КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.1928
УДК.004.056

Лаптєв Олександр Анатолійович
доктор технічних наук, старший науковий співробітник
професор кафедри систем інформаційного та кібернетичного захисту
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-4194-402X
Alaptev64@ukr.net

Собчук Валентин Володимирович
доктор технічних наук, доцент
професор кафедри вищої математики
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-4002-8206
v.v.sobchuk@gmail.com

Собчук Андрій Валентинович
PhD
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0003-3250-3799
anri.sobchuk@gmail.com

Лаптєв Сергій Олександрович
Навчально-науковий інститут Захисту інформації
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-7291-1829
salaptiev@gmail.com

Лаптєва Тетяна Олександрівна
Навчально-науковий інститут Захисту інформації
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-5223-9078
tetiana1986@ukr.net

УДОСКОНАЛЕНА МОДЕЛЬ ОЦІНЮВАННЯ ЕКОНОМІЧНИХ ВИТРАТ НА СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація. У сучасних умовах, важлива роль у забезпеченні інформаційної безпеки підприємства та особливо його економічної складової, належить процесам забезпечення інформаційної безпеки держави в цілому. Ключову роль при побудові систем безпеки інформаційних ресурсів як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єкта забезпечення інформаційної безпеки держави на усіх рівнях. У статті проведено аналіз підходів до оцінки оцінювання економічних витрат на систему захисту інформації. Здійснено вибір базової моделі. Використовуючи базову модель оцінки рівня захищеності інформації в соціальній мережі від зовнішніх впливів на інформаційний соціальний ресурс, зроблено удосконалення з метою оцінки економічної доцільності впровадження того чи іншого механізму технічних засобів захисту інформації в соціальних мережах залежно від цінності інформації. Удосконалення проведено з урахуванням припущення, яке полягає у тому, що сума засобів, виділених атакуючою стороною дорівнює цінності інформації, цінність інформації однакова для обох сторін, і протиборчі сторони знаходяться в рівних умовах. Визначили основні параметри від котрих залежить ефективність запропонованої моделі оцінювання економічних витрат. Ефективність запропонованої моделі оцінювання економічних витрат залежить від точності формулювання ймовірності успіху захисту і визначення цінності інформації. Перспектива подальших досліджень та розробок може бути спрямована на врахуванні у моделі додаткових

факторів які впливають на оцінювання затрат на систему захисту інформації, що дозволить проводити розрахунки з більшою точністю

Ключові слова: модель, безпека, захист, соціальні мережі, економічний ресурс, зовнішні впливи.

ВСТУП

Постановка проблеми. У сучасних умовах, як показала практика, важлива роль у забезпеченні інформаційної безпеки підприємства та особливо його економічної складової, належить процесам забезпечення інформаційної безпеки держави в цілому. Ключову роль при побудові систем безпеки інформаційних ресурсів як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єкта забезпечення інформаційної безпеки держави на усіх рівнях. Прийняття рішення неможливо без урахування економічних складових комплексного захисту інформації. Перспективним підходом до безпеки інформаційних ресурсів є одночасне та раціональне поєднання організаційних і технічних зусиль підприємства, спрямованих на забезпечення інформаційної безпеки, кібербезпеки та безпеки інформації, що зрештою позначиться на інвестиціях підприємства, вкладених у безпеку.

При цьому комплексування сил і засобів безпеки у кожному окремому випадку не можна вважати ефективним та таким, що гарантує досягнення очікуваного безпекового синергетичного ефекту без урахування економічної складової.

Тому питання оцінювання економічних витрат на систему захисту інформації в соціальних мережах є дуже важливим, а завдання розробки та удосконалення моделей оцінювання економічних витрат на систему захисту інформації в соціальних мережах є дуже актуальним.

Аналіз останніх досліджень і публікацій. Враховуючи стрімкий розвиток науки і техніки за останні десять років, а також інтенсивне застосування новітніх високотехнологічних розробок в соціальних мережах сутність і зміст категорії захисту інформації істотно змінилась

У роботі [1] показано, що інформаційні процеси, які відбуваються всюди у світі, висувають на перший план найважливіше завдання забезпечення безпеки інформації. Це пояснюється особливою значущістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою вразливістю і нерідко значними збитками в результаті її несанкціонованого використання.

У [2,3] наводиться методика Applied Information Economics (AIE), яка була розроблена Дугласом Хаббардом, керівником компанії Hubbard Ross. Компанія Hubbard Ross, заснована в березні 1999 року, стала першою організацією, яка використала методику AIE для аналізу цінності інвестицій в технології безпеки з фінансової та економічної точки зору. Методика AIE дозволяє підвищити точність показника «дійсна економічна вартість вкладень в технології безпеки шляхом визначення прибутковості інвестицій» (Return on Investment, ROI) до і після інвестування. Але в процесі оцінки підприємство або організація визначає економічні показники своїх споживачів шляхом відстеження доходів, витрат і прибутків по кожному замовникові окремо. Тому недолік методу полягає в труднощі формалізації процесу встановлення прямого зв'язку між інвестиціями в технології безпеки і збереженням або збільшенням числа споживачів. Цей метод застосовується в основному для оцінки ефективності корпоративних систем захисту інформації в компаніях, у яких число замовників безпосередньо впливає на всі аспекти бізнесу.

ISSN 2663 - 4023

У роботах [4-7] описується методика обчислення доданої вартості (Economic Value Added), яка пропонує несуперечливий підхід до визначення цілей і виміру показників, до оцінки стратегій, до розміщення капіталу та ін. Методика EVA пропонує розглядати службу інформаційної безпеки як «держава в державі», тобто фахівці служби безпеки продають свої послуги усередині компанії за розцінками, приблизно еквівалентним розцінками на зовнішньому ринку, що дозволяє компанії відстежити доходи і витрати, пов'язані з технологіями безпеки. Але таким чином, служба безпеки перетворюється в центр прибутку і з'являється можливість чітко визначити, як витрачаються активи, пов'язані з технологіями безпеки, і збільшуються доходи акціонерів.

У статті [8] Наводиться методика Economic Value Sourced (EVS), яка була розроблена компанією META Group Consulting. Методика передбачає точний розрахунок всіх можливих ризиків для бізнесу, пов'язаних з впровадженням і функціонуванням корпоративної системи захисту інформації. При цьому розширюється використання таких інструментальних засобів оцінки IT, як додана економічна вартість (EVA), внутрішня норма рентабельності (IRR) і повернення від інвестицій (ROI) шляхом визначення і залучення в оцінний процес параметрів часу і ризику, що дуже ускладнює процес.

У роботах [9-12] Наводиться метод життєвого циклу штучних систем System Life Cycle Analysis (SLCA).В основі методу життєвого циклу штучних систем System Life Cycle Analysis (SLCA) лежить вимір «ідеальності» корпоративної системи захисту інформації — співвідношення її корисних факторів до суми шкідливих факторів і чинників розплати за виконання корисних функцій. Оцінку передує спільна робота аналітика і провідних фахівців обстежуваної компанії з вироблення реєстру корисних, негативних і витратних факторів бізнес-системи без використання системи безпеки і присвоєння їм певних вагових коефіцієнтів. Результатом роботи є розрахункова модель, що описує стан без системи безпеки. Після цього в модель вводяться описані фактори очікуваних змін і проводиться розрахунок рівня розвитку компанії з корпоративною системою захисту інформації. Таким чином, будуються традиційні моделі «Як є» і «Як буде» з урахуванням реєстру корисних, негативних і витратних факторів бізнес-системи. Це дуже складні моделі. Вони в загальному вигляді не дозолять оцінити економічну складову безпеки інформації.

Таким чином, в результаті вивчення літературних джерел можна зробити висновок, що завдання удосконалення моделей оцінювання економічних витрат на систему захисту інформації в соціальних мережах є дуже актуальним.

Мета статті. Провести аналіз підходів до оцінки оцінювання економічних витрат на систему захисту інформації. Здійснити вибір моделі та удосконалити модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Визначити основні параметри від котрих залежить ефективність запропонованої моделі оцінювання економічних витрат.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У результаті проведеного аналізу моделей економічної ефективності системи захисту інформації та для вирішення мети статті. Зробимо вибір моделі для удосконалення моделі оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Скористуємось моделлю оцінки рівня захищеності інформації в соціальній мережі від зовнішніх впливів на інформаційний соціальний ресурс, яка описується таким способом:

ISSN 2663 - 4023

$$PR_{OZ}^{ISN} = \begin{Bmatrix} \{I^A\}, \{R^{ISN}\}, \{IM^{ISN}\}, \{RD^{ISN}\}, \\ \{SZ^{ISN}\}, \{DAZ^{ISN}\}, \{UZ^{ISN}\} \end{Bmatrix}, \quad (1)$$

де

$\{I^A\}$ – множина елементів інформації в соціальних мережах;

$\{R^{ISN}\}$ – множина елементів репутації користувачів соціальних мереж;

$\{IM^{ISN}\}$ – множина джерел впливів на систему захисту інформації;

$\{RD^{ISN}\}$ – множина вимог керівних документів по захисту інформації;

$\{SZ^{ISN}\}$ – множина можливих технічних систем захисту інформації;

$\{DAZ^{ISN}\}$ – данні аудиту захищеності інформації в соціальних мережах;

$\{UZ^{ISN}\}$ – рівень захищеності інформації в соціальних мережах.

Для визначення зв'язку між зовнішніми впливами та технічними засобами захисту інформації скористаймось виразом:

$$V^{IMSZ} = \left\| v_{ij}^{IMSZ} \right\| \quad (2)$$

При цьому необхідно враховувати, точніше приймати до уваги, що значення і ma j мають визначену прилеглі вість, а саме:

$$\forall i \in \{IM_k\} \quad ma \quad \forall j \in \{I^A\} \quad (3)$$

Матриця загроз буде мати значення:

$$\left\| V^{IM} \right\| = \begin{cases} 1, \text{ якщо для } j-\text{го інформаційного активу існують і впливів} \\ 0, \text{ якщо для } j-\text{го інформаційного активу не існують і впливів} \end{cases}$$

Кожен механізм захисту інформації в соціальних мережах $SZ_k \in \{SZ^{ISN}\}$ характеризується вектором:

$$SZ_k = (T_{SZ}, T_V, C_{SZ}), \quad (4)$$

де

T_{SZ} – тип захисту інформації;

T_V – час впровадження;

C_{SZ} – вартість системи захисту.

ISSN 2663 - 4023

Для опису зв'язку між зовнішніми впливами і технічними засобами захисту інформації використовується матриця:

$$V^{IMSZ} = \left\| v_{ij}^{IMSZ} \right\|, \quad (5)$$

де v_{ij}^{IMSZ} – відображає наявність зв'язку між *i*-їм впливом на систему захисту інформації $IM_k \in \left\{ IM^{ISN} \right\}$ та *j*-м технічним засобом захисту інформації $SZ_k \in \left\{ SZ^{ISN} \right\}$.

У моделі використані такі типи зв'язку: MZ – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_k \in \left\{ VH \right\}$; NMZ – немає механізму захисту для забезпечення протидії і-й загрозі. При цьому $v_{ij}^{IMSZ} \in \left\{ MZ, NMZ \right\}$, MZ, NMZ – наявність зв'язку певного типу між *i*-їм впливом та *j*-м технічним засобом захисту інформації. Для елементів матриці значення визначаються за правилом:

$$\left\| v_{ij}^{IMSZ} \right\| = \begin{cases} MZ, \ якщо \ i-ий \ вплив \ розкривается \ j-м \ технічним \ засобом \\ NMZ \ якщо \ i-ий \ вплив \ не \ розкривается \ j-м \ технічним \ засобом \end{cases}$$

Якщо для всіх *i* = *m*, $v_{ij}^{IMSZ} = NMZ$, то робиться висновок, що технічні засоби захисту інформації в соціальних мережах не здатні захистити інформаційні ресурси від певного деструктивного впливу, а тому, для підвищення рівня захищеності інформації, необхідно залучати додаткові кошти на механізми захисту.

Наступним кроком будемо визначати множини вимог регуляторів $\left\{ RD^{IMSZ} \right\}$, які складаються з вимог до забезпечення захисту інформації в соціальних мережах – $\left\{ R_{RD} \right\}$, зазначених у міжнародних і національних рекомендацій, множини оцінок ступеня виконання вимог безпеки $\left\{ OV_{RD} \right\}$ та множини підсумкового рівня відповідності захисту інформації соціальних мережах вимогам з множини $\left\{ IU_{RD} \right\}$, остаточно маємо:

$$\left\{ RD^{IMSZ} \right\} = \left\{ R_{RD} \right\} \cup \left\{ OV_{RD} \right\} \cup \left\{ IU_{RD} \right\}. \quad (6)$$

Визначення узагальненого показника рівня захищеності інформації в соціальній мережі, який дозволяє оцінити рівень відповідності технічних засобів захисту інформації вимогам рекомендацій та документам будуть визначатися:

$$OPZ^{ISN} = \sum_{i=1}^{k} OPZ_i, \quad (7)$$

де *k* – кількість окремих показників захисту інформації;

OPZi – окремий показник набуває значення з множини: OPZi – відсутність неприпустимих ризиків, при створенні системи захисту інформації необхідно визначити

ISSN 2663 - 4023

моделі загроз. При складанні моделі загроз / моделі зловмисника і оцінки ризиків (якщо виявлені неприпустимі за своїм рівнем ризики, то OPZi = 0, в іншому випадку – OPZi = 1);

OPZ2 – відсутність небезпечних загроз (якщо виявлені загрози вже заблоковані технічними засобами захисту інформації, то OPZ2 = 1, у разі, якщо в системі захисту інформації в соціальних мережах, при складанні моделі виявлені загрози або впливи, які не можуть бути заблокованими технічними засобами захисту інформації існуючий системи – OPZ2 = 0); OPZ3 – рівень відповідності захищеності інформації в соціальній мережі вимогам рекомендацій до систем захисту (якщо визнаний рекомендованим – OPZ3 = 1, в разі, якщо визнано нерекомендованим – OPZ3 = 0). На підставі отриманих даних системі присвоюється один із трьох рівнів захищеності – UZ^{ISN} ={низький, середній, високий}, при чому:

$$UZ^{ISN} = \begin{cases} високий, якщо \quad OPZ^{ISN} = 3 \\ високий, якщо \quad 1 \le OPZ^{ISN} \le 3 \\ низький, якщо \quad OPZ^{ISN} = 0 \end{cases} \tag{8}$$

Отримана в результаті аудиту оцінка захищеності інформації в соціальній мережи дозволяє визначити найбільш цінні інформаційні активи інформації, ефективність використовуваних засобів для їх захисту, а також ступінь відповідності системи технічного захисту інформації вимогам до захисту і рівнем захищеності регулятора, виявити найбільш уразливі місця і виробити рекомендації щодо підвищення, в разі необхідності, захищеності інформації.

Для оцінки економічної доцільності впровадження того чи іншого механізму технічних засобів захисту інформації в соціальних мережах залежно від цінності інформації введемо такі позначення:

V_{IS}^{ISN} – цінність інформації для користувачів соціальної мережи (сторони, що володіють інформацією, і намагаються її захистити);

V_{IS}^{IZ} – цінність інформації для атакуючої сторони (яка намагається отримати інформацію);

SZ^{ISN} – засоби можливих технічних засобів захисту інформації;

$SV^{SN} = \{SV^{ISN}, SV^{SNZ}, SV^{SNZT}\}$ – засоби, що виділяються на отримання інформаційних ресурсів;

SV^{ISN} – засоби злому механізмів системи доступу до інформації;

SV^{SNZ} – засоби злому механізмів системи конфіденційності інформації;

SV^{SNZT} – засоби злому механізмів технічних засобів захисту інформації.

Виходячи з вище викладеного будемо мати:

$$SV^{SN} = \{SV^{ISN}\} \cap \{SV^{SNZ}\} \cap \{SV^{SNZT}\} \tag{9}$$

Очевидним визнається факт, що безглуздо вкладати кошти в захист або отримання інформації більше, ніж цінність самій інформації не має цензу. Тобто вірні нерівності:

$$V_{IS}^{IZ} \ge SV^{SN}, \quad V_{IS}^{SN} \ge SV^{ISN} \tag{10}$$

ISSN 2663 - 4023

Для подальшого розвитку моделі оцінювання економічних витрат, зробимо припущення, що ймовірності визначаються виразами:

$$P_{Zj} = \frac{q_Z \times SV^{ISN}}{q_Z \times SV^{SN} + q_V \times SV^{ISN}}, \quad (11)$$

$$P_{Vj} = \frac{q_Z \times SV^{ISN}}{q_Z \times SV^{SN} + q_V \times SV^{ISN}}, \quad (12)$$

де

q_V, q_Z – вагові коефіцієнти, що визначають наскільки кожна зі сторін близька до мети;

P_{Vj} – ймовірність реалізації хоча б однієї *i*-ї загрози *j*-му активу (ймовірність успіху нападаючою стороною);

P_{Zj} – ймовірність захисту від *i*-ой загрози *j*-му активу (ймовірність успіху захищається стороною).

Припустимо, що сума засобів, виділених атакуючою стороною дорівнює цінності інформації, цінність інформації однакова для обох сторін, і протиборчі сторони знаходяться в рівних умовах, тоді економічна вартість витрат на захист інформації в соціальних мережах не повинна перевищувати:

$$SV^{ISN} = V_{IS}^{ISZ} \times \frac{\sqrt{5}-1}{2} \quad (13)$$

Таким чином удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Ефективність запропонованої моделі оцінювання економічних витрат залежить від точності формулювання ймовірності успіху захисту і визначення цінності інформації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведено аналіз підходів до оцінки оцінювання економічних витрат на систему захисту інформації. Здійснити вибір базової моделі.

На основі базової моделі оцінки рівня захищеності інформації в соціальній мережі від зовнішніх впливів на інформаційний соціальний ресурс, зроблено удосконалення з метою оцінки економічної доцільності впровадження того чи іншого механізму технічних засобів захисту інформації в соціальних мережах залежно від цінності інформації. Удосконалення проведено з урахуванням припущення, яке полягає у тому, що сума засобів, виділених атакуючою стороною дорівнює цінності інформації, цінність інформації однакова для обох сторін, і протиборчі сторони знаходяться в рівних умовах.

Визначили основні параметри від котрих залежить ефективність запропонованої моделі оцінювання економічних витрат. Ефективність запропонованої моделі оцінювання економічних витрат залежить від точності формулювання ймовірності успіху захисту і визначення цінності інформації.

Перспектива подальших досліджень та розробок може бути спрямована на врахуванні у моделі додаткових факторів які впливають на оцінювання затрат на систему захисту інформації, що дозволить проводити розрахунки з більшою точністю.

СПИСОК ВИКОРОСТАНИХ ДЖЕРЕЛ

1. Yevseiev S., Kots H., & Korol O. (2015). Analysis of the legal framework for the information security management system of the NSMEP. Eastern-European Journal of Enterprise Technologies, 5(3(77), 48–59. https://doi.org/10.15587/1729-4061.2015.51468
2. Yevseiev S., & Abdullayev V. (2015). Monitoring algorithm of two-factor authentication method based on passwindow system. *Eastern-European Journal of Enterprise Technologies*, *2*(2(74), 9–16. https://doi.org/10.15587/1729-4061.2015.38779
3. Yevseiev, S., Kots, H., & Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies*, *6*(4 (84), 11–23. https://doi.org/10.15587/1729-4061.2016.86175
4. Yevseiev, S., Korol, O., & Kots, H. (2017). Construction of hybrid security systems based on the cryptocode structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*, *4*(9 (88), 4–21. https://doi.org/10.15587/1729-4061.2017.108461
5. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V., & Yarovyi A. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. *Eastern-European Journal of Enterprise Technologies*, *4*(9 (100), 6–19. https://doi.org/10.15587/1729-4061.2019.175978
6. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S., Korolev, R., Kots, H., Milov, O., & Shmatko, O. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies*, *6*(4 (96), 24–31. https://doi.org/10.15587/1729-4061.2018.150903
7. Korchenko, O., Skachek, L., & Khoroshko, V. (2014). *Banking Security*. PVP "Zadruga.
8. Shiyan, A. (2016). Methodology of complex protection of people and social groups from negative information and psychological influence. *Information security*, *1*(22), 94–98.
9. Korchenko, O., Kazmirchuk, S., & Ivanchenko, E. (2017). The methodology for the synthesis of adaptive risk assessment systems of security information system resources. *Ukrainian Information Security Research Journal*, *19*(3). https://doi.org/10.18372/2410-7840.19.11898
10. Yudin, O., & Buchyk, S. (2015). Methodology of Defence of State Informative Resources Comparative Analysis of BASIC Terms and Determinations. *Ukrainian Information Security Research Journal*, *17*(3). https://doi.org/10.18372/2410-7840.17.9518
11. Zhurilenko, B. (2015). Construction and Analysis Methodology of Complex Technical Information Security with Probabilistic Reliability and Counting of Temporal Breaking attempts. *Ukrainian Information Security Research Journal*, *17*(3). https://doi.org/10.18372/2410-7840.17.9515
12. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks. *EUREKA: Physics and Engineering*, (1), 24-31. https://doi.org/10.21303/2461-4262.2021.001615
13. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., & Biehun A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security* (IJCNIS), Vol. 13, No. 1, pp.1-14.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Oleksandr A.Laptiev
Doctor of Technical Science, Senior Researcher
Professor of the Department of Information and Cyber Security Systems
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-4194-402X
Alaptev64@ukr.net

Valentyn V.Sobchuk
Doctor of Engineering, Associate Professor
Professor of the Department of Higher Mathematics
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-4002-8206
v.v.sobchuk@gmail.com

Andrii V.Sobchuk
PhD
Faculty of Information Technology
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0003-3250-3799
anri.sobchuk@gmail.com

Serhii O. Laptiev
Institute of Information Protection
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-7291-1829
salaptiev@gmail.com

Tatiana O. Laptieva
Institute of Information Protection
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-5223-9078
tetiana1986@ukr.net

IMPROVED MODEL OF ESTIMATING ECONOMIC EXPENDITURES ON THE INFORMATION PROTECTION SYSTEM IN SOCIAL NETWORKS

Abstract. In modern conditions, an important role in ensuring the information security of the enterprise and especially its economic component belongs to the processes of information security of the state as a whole. The key role in building security systems of information resources as components of national information resources of the state is played by theory and practice, in which the scientific and methodological basis is the basis for making sound and effective management decisions of the information security of the state at all levels. The article analyzes the approaches to estimating the assessment of economic costs for the information security system. The base model is selected. Using the basic model of assessing the level of protection of information in the social network from external influences on the information social resource, improvements were made to assess the economic feasibility of implementing a mechanism of technical means of information protection in social networks depending on the value of information. The improvement is based on the assumption that the amount of funds allocated by the attacking party is equal to the value of the information, the value of the information is the same for both parties, and the opposing parties are on equal terms. The main parameters on which the efficiency of the proposed model of estimating economic costs depends. The efficiency of the proposed model of estimating economic costs depends on the accuracy of formulating the probability of success of protection and determining the value of information. The prospect of further research and development may be aimed at taking into account in the model additional factors that affect the estimation of costs for the information security system, which will allow calculations to be performed with greater accuracy

Keywords: model, security, protection, social networks, economic resource, external influences.

REFERENCES

1 Yevseiev S., Kots H., & Korol O. (2015). Analysis of the legal framework for the information security management system of the NSMEP. Eastern-European Journal of Enterprise Technologies, 5(3(77), 48–59. https://doi.org/10.15587/1729-4061.2015.51468

2 Yevseiev S., & Abdullayev V. (2015). Monitoring algorithm of two-factor authentication method based on passwindow system. *Eastern-European Journal of Enterprise Technologies*, *2*(2(74), 9–16. https://doi.org/10.15587/1729-4061.2015.38779

3 Yevseiev, S., Kots, H., & Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies*, *6*(4 (84), 11–23. https://doi.org/10.15587/1729-4061.2016.86175

4 Yevseiev, S., Korol, O., & Kots, H. (2017). Construction of hybrid security systems based on the cryptocode structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*, *4*(9 (88), 4–21. https://doi.org/10.15587/1729-4061.2017.108461

5 Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V., & Yarovyi A. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. *Eastern-European Journal of Enterprise Technologies*, *4*(9 (100), 6–19. https://doi.org/10.15587/1729-4061.2019.175978

6 Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S., Korolev, R., Kots, H., Milov, O., & Shmatko, O. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies*, *6*(4 (96), 24–31. https://doi.org/10.15587/1729-4061.2018.150903

7 Korchenko, O., Skachek, L., & Khoroshko, V. (2014). *Banking Security*. PVP "Zadruga.

8 Shiyan, A. (2016). Methodology of complex protection of people and social groups from negative information and psychological influence. *Information security*, *1*(22), 94–98.

9 Korchenko, O., Kazmirchuk, S., & Ivanchenko, E. (2017). The methodology for the synthesis of adaptive risk assessment systems of security information system resources. *Ukrainian Information Security Research Journal*, *19*(3). https://doi.org/10.18372/2410-7840.19.11898

10 Yudin, O., & Buchyk, S. (2015). Methodology of Defence of State Informative Resources Comparative Analysis of BASIC Terms and Determinations. *Ukrainian Information Security Research Journal*, *17*(3). https://doi.org/10.18372/2410-7840.17.9518

11 Zhurilenko, B. (2015). Construction and Analysis Methodology of Complex Technical Information Security with Probabilistic Reliability and Counting of Temporal Breaking attempts. *Ukrainian Information Security Research Journal*, *17*(3). https://doi.org/10.18372/2410-7840.17.9515

12 Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks. *EUREKA: Physics and Engineering*, (1), 24-31. https://doi.org/10.21303/2461-4262.2021.001615

13 Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., & Biehun A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security* (IJCNIS), Vol. 13, No. 1, pp.1-14.