2019 р.