УДК: 004.9 DOI 10.33111/mise.102.11

Лютий О.І., к.тех.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Калганова В.І., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Стець К.М., магістрант ННІ «ІІТЕ»,
Київський національний економічний університет
імені Вадима Гетьмана

Liutyj O.I., Candidate of Technical Sciences, Associate Professor
of the Computer Mathematics and Information Security Department,
KNEU named after V. Hetman

Kalganova V.I., lecturer
of the Computer Mathematics and Information Security Department,
KNEU named after V. Hetman

Stets K.M., graduate student,
Institute of Information Technologies in Economics,
KNEU named after V. Hetman

МЕТОДИ ВИЗНАЧЕННЯ ВИТРАТ НА КІБЕРБЕЗПЕКУ

METHODS FOR DETERMINING CYBERSECURITY COSTS

Анотація. *У статті обговорюється проблема вартості збереження секретної інформації, а отже, проблема витрат на кібербезпеку в організації бізнесу в цілому. Звернено увага на фінансовий аспект організації системи кібербезпеки навколо бізнес-даних та інформації. Для того щоб ефективно вести бізнес у конкурентному середовищі, необхідно правильно керувати інформацією та даними підприємства. Особливо, якщо ця інформація є секретною і приносить підприємству велику користь у його діяльності. Для ефективного використання секретної інформації потрібно створити систему захисту і режим обмеження доступу до інформації чи її вільного розповсюдження, за якого ефект від використання інформації з урахуванням позитивних і негативних наслідків досягатиме максимального значення. Для порівняння інформації у контексті необхідності обмеження доступу до неї пропонується оцінювати інформацію за рівнем прояву всієї сукупності загроз у разі їх вільного поширення та можливих витрат на обмеження доступу до них та визначити ваги загроз, переваг і витрат для отримання єдиного показника, що характеризує інтегральний ефект від обмеження поширення інформації. Авторами запропоновано модель розрахунку значення інтегрального показника обра-*

ного способу розповсюдження інформації, який включає потенційно можливий розмір шкоди у разі поширення інформації, потенційно можливий розмір вигоди під час вільного розповсюдження інформації, ймовірність шкоди та користі протягом життєвого циклу інформації, витрати на захист інформації. Висвітлено зв'язок між витратами на захист інформації та потрібним рівнем захисту секретної інформації. Запропоновано авторську класифікацію витрат на забезпечення кібербезпеки підприємства.

Ключові слова: *інформація, витрати, кібербезпека, підприємство, секретність*

Abstract. *The article discusses the problem of cost for maintaining secret information and therefore, problematic of cybersecurity costs throughout business organization overall. Attention is drawn to the financial aspect of organization of cybersecurity system around business data and information. In order to effectively conduct business in a competitive environment, you need to properly manage the information and data of the enterprise. Especially if this information is secret and brings great benefits to the enterprise in its activities. In order to effectively use secret information, it is necessary to create a system of protection and a regime of restriction of access to information or its free distribution, in which the effect of using information, taking into account the positive and negative consequences, would reach the maximum value. To compare information from the point of view of the need to restrict access to it, it is proposed to evaluate the information by the degree of manifestation of the entire set of threats in case of their free dissemination and possible costs of restricting access to them and to determine the "weights" of threats, benefits and costs in order to obtain a single measure that characterizes the integral effect of restricting the dissemination of information. The author proposes a model for calculating the value of the integral indicator of the chosen mode of information dissemination, which includes the potentially possible amount of damage during the dissemination of information, the potentially possible amount of benefit during the free dissemination of information, the probability of harm and benefit during the life cycle of information, the cost of protecting information. Thus, the relationship between the costs of information protection and the required level of protection of classified information is highlighted. The author also proposes a classification of costs for ensuring cybersecurity of the enterprise.*

Keywords: *Information, costs, cybersecurity, enterprise, secrecy*

Постановка наукової проблеми та її значення. Питання наявності секретності інформації, усіх пов'язаних з цим технічних процесів та скорочення витрат на всіх видах підприємств, як державних, так і приватних, постає доволі гостро у реальності повномасштабної війни та постійних кібератак і маніпуляцій. В час, коли рішення повинні ухвалюватися достатньо швидко, система має бути вибудована ефективно. В стані постійного примусового зниження витрат, першочергово постає питання про оптимізацію процесів. Класифікація витрат, створення режимів поширення інформації у зв'язку з матеріальними ризиками щодо її поширення дозволять будь-яким підприємствам створити оптимальну систему захисту секретної інформації та оптимізувати фінансових аспект роботи служби кібербезпеки всередині організації.

Аналіз останніх досліджень і публікацій. Над розв'язанням проблеми економічного аспекту кібербезпеки на підприємстві працювали наступні вітчизняні науковці: М. Г. Романюков, О. А. Лаптієв, В. В. Собчук, А. В. Собчук, С. О. Лаптієв, Т. О. Лаптієв. Проте питання саме витратної частини системи захисту інформації залишається мало дослідженим.

Мета і завдання статті. Метою статті є осмислення проблематики витрат бізнесу на кіберзахист інформації з позицій рівня секретності інформації та потенційних втрат в разі її розповсюдження. Також теоретичне узагальнення та класифікація витрат на кіберзахист даних і створення моделі прорахунку інтегрального показника обраного режиму розповсюдження інформації. Досягнення поставленої мети передбачає вирішення таких завдань: класифікувати витрати підприємства на кіберзахист даних, проаналізувати взаємозалежність між фінансовими результатами та режимом розповсюдження інформації, створити якісну модель оцінки параметрів захисту інформації.

Виклад основного матеріалу. Секретність у ринковій економіці — економічна категорія. Інформація, яка захищається, повинна приносити певну користь її власнику і виправдовувати кошти, які витрачаються на її захист. Рівень секретності зазвичай з часом зменшується і рідше (історичні документи) збільшується. Тому рівень секретності має переглядатися. Інформація повинна залишатися конфіденційною доти, доки цього вимагають інтереси національної безпеки або комерційної діяльності підприємства.

Для найбільш ефективного використання інформації за час її життєвого циклу, протягом якого вона є актуальною, необхідно обрати такий режим її розповсюдження, за якого ефект від використання інформації з урахуванням позитивних та негативних наслідків досягав би максимальної величини. За такого підходу обмеження поширення інформації на певний час є одним із способів керування інформаційним ресурсом власника на користь досягнення максимального ефекту від його використання.

Слід враховувати, що оцінка позитивних і негативних наслідків від обмеження поширення інформації становить значні труднощі. Ці наслідки можуть виявлятися у різних сферах діяльності підприємства, оцінюватися у різних шкалах та одиницях виміру.

Для порівняння відомостей з позицій необхідності обмеження доступу до них пропонується:

• оцінити ці відомості за ступенем прояву всієї сукупності загроз у разі їх вільного поширення та можливих витрат (або втраченої вигоди) у разі обмеження доступу до них;

• ранжувати чи визначити ваги загроз, вигід і витрат з тим, щоб отримати єдину міру, яка характеризує інтегральний ефект від обмеження поширення відомостей (для вирішення цього завдання необхідно визначити переліки можливих загроз від несанкціонованого поширення інформації, вигід / переваг вільного поширення інформації та статей витрат на її захист);

• з урахуванням усіх цих факторів необхідно обрати такий режим розповсюдження інформації, який би на кінець періоду її активного життєвого циклу забезпечував би максимальний ефект від використання інформації.

Для визначення вагів збитків, вигід і витрат доцільно звернутись до допомоги експертів, які добре розуміють цінність відомостей та їх взаємозв'язок із зазначеними факторами. Можливість прояву різних факторів у динаміці життєвого циклу інформації оцінюється суб'єктивною ймовірністю.

На основі порівняльних оцінок окремих факторів з урахуванням можливості їх прояву обчислюється значення інтегрального показника обраного режиму розповсюдження інформації

$$W = U \times p - V \times q - Z, \qquad (1)$$

де U — потенційно можлива величина шкоди під час поширення відомостей; V — потенційно можлива величина вигоди при вільному розповсюдженні відомостей; p — ймовірність прояву шкоди під час життєвого циклу відомостей; q — ймовірність прояву вигоди в період життєвого циклу при вільному поширенню відомостей; Z — величина витрат за захист відомостей.

Якщо розраховане значення інтегрального показника виявляється більше від нуля, то включення аналізованої інформації до переліку відомостей, віднесених до інформації обмеженого доступу, доцільно.

Віднесення інформації до інформаційних ресурсів, що підлягають захисту від несанкціонованих і ненавмисних впливів, доцільно, якщо величина шкоди, яка запобігається при цьому, перевищує величину витрат на її захист.

Наочною ілюстрацією залежності параметрів та характеристик, що визначають умови захисту засекреченої інформації, може бути така модель (рис. 1).

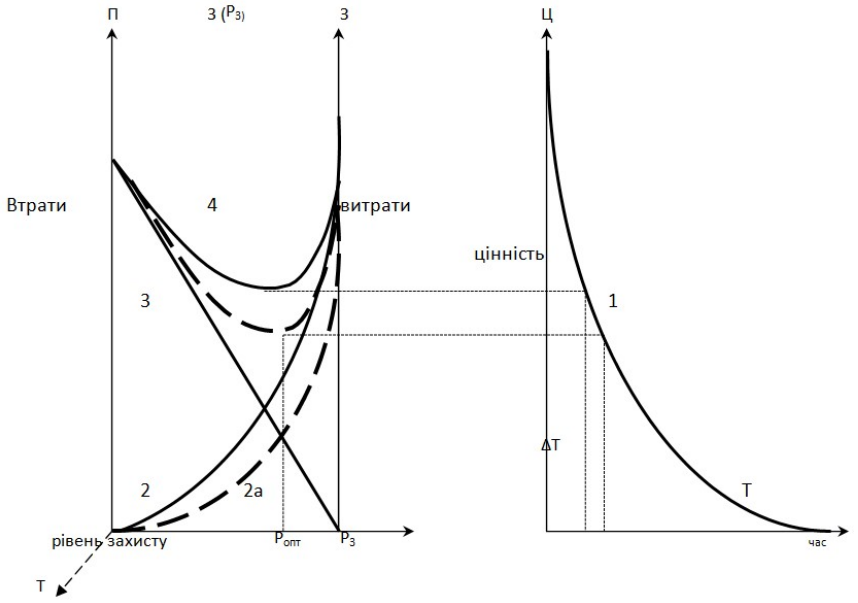

Рис. 1. Якісна модель завдання оцінки параметрів захисту інформації

На цій моделі показано якісний взаємозв'язок параметрів інформації, що охороняється, таких, як її цінність, необхідний рівень захисту, час збереження секретності, з одного боку, та економічних характеристик захисних заходів, таких як витрати на забезпечення захисту та можливі втрати внаслідок недосконалості системи захисту інформації, з другого. На рис. 1 показано, що Ц — цінність інформаційного ресурсу — об'єкта засекречення (наприклад, науково-технічного звіту, що містить опис нової перспективної технології); Т — час; Ц(Т) — характеристика старіння інформації — зменшення цінності інформаційного ресурсу з часом; РЗ — рівень (ймовірність) забезпечення захисту. На практиці РЗ <1, оскільки абсолютно надійний захист інформації навряд чи здійсненний; З(РЗ) — витрати на захист інформації як функція від необхідного рівня її захисту. Ці витрати зростають у разі підвищення вимог до рівня захисту. Прагнення досягти дуже високого рівня захисту зазвичай тягне за собою різке зростання витрат, які можуть перевищити цінність самої інформації, що захищається. П — ймовірні втрати внаслідок недосконалості захисту, які є функцією цінності інформації та реалізованого рівня її

захисту. У нульовому наближенні ці втрати апроксимуються добутком цінності інформації на ймовірність її витоку. Ймовірність витоку інформації перебуває у зворотній залежності до досягнутого рівня захисту. За такого допущення П ~ Ц(1 – р3).

Якщо сума З(Р3) + П(Р3) визначає витрати, пов'язані з засекречуванням інформації, то рівень захисту Ропт(З,П) відповідний на рис. 1 мінімум суми витрат на захист і ймовірнісних втрат внаслідок неповноти захисту інформації можна розглядати як оптимальний. Прагнення перевищити його призведе до різкого зростання витрат на забезпечення захисту інформації; зниження ж рівня захисту може призвести до збільшення втрат внаслідок її недосконалості.

Якщо вважати, що ΔТ — тимчасовий інтервал, протягом якого засекречення інформації може бути економічно виправдане (при цьому величина витрат на захист інформації в сумі з імовірнісними втратами менша за вартість засекречуваної інформації з урахуванням її старіння), то, як показано на рис. 1: ΔТmax = = ΔТ (Ц, Ропт(З, П)). Для спрощення ми нехтуємо залежністю З(ΔТ) — зростанням сумарних витрат на захист інформації, що засекречується, з часом, що можна було б легко проілюструвати, представивши ліву частину рис. 1 у тривимірних координатах.

Внаслідок того, що значення величини досягнутого рівня захисту інформації Р3 залежить як мінімум від двох параметрів: Rзі — використовуваних ресурсів (зокрема матеріальних витрат на забезпечення захисту) та Емзі — ефективності механізму захисту (використання цих ресурсів), у рамках цієї моделі можлива оптимізація.

Фактично Емзі — показник досконалості створеної та функціонуючої системи захисту інформації. За більш якісного проєктування та практичної реалізації механізму захисту — максимально ефективного залучення всіх ресурсів — той самий рівень забезпечення захисту інформації може бути досягнутий за менших матеріальних витрат. На рис. 1 це ілюструє крива 2*а*. Відповідно, при цьому про оптимальний рівень захисту інформації може бути вищим, а економічно виправдана тривалість засекречування ΔТ — більшою.

Витрати на забезпечення кібербезпеки підприємства можна поділити на одноразові та систематичні.

Одноразові витрати включають:

1) витрати формування ланки управління системою захисту інформації та інші організаційні витрати;

2) витрат на придбання та встановлення засобів захисту.

Систематичні витрати включають:

1. Витрати обслуговування системи кібербезпеки:

– витрати на здійснення технічної підтримки виробничого персоналу під час впровадження засобів захисту інформації;

– витрати на організацію системи допуску виконавців та співробітників конфіденційного діловодства;

– витрати на обслуговування та налаштування програмно-технічних засобів захисту, операційних систем, мережевого обладнання;

– витрати на організацію безпечного використання інформаційних систем;

– витрати на забезпечення безперебійної роботи системи захисту інформації.

2. Витрати на контроль роботи системи безпеки:

• витрати на контроль змін стану інформаційного середовища підприємства;

• витрати на контроль за діями персоналу;

• витрати на планові перевірки та випробування програмно-технічних засобів захисту інформації;

• витрати на проведення перевірок навичок персоналу підприємства з експлуатації засобів захисту;

• витрати на контроль правильності введення даних до прикладних систем;

• оплата праці інспекторів з контролю вимог, які пред'являються до захисних засобів, що забезпечують управління захистом комерційної таємниці.

3. Витрати на забезпечення належної якості інформаційних технологій та їх відповідності вимогам стандартів:

– витрати на забезпечення відповідності вимогам якості інформаційних технологій;

– витрати на забезпечення відповідності прийнятим стандартам та вимогам достовірності інформації, дієвості засобів захисту;

– витрати на доставку та обмін конфіденційної інформації;

– Витрати задоволення суб'єктивних вимог користувачів: стиль, зручність інтерфейсів.

4. Витрати на підвищення кваліфікації персоналу у питаннях використання наявних засобів захисту, виявлення та запобігання загрозам безпеки.

5. Витрати, пов'язані з переглядом політики кібербезпеки підприємства:

• витрати на ідентифікацію загроз безпеки;

• витрати на пошук вразливості системи захисту інформації;

• оплата роботи фахівців, які виконують роботи з визначення можливої шкоди та переоцінки ступеня ризику;

• витрати на використання додаткових засобів захисту інформації.

6. Витрати на ліквідацію наслідків порушення режиму кібербезпеки:

– витрати на відновлення системи безпеки до відповідності вимогам політики безпеки.

– витрати на придбання нових технічних засобів;

– витрати на утилізацію ресурсів, що прийшли в непридатність;

– витрати на відновлення баз даних та інших інформаційних ресурсів;

– витрати на проведення заходів щодо контролю достовірності даних, які зазнали атаки на цілісність;

– витрати на проведення додаткових випробувань та перевірок інформаційних систем;

– витрати на проведення розслідувань порушень безпекової політики;

– витрати на юридичні спори та виплати компенсацій;

– витрати, що виникли внаслідок розриву ділових відносин із партнерами.

7. Витрати, що виникають внаслідок втрати новаторства:

• витрати на проведення додаткових досліджень та розробки нової ринкової стратегії для підприємства у зв'язку з відмовою від організаційних, науково-технічних, комерційних рішень, які стали неефективними внаслідок витоку відомостей;

• витрати, що виникли через зниження пріоритету в наукових дослідженнях та неможливість патентування та продажу ліцензій на науково-технічні досягнення.

Класифікація витрат умовна, оскільки детальна розробка переліку залежить від особливостей конкретної організації та її систем захисту кібербезпеки.

Зазвичай неминучі витрати, які необхідно враховувати навіть тоді, коли рівень загроз безпеки досить низький, включають такі статті:

– обслуговування технічних засобів захисту;

– конфіденційне діловодство;

– функціонування та аудит системи безпеки;

– мінімальний рівень перевірок та контролю із залученням спеціалізованих організацій;

– навчання персоналу методам кібербезпеки.

За дотримання політики безпеки та проведення профілактичних заходів можна виключити або суттєво знизити такі витрати:

• на відновлення системи безпеки до відповідності вимогам політики безпеки;

• на відновлення ресурсів інформаційного середовища підприємства;

• на переробки всередині системи безпеки;

• на юридичні спори та виплати компенсацій;

• на виявлення причин порушення політики безпеки.

Вихідні постановки завдань захисту державної та комерційної таємниці можна подати, як показано в табл. 1.

Таблиця 1

ВИХІДНІ УМОВИ ЗАВДАНЬ ЗАХИСТУ ДЕРЖАВНОЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Параметри				
Об'єкти захисту	Цінність інформації	Необхідний рівень захисту інформації	Витрати захисту засекреченої інформації	Тривалість секретності
Державна таємниця	Визначається державою	Встановлюється державою (високий)	Визначаються безумовною необхідністю забезпечення необхідного рівня захисту інформації	Визначаються у відповідності з нормами законодавства про державну таємницю
Комерційна таємниця	Суб'єктивна оцінка власника інформації	Оптимальний	Гранично допустимі для власника комерційної таємниці з обліком прийнятного для нього ризику	Може бути змінена власником

В умовах стабільної економіки державне замовлення для підприємця із засекречення інформації виглядає пріоритетним, оскільки воно не пов'язане з ринковим ризиком реалізації продукції. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Зазначені витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею. Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому Законом України «Про державну таємницю» [1].

Вимоги до умов та рівня захисту задаються державними нормативними документами та є імперативними.

Власник комерційної таємниці зацікавлений у максимально високому рівні захисту своєї комерційної таємниці та мінімізації витрат на її захист. Це вимагає визначення їм допустимого ризику та пошуку оптимального рішення.

Висновки та перспективи подальшого дослідження. Нині питання оптимального використання фінансових ресурсів постає достатньо важливим за умови постійного скорочення фінансування та зменшення бюджетів. Також в реаліях повномасштабної російсько-української війни потрібно зважено вибирати режим розповсюдження і надання доступу до секретних даних та матеріалів як на приватному підприємстві, так і в державних структурах. Хоча загалом зараз на всіх підприємствах існують служби кібербезпеки, або працюють хоча б кілька спеціалізованих фахівців, втім загального підходу для менеджменту взаємодії між витратами на захист інформації та необхідним рівнем захисту інформації з обмеженим доступом немає серед індустрії.

Класифікація витрат, створення режимів поширення інформації у зв'язку з матеріальними ризиками щодо її поширення дозволять будь-яким підприємствам створити оптимальну систему захисту секретної інформації та оптимізувати фінансових аспект роботи служби кібербезпеки всередині організації.

Бібліографічні посилання

1. Про державну таємницю: Закон України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

2. Про основні засади забезпечення кібербезпеки України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Центрального управління Служби безпеки України від

23 грудня 2020 р. № 383. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#n7
4. Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8
5. Про інформацію: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Про електронні документи та електронний документообіг: Закон України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
7. Про національну безпеку України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
8. Контроль за законністю заходів із кібербезпеки України. Ст. 15 КУ. URL:https://protocol.ua/ua/pro_osnovni_zasadi_zabezpe_vid_05_10_2017_2163_viii_stattya_15/
9. Меморандум про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту. URL: https://interacademy.info/ekspert-mizhnarodnoi-akademii-informatsii-vziav-uchast-u-pidpysanni-memorandumu-pro-vzaiemodiiu/
10. ISO/IEC27000:2019 — Інформаційні технології — Методи і засоби забезпечення безпеки — Системи управління інформаційною безпекою — Загальні відомості і словник.
11. ISO/IEC 27001:2013 — Інформаційні технології — Методи захисту — Системи управління інформаційною безпекою — Вимоги
12. ISO/IEC 27002:2013/COR 2:2015 — Інформаційні технології — Методи захисту — Звіт рекомендованих правил для управління інформаційною безпекою
13. ISO/IEC 27005:2018 — Інформаційні технології — Методи безпеки — Управління ризиками інформаційної безпеки
14. ISO 27035 — Управління інцидентами
15. Рекомендація КОМІСІЇ (ЄС) 2017/1584 від 13 вересня 2017 року про скоординоване реагування на великомасштабні інциденти і кризи в області кібербезпеки
16. Постанова 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 р. про ENISA (Агентство Європейського Союзу з кібербезпеки) і про сертифікацію кібербезпеки інформаційних і комунікаційних технологій і скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку)
17. Валюшко І.О. Кібербезпека України: наукові та практичні виміри сучасності. URL: http://visnyk-psp.kpi.ua/article/view/140496/137578
18. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S., & Laptieva, T. (2021). Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/249

Статтю подано до редакції 29.11.2022