УДК 327.7:316.4

Олена Бондаренко,
кандидат психологічних наук,
доцент кафедри міжнародної інформації та країнознавства
Хмельницький національний університет
Хмельницький, Україна
elenaivbond@gmail.com

КОГНІТИВНЕ МОДЕЛЮВАННЯ РОЗВИТКУ ЗАГРОЗ ПРИВАТНОСТІ ОСОБИСТОСТІ ТА БЕЗПЕЦІ КРАЇНИ

У статті здійснено когнітивного моделювання розвитку загроз приватності особистості та безпеці країни. Для моделювання були обрані наступні фактори: «Приватність особистості», «Безпека розвитку країни», «Розробка систем захисту», «Он-лайн присутність», «Кібер-атаки», «Втрати від кіберзлочинів», «Витрати на захист», «Сталий розвиток». Результати показали, що всі фактори в системі є дестабілізуючими і чутливими до змін. Найбільш чутливим є фактор «Он-лайн присутність». Такий характер системи свідчить про те, що будь-які зміни можуть дестабілізувати систему, привести до змін всі інші фактори. При цьому система сама буде сприяти таким змінам, оскільки є нестійкою. Таким чином, вся система забезпечення захисту приватності особистості та безпеки країни потребує постійної уваги та моніторингу змін всіх факторів. Фактори «Приватність особистості» та «Безпека розвитку країни» є взаємозалежними, оскільки демонструють майже однаковий вплив на них всіх інших факторів системи. Так, ці фактори будуть підсилюватись при зростанні факторів «Розробка систем захисту», «Он-лайн присутність», «Витрати на захист» та «Сталий розвиток». Зростання рівня захисту приватності особистості сприятиме зростанню рівня безпеки країни і, навпаки. При цьому «Приватність особистості» сильніше впливає на зміцнення рівня безпеки країни порівняно з впливом безпеки країни на захист приватності особистості при її присутності в мережі Інтернет. Лише два фактори - «Кібер-атаки» та «Втрати від кіберзлочинів» будуть зменшувати рівень захисту приватності та безпеки країни при їх зростанні. Рівень захисту приватності є більш чутливим до впливу на неї з боку кібер-атак порівняно з чутливістю рівня безпеки країни. На рівень безпеки розвитку країни найбільше впливає рівень захисту приватності особистості, і цей вплив є на 14% більш потужним порівняно з протилежним впливом факторів. Аналіз показав, що основним пріоритетом при розвитку мережевих технологій, впровадженні 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 з захистом приватності особистості, при цьому на 4% менше буде впливати на сталий розвиток.
Ключові слова: *кібербезпека; приватність особи; персональні дані; кіберзлочин.*

1. ВСТУП

Постановка наукової проблеми та її значення. У сучасному світі спостерігається інтенсивний процес розвитку, поширення і впровадження різних інформаційно-комунікаційних технологій в усі сфери діяльності людини, суспільства і держави. Рівень розвитку національної інформаційної інфраструктури впливає на оборонний і політичний потенціал держав і є одним з ключових чинників зростання і підвищення конкурентоспроможності на світовій арені. Якість сучасного життя людини також пов’язують з проникненням інформаційно-комунікативних технологій. Однак, розвиток ІКТ

породжує на ряду з позитивними явищами і негативні, такі як інформаційні загрози. Саме унікальні особливості інформаційних технологій полегшують їх використання в деструктивних цілях.

Багато країн світу потребують прискорення розвитку важливих індикаторів в сфері кібербезпеки, підвищенні ефективності кіберпростору. Вирішення проблеми вимагає впровадження комплексу організаційно-технічних заходів і процедур в системі світового кіберпростору з урахуванням негативних чинників вразливості механізмів безпеки. Забезпечення міжнародної безпеки у світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, але і розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам повинні розглядатися спільними зусиллями міжнародного співтовариства, оскільки торкаються вони не тільки кожної країни окремо, але і кожної людини. Таким чином, забезпечення кібербезпеки стає глобальною проблемою людства.

Активне використання персональних даних органами державної влади, комерційними та громадськими організаціями суттєво посилює ризик несанкціонованого вторгнення сторонніх осіб в 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 з персональними даними залишається невирішеною. Тому визначення тенденцій глобальних загроз у міжнародному інформаційному просторі і аналіз сучасного стану розвитку загроз приватності особи в умовах зростання злочинності в інформаційній сфері є актуальними для розробки і здійснення превентивних заходів проти кібератак і кіберзлочинів.

Мета і методологічна база дослідження: проведення когнітивного моделювання розвитку загроз приватності особистості та безпеки країни за методикою, запропонованою Малигіним О.В. [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 було виявлено [2], що злочинність в інформаційній сфері чинить суттєві перешкоди для розвитку країн. Серед найбільш небезпечних напрямків кіберзлочинності є 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 та ризиків кібер-безпеки у світі зростає, тому необхідне посилення міжнародної політики та розробки механізмів протидії кіберзлочинності. Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері [3] показав, що із зростанням розвитку ІКТ та мережевих технологій, зростає і 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 даних, які втрачені, розкриті або викрадені у наслідок дій кіберзлочинців. Прогнозування показало, що обсяг компрометованих даних буде знижуватися.

Тому для когнітивного моделювання були обрані наступні фактори: «Приватність особистості», «Безпека розвитку країни», «Розробка систем захисту», «Он-лайн присутність», «Кібер-атаки», «Втрати від кіберзлочинів», «Витрати на захист», «Сталий розвиток». Обрані фактори для когнітивної моделі мають наступне тлумачення:

Фактор «Приватність особистості» передбачає рівень захищеності особистості під час її присутності он-лайн, захищеність її особистих даних, її облікових записів у фінансових, державних установах. Теоретично, високий

рівень приватності не потребує систем захисту та не приводить до втрат від кіберзлочинів, робить не потрібними або безперспективними кібер-атаки, але у дійсності такий рівень є недосяжним, тому необхідні витрати на захист. Зрозуміло, що захищена особа є основою захищеності країни і навпаки.

Фактор «Безпека розвитку країни» відрізняється від фактору приватності лише масштабом потрібних заходів для її досягнення. Безпека країни сприяє сталому розвитку і 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 в себе всі технічні та програмні заходи захисту від кібер-атак. Крім того, сюди відносяться підготовка персоналу і 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 та зростає рівень присутності он-лайн. У той же час, розробка систем захисту вимагає певних витрат з боку суспільства, як фінансових так і людських, натомість платою за це є зменшення рівня кібер-атак та втрат від них.

Фактор «Он-лайн присутність» означає активне представлення особистості або організації, підприємства чи установи в мережі Інтернет, використання соціальних мереж, виконання фінансових транзакцій тощо. За присутність он-лайн приходиться платити зменшенням рівня приватності та безпеки країни. Присутність он-лайн стимулює сталий розвиток, розробку систем захисту та коштів на них, а також збільшення кібер-атак та пов’язаних з цим втрат.

Фактор «Кібер-атаки» включають всі види кіберзлочинів, як-то шахрайство, фішинг, здирництво, викрадення особових даних, шпигунство, напади на інформаційну інфраструктуру. Кібер-атаки уповільнюють сталий розвиток країни, та змушують обмежувати присутність он-лайн і направлені

проти захисту приватності особистості та безпеки країни. З іншого боку їх зростання вимагає більших розробок систем захисту та витрат на захист, оскільки без цього зростають втрати від кіберзлочинів.

Фактор «Втрати від кіберзлочинів» включають у себе як фінансові втрати, так і репутаційні. Так, наприклад, оприлюднення інтимних фото особи не завжди несе фінансові втрати, однак завжди веде до репутаційних втрат. Зрозуміло, що зростання таких втрат змушує обмежувати свій рівень присутності он-лайн, порушує рівень приватності особистості та безпеки країни, і разом з тим, зменшує рівень сталого розвитку.

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

Фактор «Сталий розвиток» це комплексний фактор, який включає в себе зростання рівня життя населення, підвищення соціальних стандартів, підвищення захищеності суспільства, розвиток всіх сфер його діяльності. Цей фактор сприяє розвитку всіх вище названих факторів за виключенням кількості кібер-атак, які можуть бути суттєво зменшені через те, що потреби у фінансових крадіжках (основного мотиву кіберзлочинців) будуть меншими через високий рівень життя всього населення.

Оскільки необхідно проаналізувати рівень приватності особистості та безпеку країни в умовах кіберзлочинності, то в даній моделі представлені два цільових фактори – «Приватність особистості» та «Безпека розвитку країни», решта факторів виступають керуючими.

Для оцінки впливу скористаємося наступною системою переходу від лінгвістичних змінних до числових значень, що відповідає шкалі Чедока: якщо маємо дуже сильний вплив, приймаємо значення 0,9, значний вплив - 0,7, істотний вплив - 0,5, помірний вплив - 0,3, слабкий вплив - 0,1, проміжні значення, що лежать між приведеними лінгвістичними змінними - 0,8; 0,6; 0,4;

0,2. Негативне значення для впливу одного фактору на інший обираємо у випадку, якщо зростання (посилення) одного фактору приводить до спадання (послаблення) іншого. Результати проведеного аналізу взаємодії факторів з урахуванням напрямків їх зміни наведені у когнітивній карті (див. рис. 1).

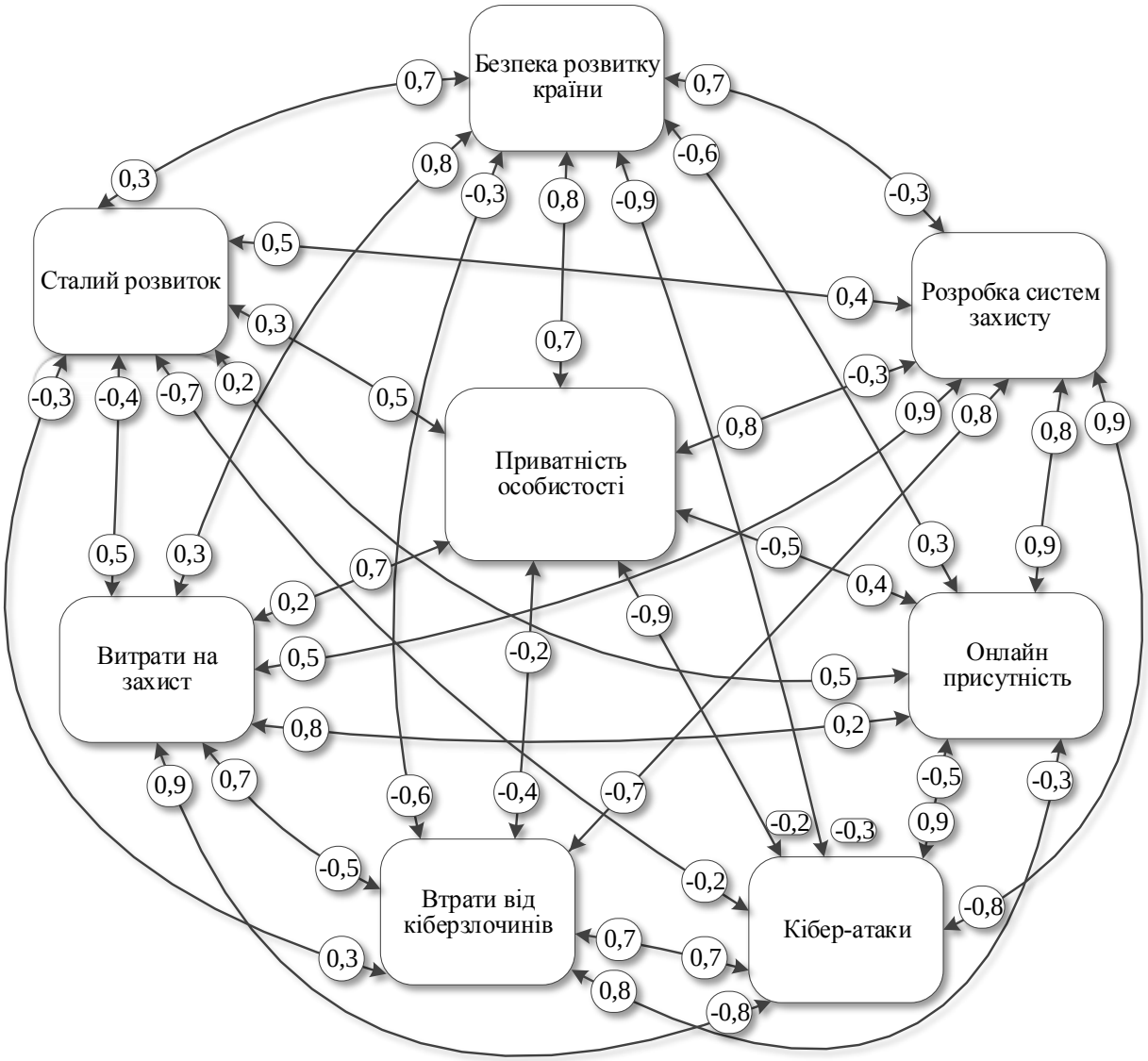

Рис. 1. *Когнітивна карта моделі розвитку загроз приватності особистості та безпеці країни*

Для проведення моделювання необхідно врахувати комплексну взаємодію факторів системи між собою. Усі необхідні розрахунки проведені за методикою когнітивного аналізу, запропонованою Малигіним О.В. [1] та розробленою ним програми «Когнітивний аналіз». Результати розрахунків значень узагальнених контурів зворотного зв'язку для обраних факторів системи показали, що вони більше за 1. Тому отриману матрицю було

нормалізовано. Для нормалізації зменшили масштаб отриманих результатів, розділивши всі значення матриці на стале число - 59. Результати нормалізованої матриці зведені у таблиці 1.

Таблиця 1

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

Фактори	Приватність особистості	Безпека розвитку країни	Розробка систем захисту	Он-лайн присутність	Кібер-атаки	Втрати 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
Он-лайн присутність	0,38	0,39	0,06	0,67	-0,19	-0,22	0,16	0,3
Кібер-атаки	-0,09	-0,1	-0,07	0,15	0,31	0,13	0,03	-0,02
Втрати 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 у результаті розрахунків значення узагальнених коефіцієнтів зворотного зв’язку показані на рисунку 2.

За результатами моделювання, представлених на рисунку 2, видно, що всі фактори в системі є дестабілізуючими, а значить і чутливими до змін. Найбільш чутливим фактором є фактор «Он-лайн присутність». Такий характер системи свідчить про те, що будь-які зміни у той чи інший бік (збільшення або зменшення) може дестабілізувати систему, привести до змін всі інші фактори. При цьому система сама буде сприяти таким змінам, оскільки є нестійкою. Таким чином, наприклад, зростання он-лайн присутності призведе до зростання як кібер-атак, так і розробок систем захисту, витрат на них, втрат від кіберзлочинів.

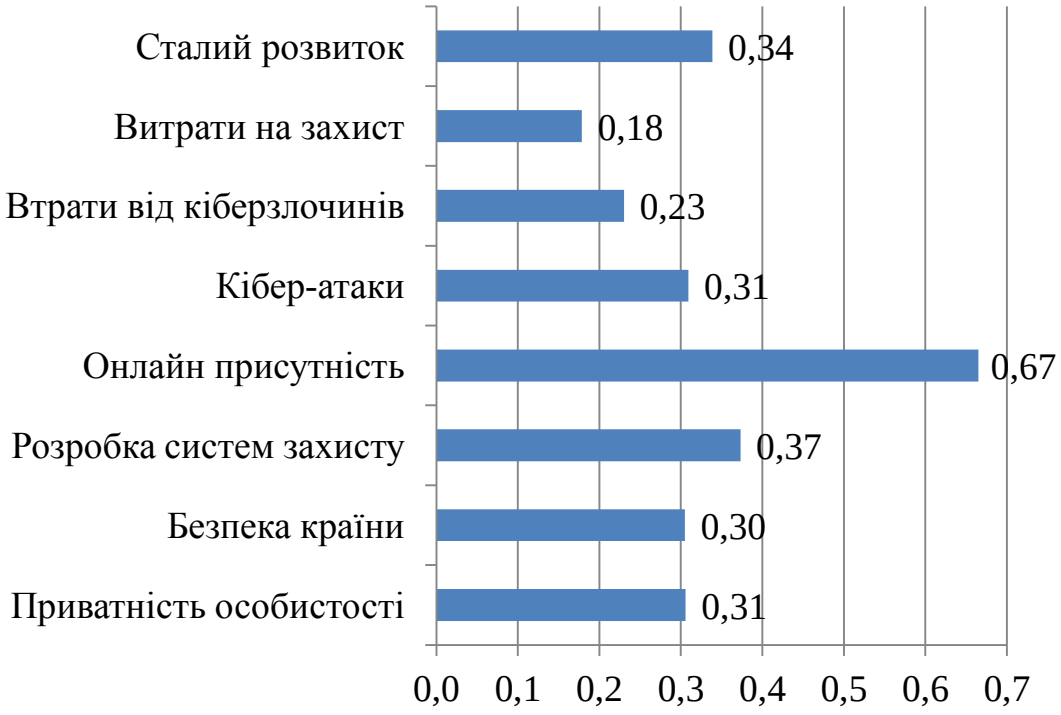

Рис. 2. *Значення узагальнених коефіцієнтів зворотного зв'язку когнітивної моделі розвитку загроз приватності особистості та безпеці країни*

Отриманий результат дає підстави зробити висновок. Що вся система забезпечення захисту приватності особистості та безпеки країни потребує постійної уваги та моніторингу змін всіх факторів. Такий висновок підтверджується і останніми законодавчими ініціативами, наприклад: у 2018 році увійшли в силу глобальні нормативно-правові акти про захист даних, такі як «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).

Отримані значення дають лише уявлення про характер поведінки системи, тому проаналізуємо вплив керуючих факторів системи на цільові «Приватність особистості» та «Безпека розвитку країни». Результати обчислень представлені на рисунку 3.

Результати моделювання свідчать, що фактори «Приватність особистості» та «Безпека розвитку країни» є взаємозалежними, оскільки демонструють майже однаковий вплив на них всіх інших факторів системи. Так, ці фактори

будуть підсилюватись при зростанні факторів «Розробка систем захисту», «Онлайн присутність», «Витрати на захист» та «Сталий розвиток».

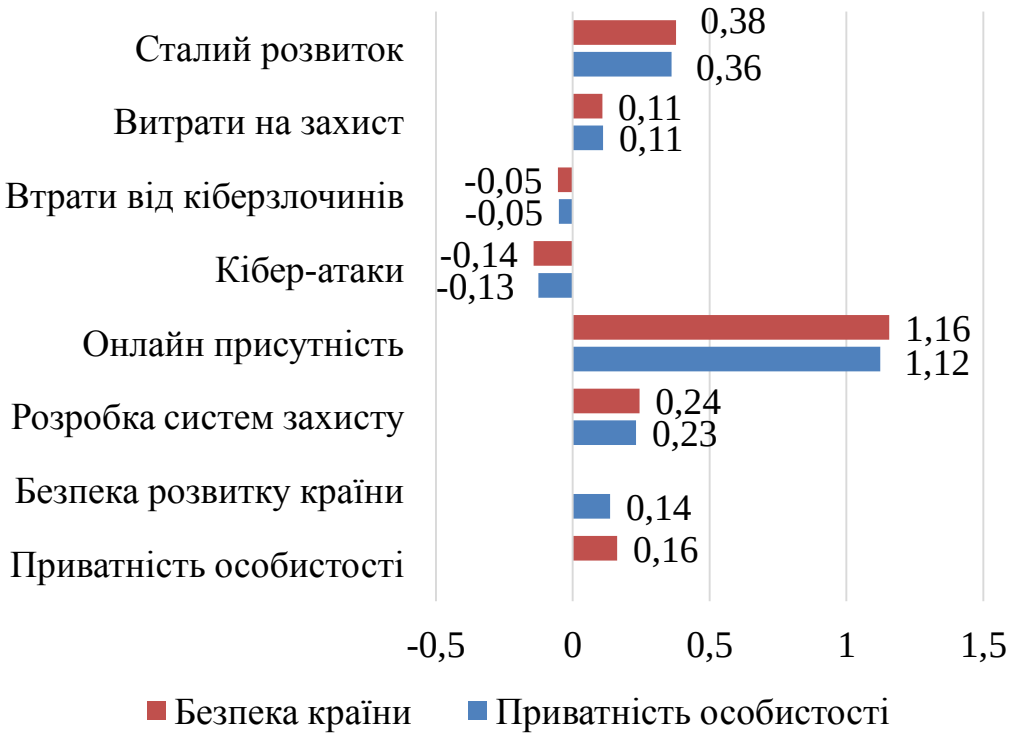

Рис. 3. *Приведені коефіцієнти впливу факторів системи на цільові фактори «Приватність особистості» та «Безпека розвитку країни»*

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

Лише два фактори - «Кібер-атаки» та «Втрати від кіберзлочинів» будуть зменшувати рівень захисту приватності та безпеки країни при їх зростанні. Рівень захисту приватності є більш чутливим до впливу на неї з боку кібер-атак 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 та безпеці країн (див. рис. 4).

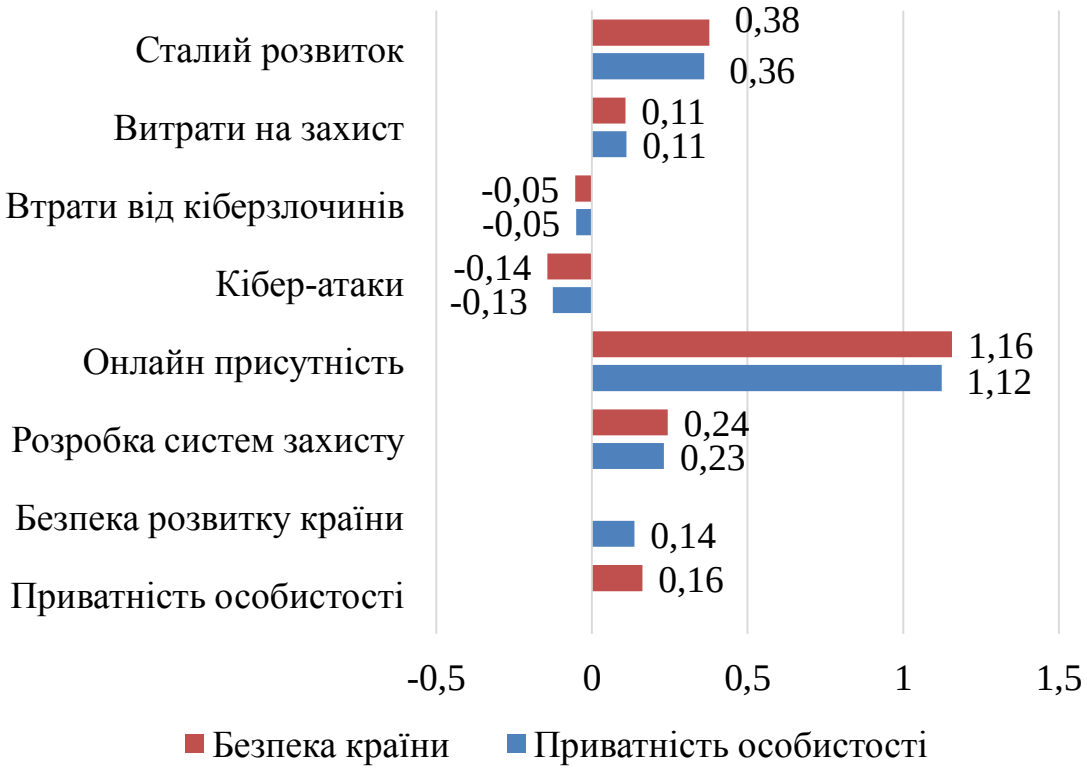

Рис. 4. *Коефіцієнти впливу цільових факторів «Приватність особистості» та «Безпека розвитку країни» на керуючі фактори системи*

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

3. ВИСНОВКИ

Таким чином, можна зробити висновок, що основним пріоритетом при розвитку мережевих технологій, впровадженні 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 з захистом приватності особистості, при цьому на 4% менше буде впливатиме на сталий розвиток.

Слід зауважити, що за результатами моделювання посилення рівня захисту приватності особистості більш суттєво зменшить рівень втрат від

кіберзлочинності (на 17%) та кількість кібер-атак (на 18%) порівняно з аналогічним підсиленням рівня безпеки розвитку країни. Негативним наслідком підсилення рівня захисту приватності особистості та безпеки держави буде зменшення рівня он-лайн присутності. У реальному житті таке протиріччя, як розширення використання інформаційних технологій, розвиток інформаційної економіки при необхідності зменшення рівня присутності он-лайн розв'язується створенням захищеного середовища, доступ до якого обмежений, що і зовні виглядатиме як обмеження присутності он-лайн. Так, наприклад, в соціальних мережах створюються пабліки, які не доступні он-лайн будь-кому, а доступ мають лише ті користувачі, яким дозволено такий доступ. Тобто особа не є присутньою в усьому інформаційному просторі. Аналогічним чином створюються корпоративні середовища на підприємствах щодо обміну інформації, листування, тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малигін О.В., Бондаренко О.І. Когнітивне моделювання міжнародних відносин: особливості та удосконалення методики досліджень // Науковий вісник Східноєвропейського національного університету ім. Лесі Українки. Серія : Міжнародні відносини. - Луцьк: Вежа-Друк, 2017. -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. Аналіз загроз безпеці розвитку країн крізь призму кіберзлочинності. // Науковий вісник Східноєвропейського національного університету імені Лесі Українки : наук. журн. – Луцьк, 2018. – № 2 (375). – С. 54-64. URL: http://elar.khnu.km.ua/jspui/handle/123456789/7111

3. Бондаренко О. І., Малигін О.В. Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері. // Науковий вісник Східноєвропейського національного університету імені Лесі Українки : наук. журн. – Луцьк, 2018. – № 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. Kohnityvne modeliuvannia mizhnarodnykh vidnosyn: osoblyvosti ta udoskonalennia metodyky doslidzhen // Naukovyi visnyk Skhidnoievropeiskoho natsionalnoho universytetu im. Lesi Ukrainky. Seriia : Mizhnarodni vidnosyny. - Lutsk: Vezha-Druk, 2017. -Vyp. 6 (355). - S. 64 – 69. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/7866/3/Nvvnum_2017_6_13.pdf

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

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

Стаття надійшла до редколегії 12.11.2019 р.