УДК 621.391

МАТЕМАТИЧНА МОДЕЛЬ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПРОЕКТУВАННІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ НА ОБ'ЄКТІ ІНФОРМАТИЗАЦІЇ

С.В. Пшеничних, І.С. Добринін, Д.Ю. Клочкова
Харківський національний університет радіоелектроніки

Abstract *– This article addresses and resolves the problem of optimal selection of information security measures in the face of security threats when designing a comprehensive information security system for an informatization facility. An analysis of existing approaches to assessing the effectiveness of information security systems is conducted, and a mathematical model for the optimal selection of security measures is proposed. To choose security measures, a new efficiency metric is suggested, which takes into account the costs of implementation and operation of a given measure and its ability to simultaneously protect against multiple threats. Based on this metric, a criterion for the optimal selection of security measures against security threats is proposed for each specific information resource in the information system. The article presents an algorithm for the optimal selection of a set of security measures for an information system, implementing a simple search method. The mathematical formulation of the problem is carried out for the purpose of optimization based on the maximum criterion of the proposed efficiency metric. The optimization of the entire set of security measures is performed based on the maximum criterion of the integral efficiency metric. To demonstrate the use of the pro-posed model, the article considers an example of the optimal selection of a set of security measures for a computer network in the presence of three security threats and the availability of five available security measures. The proposed model can be used to optimize the composition of a set of security measures at informatization facilities. The prerequisite for the application of this model is the availability of input data in the form of threat models to information resources and information about available security measures, namely their capabilities in preventing threats and the cost of their acquisition, implementation, and operation.*

Анотація – У статті розглядається та вирішується задача оптимального вибору засобів захисту інформації від загроз безпеки при проектуванні комплексної системи захисту інформації на об'єкті інформатизації. Проводиться аналіз наявних підходів до оцінки ефективності систем захисту інформації і пропонується математична модель оптимального вибору складу засобів захисту. При цьому для вибору засобів захисту пропонується використовувати новий показник ефективності, який дозволяє враховувати витрати на впровадження та експлуатацію даного засобу та його можливості з одночасним захистом від декількох загроз. На основі цього показника пропонується критерій оптимального вибору засобів захисту від загроз безпеки для кожного конкретного інформаційного ресурсу інформаційної системи. У статті запропонований алгоритм оптимального вибору складу комплексу засобів захисту для інформаційної системи, який реалізує метод простого пошуку. Математична постановка задачі виконана для оптимізації вибору на основі критерія максимуму запропонованого показника ефективності. Оптимізація всього комплексу засобів захисту здійснюється на основі критерія максимуму інтегрального показника ефективності. Для демонстрації використання запропонованої моделі в статті розглядається приклад оптимального вибору складу засобів захисту для комп'ютерної мережі за наявності трьох загроз безпеці та наявністю п'яти доступних засобів захисту. Пропоновану модель можна використовувати для оптимізації складу комплексу засобів захисту на об'єктах інформатизації. Необхідною умовою застосування цієї моделі є наявність вихідних даних у формі моделі загроз інформаційним ресурсам та даних про доступні засоби захисту, а саме їхні можливості щодо запобігання загрозам та вартість їх придбання, впровадження та експлуатації.

Вступ

На даний час одним із найважливіших завдань оптимальної побудови комплексної системи захисту інформації на об'єкті інформатизації (ОІ) є вибір із множини наявних засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх по-

тенційно можливих інформаційних загроз із найкращою якістю та мінімально можливими витраченими на це ресурсами.

Відомо, що найефективніше завдання вибору засобів захисту інформації вирішуються під час проектування комплексної системи захисту інформації (КСЗІ), коли оцінюються потенційно можливі загрози та обираються адекватні механізми захисту від них. При цьому на етапі проектування системи захисту інформації розробник, не маючи статистичних даних про результати функціонування створюваної системи, змушений приймати рішення про склад комплексу засобів захисту інформації, перебуваючи в умовах апріорної невизначеності. Тим не менш, методологія проектування систем захисту інформації має надавати можливість реалізації запобіжної стратегії захисту.

На сьогоднішній день методичне забезпечення щодо комплектування КСЗІ засобами захисту для ОІ, у тому числі для телекомунікаційних систем, сформовано недостатньо повно. Зазвичай, згідно з чинними нормативними документами щодо побудови КСЗІ вибір необхідного комплексу засобів захисту (КЗЗ) для забезпечення функціонування даної системи здійснюється відповідно до категорії об'єкта [1, 2]. Але побудова КСЗІ на основі використання нормативного підходу не дозволяє говорити про її оптимальність, тому що не визначається ефективність та не враховується вартість конкретних механізмів захисту.

Таким чином, завдання розвитку та розробки методичного забезпечення щодо оптимального вибору складу КЗЗ на етапі проектування КСЗІ на ОІ є актуальним.

І. Чинні підходи до оцінки ефективності комплексної системи захисту інформації

Ефективність системи – це властивість системи, що характеризує її здатність тією чи іншою мірою виконувати свою цільову функцію. Для оцінки ефективності системи необхідно визначити якісні та кількісні показники ефективності, а також необхідно визначити інтегральний показник ефективності системи в цілому.

Для того, щоб можна було порівняти різні варіанти КСЗІ щодо їхньої ефективності, необхідно на основі наявних показників ефективності виробити деяке правило переваги – критерій ефективності. Ефективність КСЗІ оцінюється як на етапі розробки, так і під час її експлуатації. При оцінці ефективності КСЗІ залежно від використовуваних показників та методів їх отримання можна виділити три підходи:

– класичний;
– нормативний;
– експериментальний.

При класичному підході для оцінки ефективності КСЗІ та отримання критерію ефективності за умов використання деякої множини n показників використовують ряд методів.

1) Метод головного критерію. Сутність методу головного критерію полягає у виділенні головного критерію, який значно перевершує за важливістю всі інші (на практиці втричі і більше разів). Потім розраховується його максимальне значення за умови, що інші критерії не менші за деякі гранично допустимі значення.

2) Методи, що засновані на ранжируванні показників за важливістю. При порівнянні систем однойменні показники ефективності зіставляються в порядку зменшення їхньої важливості за певними алгоритмами. По суті, при використанні даного підходу здійснюється скорочення числа альтернатив у вихідній множині, при якій виключаються свідомо погані альтернативи.

3) Мультиплікативні та адитивні методи отримання критеріїв ефективності, які ґрунтуються на об'єднанні всіх або частини показників за допомогою операцій множення або додавання до узагальнених показників.

4) Метод Парето: під час використання n показників ефективності системі відповідає точка в n-вимірному просторі. У n-вимірному просторі будується область парето-оптимальних рішень, для яких поліпшення будь-якого показника неможливе без погіршення інших показників ефективності. Вибір найкращого рішення з поміж парето-оптимальних може здійснюватися за різними правилами.

Незважаючи на певну кількість альтернативних методів, класичні підходи передбачають формування цільової функції $F(X)$ та її максимізацію на просторі наявних альтернатив A:

$$F\left(X\right) \to \max,\ X \in A\,. \tag{1}$$

Нормативний підхід не передбачає вирішення багатокритеріальних оптимізаційних задач і ґрунтується виключно на використанні нормативних документів та актів із питань побудови КСЗІ, де зазначаються вимоги до захищеності інформації різних категорій конфіденційності та важливості. Вимоги задаються переліком механізмів захисту інформації, які необхідно мати у КСЗІ, щоб вона відповідала певному стандартному функціональному профілю захищеності. Таким чином, критерієм ефективності КСЗІ є її клас захищеності. Безперечною перевагою такого нормативного підходу є простота використання. Його основним недоліком є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності чи відсутності. Крім того, не враховуються витрати на впровадження та експлуатацію засобів захисту. Цей недолік певною мірою компенсується заданням у деяких документах докладних вимог до цих механізмів захисту.

Під експериментальним підходом розуміється організація процесу визначення ефективності наявних засобів КСЗІ шляхом спроб подолання захисних механізмів системи фахівцями, які виступають у ролі зловмисників. За такої умови складається план проведення експерименту, у якому визначаються черговість та матеріально-технічне забезпечення проведення експериментів щодо визначення слабких ланок у сис-

темі захисту. Служба безпеки до моменту подолання захисту зловмисниками має запровадити в КСЗІ нові механізми захисту (змінити старі), щоб уникнути «зламування» системи захисту.

З огляду на те, що засоби безпеки мають обмежені можливості щодо протидії загрозам, завжди існує ймовірність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї ймовірності мають проводитися додаткові дослідження. У методичному плані визначення ефективності КСЗІ повинне полягати у виробленні судження щодо придатності способу дій персоналу чи пристосованості технічних засобів до досягнення мети захисту на основі вимірювання відповідних показників при функціональному тестуванні.

Ефективність оцінюється для вирішення таких задач:

– ухвалення рішення про допустимість практичного використання КСЗІ в конкретній ситуації;
– виявлення впливу різних факторів у досягнення мети;
– встановлення шляхів підвищення ефективності КСЗІ;
– порівняння альтернативних варіантів систем.

Вирішенням проблеми оцінювання ефективності КСЗІ може стати використання системного підходу, який дозволить ще на стадії проектування КСЗІ кількісно оцінити рівень безпеки та надати умови для ефективного управління ризиками. Однак цей шлях може бути реалізований за наявності відповідної системи показників та критеріїв.

Високий ступінь невизначеності вихідних даних при проектуванні КСЗІ є причиною того, що її ефективність не може бути адекватно виражена та описана детермінованими показниками. Тому об'єктивною характеристикою якості КСЗІ може бути лише ймовірність, яка характеризує ступінь відповідності системи, що оцінюється, своєму призначенню – досягненню необхідного рівня безпеки в умовах реального впливу випадкових факторів при заданому комплексі умов. Така характеристика називається ймовірністю виконання завдання системою. Ця ймовірність має бути покладена в основу комплексу показників та критеріїв оцінки ефективності КСЗІ. При цьому критеріями оцінки є поняття придатності та оптимальності. Придатність означає виконання всіх встановлених до КСЗІ вимог, а оптимальність - досягнення однієї з характеристик екстремального значення при дотриманні обмежень та умов інших властивостей системи. При виборі конкретного критерію необхідне його узгодження з метою КСЗІ.

У ряді робіт, що присвячені питанням оцінки ефективності захисту інформації в якості показника ефективності, розглядається залишковий ризик — величина збитку R з урахуванням ймовірності реалізації події, що призводить до збитку

$$R = \sum_{k=1}^{K} P_k \cdot C_k , \qquad (2)$$

де P_k – ймовірність реалізації k-ї загрози після встановлення певного варіанту КЗЗ; C_k – величина збитку від реалізації k-ї загрози; K – кількість загроз.

Величини P_k та C_k визначаються методом експертних чи аналітичних оцінок. Розмір збитку є випадковою величиною з функцією розподілу $F(C)$, де $C \in [0, \infty)$, а як міру збитку у виразі (2) приймають математичне очікування величини збитку.

Часто при визначенні ризику враховують витрати на реалізацію захисних заходів – S. У цьому випадку вираз (2) перетворюється у такий вигляд:

$$R = \sum_{k=1}^{K} P_k \cdot (C_k + S_k), \tag{3}$$

де S_k – вартість реалізації захисних механізмів від k-ї загрози.

Однак за такого підходу витрати на впровадження та експлуатацію засобів захисту прирівнюються до збитків від реалізації загрози, що не завжди є коректним.

У роботі [3], як показник ефективності розробки КСЗІ використовується величина, яка дорівнює різниці між збитками, які вдалося запобігти та витратами на впровадження та експлуатацію засобів безпеки:

$$E = \sum_{k=1}^{K} \left(C_k^0 - C_k^* \right) - \sum_{b=1}^{B} \left(S_b^{вп} + S_b^{ек} \right), \tag{4}$$

де E – ефективність розробки КСЗІ; C_k^0 – величина збитків від реалізації k-ї загрози до впровадження КСЗІ; C_k^* – величина збитків від реалізації k-ї загрози після впровадження КСЗІ; B – кількість засобів захисту; $S_b^{вп}$ – витрати на впровадження b-го засобу захисту; $S_b^{ек}$ – витрати на експлуатацію b-го засобу захисту.

Аналіз показав, що за такого підходу не враховуються ймовірності реалізації загроз, що не дозволяє оптимальним чином вибрати адекватні методи і засоби захисту. Доцільно таким чином формувати КЗЗ, щоб витрати на безпеку були адекватні потенційним загрозам. Подібна ситуація визначає необхідність оцінювання та врахування ймовірностей реалізації загроз.

II. Визначення показника ефективності та критерію оптимальності комплексної системи захисту інформації

Оцінювання ймовірності реалізації загроз та пов'язана з цим оцінка можливих втрат – найскладніша та найвідповідальніша частина всього процесу забезпечення безпеки. Від того, наскільки повно виявлені реальні та прогнозовані (потенційні) загрози, залежить ступінь захищеності об'єкта. З іншого боку, свідоме перевищення достатності при врахуванні тих загроз, вплив яких безпосередньо на функціонування об'єкта малоймовірний або локалізація яких неможлива або малоефективна, призведе до значного підвищення витрат на безпеку і може суттєво позначитися на реально досягненій економічній ефективності захисту.

Звідси постає завдання оптимізації рівня захищеності об'єкта від загроз, що дозволяє досягти максимальної ефективності обраного варіанта комплексу захисних заходів. При цьому необхідно враховувати дуже важливе обмеження: незважаючи на видиму пряму залежність між обсягом ресурсів, виділених на захист і ефективністю захисту, існує максимально припустима величина витрат, що визначається прибутковістю проектованої системи захисту – нормою прибутку на інвестовані в неї кошти. Підвищення рентабельності захисту можливе як завдяки обґрунтованій економії витрат на його організацію і експлуатацію, так і завдяки їхньому оптимальному розподілу в просторі загроз.

Що стосується комп'ютерних мереж, то їхня вразливість суттєво перевищує вразливість автономних комп'ютерів. Це пов'язано, перш за все, з відкритістю, масштабністю та неоднорідністю самих комп'ютерних мереж. Існує чимало способів атак на сучасні комп'ютерні мережі [4-10]. При цьому кількість загроз інформаційній комп'ютерній безпеці та способів їхньої реалізації постійно збільшується. Основними причинами тут є недоліки сучасних інформаційних технологій, а також неухильне зростання складності програмно-апаратних засобів.

Для ефективного вирішення завдання захисту інформації в комп'ютерній мережі необхідний ретельний аналіз усіх можливих загроз інформаційної безпеки, що дозволить своєчасно прийняти заходи протидії загрозам. При аналізі загрози необхідно оцінити можливість її прояву, а також збитки, які будуть завдано підприємству в разі незапобігання загрози.

Для протидії одній і тій самій загрозі зазвичай існує кілька засобів захисту, які випускаються різними виробниками, розрізняються за вартістю реалізації та забезпечують різну можливість запобігання загрозам. У найпростішому випадку можна було б припустити, що кожен засіб захищає від однієї загрози. Але в реальних умовах ринок засобів інформаційної безпеки надає засоби захисту, які протидіють довільній кількості загроз, причому можливість запобігання кожній загрозі різна.

Математична модель оптимального вибору методів та засобів захисту від загроз *для* кожного інформаційного ресурсу на ОІ надає можливість економічно обґрунтувати склад комплексу спеціальних технічних засобів *для* КСЗІ в цілому. Критерієм оптимальності цієї композиції може бути обрана сума середніх втрат від реалізації загроз та витрат на систему захисту.

Припустимо, що на ОІ виявлено *M* критичних інформаційних ресурсів. *Для* кожного ресурсу визначені загрози та вразливості та існує набір засобів захисту $X = \{X_1, X_2, ..., X_B\}$. Задача полягає в виборі складу засобів захисту відповідно до певного критерію оптимальності.

Позначимо ймовірність реалізації *k*-ї загрози щодо *m*-го ресурсу у випадку, якщо не використовуються засоби захисту, як P_{km}, і збиток компанії від її реалізації – C_{km}. Тоді ризик від реалізації *k*-ї загрози (R_{km}) дорівнює

$$R_{km} = P_{km} \cdot C_{km}. \quad (5)$$

Після впровадження засобу захисту X_i величина ризику стане рівною

$$R_{km}(X_i) = P_{km}(X_i) \cdot C_{km}. \quad (6)$$

Якщо захисні характеристики засобів задаються можливостями запобігання загрозі, то ймовірність реалізації загрози при впровадженому засобу захисту буде визначатися сумісною ймовірністю

$$P_{km}(X_i) = P_{km} \cdot (1 - U_{km}(X_i)), \quad (7)$$

де $U_{km}(X_i) = \{0, \ldots, 1\}$ – можливість запобігання загрози, яка забезпечується засобом X_i. Тобто, якщо засіб не забезпечує запобігання загрози ($U_{km}(X_i) = 0$), то ймовірність її реалізації не змінюється. І навпаки, якщо засіб гарантує абсолютне запобігання загрози ($U_{km}(X_i) = 1$), то ймовірність реалізації цієї загрози дорівнює 0.

З урахуванням вартості цього засобу захисту X_i пропонується використовувати наступний показник ефективності:

$$E_{km}(X_i) = \left(\frac{R_{km} - R_{km}(X_i)}{R_{km}} \cdot 100\% \right) - \left(\frac{S_i}{R_{km}} \cdot 100\% \right). \quad (8)$$

Цей показник відображає зменшення ризику для m-го інформаційного ресурсу (у грошовому еквіваленті) завдяки використанню засобу захисту в разі реалізації k-ї загрози відносно ресурсу, що захищається, з урахуванням вартості заходу щодо захисту (з урахуванням вартості обладнання, його встановлення та експлуатації).

Однак у (8) не враховується те, що один і той самий засіб може забезпечувати захист інформації відразу від кількох загроз. Але це можна врахувати при обчисленні параметру $E_{km}(X_i)$ таким чином:

$$E_{km}(X_i) = \left(\frac{R_{km} - R_{km}(X_i)}{R_{km}} \cdot 100\% \right) - \left(\frac{S_i \cdot A_{im}}{R_{km}} \cdot 100\% \right), \quad (9)$$

де A_{im} – булева змінна, яка вказує на повторне використання засобу захисту X_i. Якщо $A_{im} = 1$, то засіб захисту вибирається перший раз, інакше $A_{im} = 0$. Результатом цього буде підвищення значення параметру $E_{km}(X_i)$.

Завданням оптимізації є вибір такого засобу захисту із множини $X = \{X_1, X_2, ..., X_B\}$, для якого виконується умова:

$$X_{km}^{opt} = \arg\max E_{km}(X_i), \quad (10)$$

де X_{km}^{opt} – оптимальний засіб захисту інформації при реалізації *k*-ї загрози щодо *m*-го ресурсу, що захищається, $E_{km}(X_i)$ – показник ефективності засобу захисту (X_i) при реалізації *k*-ї загрози щодо *m*-го ресурсу, який захищається.

Іншими словами, цей засіб повинен забезпечувати максимальне зменшення ризику при мінімальних витратах. У деяких випадках максимальне значення параметра $E_{km}(X_i)$ може приймати значення близькі до нуля, що є прийнятним. Однак, якщо максимальне значення параметра оптимізації набуває негативних значень, це свідчить про перевищення витрат і необхідність використання більш дешевих засобів та методів захисту.

Загалом для комплексу засобів захисту *M* інформаційних ресурсів, які виявлені на ОІ в ході попереднього обстеження (інвентаризації) для множини загроз $Y=\{Y_1, Y_2, \ldots, Y_K\}$, вираз для показника ефективності можна записати в наступному вигляді:

$$E(X)=\sum_{m=1}^{M}\sum_{k=1}^{K}E_{km}(X_i). \qquad (11)$$

Розв'язком оптимізаційної задачі для КСЗІ буде склад комплексу засобів захисту $X=\{X_1, X_2, ..., X_B\}$, для якого буде виконуватись умова:

$$X_{opt}=\arg\max E\left(X, Y, P, C, S\right), \qquad (12)$$

де $P=\{P_1, P_2, \ldots, P_K\}$ – ймовірності реалізації загроз, $C=\{C_1, C_2, \ldots, C_K\}$ – збитки від реалізації загроз, $S=\{S_1, S_2, \ldots, S_B\}$ – вартості реалізації засобів захисту.

Згідно з критерієм (12), оптимальний КЗЗ повинен забезпечувати максимальне зменшення ризику при мінімальних витратах на його впровадження та експлуатацію.

III. Алгоритм оптимального вибору засобів захисту інформації

Алгоритм оптимізації складу КЗЗ відповідно до запропонованої математичної моделі наданий у вигляді блок-схеми на рис. 1.

Принцип дії алгоритму полягає в наступному:

–на кроці 2 визначаються інформаційні ресурси на ОІ, що підлягають захисту;

–на кроці 3 визначаються доступні засоби захисту та вартість їх впровадження й експлуатації;

–на кроці 4 визначаються наявні загрози для кожного ресурсу, ймовірності їх реалізації P_{km} та можливі збитки C_{km} від їхньої реалізації;

–на кроці 5 вибирається один із інформаційних ресурсів *m*, що є на ОІ;

–на кроці 6 обирається одна із загроз для ресурсу *m*, ймовірність її реалізації P_{km} та можливі збитки C_{km} від її реалізації;

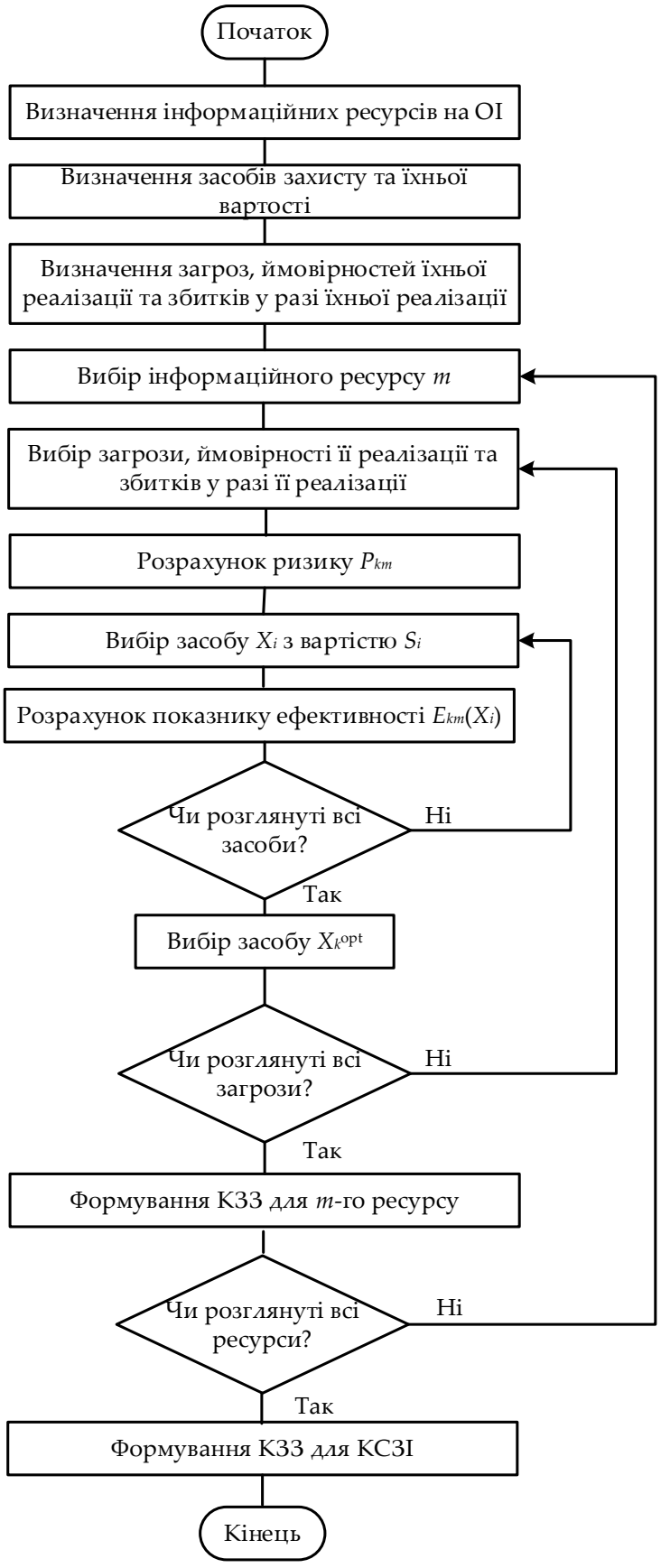

Рис. 1. Блок-схема алгоритму формування комплексу засобів захисту

–на кроці 7 розраховується ризик R_{km} (5);

–на кроці 8 обирається один із доступних засобів захисту інформації X_i із відповідній йому вартістю впровадження та експлуатації S_i для запобігання *k*-ї загрози для ресурсу *m*;

–на кроці 9 розраховується показник ефективності $E_{km}(X_i)$ для вибраного засобу захисту за виразом (9);

–на кроці 10 циклічно перевіряється наявність альтернативних засобів захисту для запобігання тієї ж загрози. При їх наявності для кожного засобу розраховується показник ефективності $E_{km}(X_i)$;

–на кроці 11 із наявних засобів захисту вибирається той, що відповідає критерію оптимальності (10);

–на кроці 12 здійснюється перехід до інших загроз безпеці інформації для того ж ресурсу *m*, і, таким чином, обираються оптимальні засоби захисту для запобігання цим загрозам;

–на кроці 13 здійснюється формування оптимального комплексу засобів захисту для запобігання загроз безпеки для ресурсу *m*;

–на кроці 14 здійснюється перехід до інших інформаційних ресурсів для кожного з яких вибираються засоби захисту відповідно до критерія оптимальності (10). Для кожного з них формується КЗЗ для запобігання всім загрозам безпеки.

Якщо процедурою формування КЗЗ були охоплені всі інформаційні ресурси, що були виявлені на ОІ, то на кроці 15 остаточно формується КЗЗ для КСЗІ на ОІ. Оптимальність складу КЗЗ перевіряється за критерієм (12).

IV. Приклад оптимального вибору складу засобів захисту від загроз безпеки у комп'ютерній мережі підприємства

Для демонстрації використання запропонованої математичної моделі розглянемо невеликий приклад, що показує її практичне застосування. В якості об'єкту інформатизації в даному випадку візьмемо комп'ютерну мережу підприємства на періоді її функціонування *T*=1 рік. Для прикладу розглянемо три загрози безпеки та п'ять засобів захисту. У реальних системах кількість загроз та можливих для їх запобігання засобів захисту може досягати кількох десятків і більше.

У табл. 1 наведено три типові загрози для комп'ютерної мережі підприємства (реально їх набагато більше). Можливості прояву загроз вибрано на основі статистичних досліджень. Дані про середні збитки від можливого запобігання загрозам безпеці сильно залежать від специфіки діяльності компанії та обрані на основі деяких середніх показників для типового підприємства.

У табл. 2 наведено характеристики п'яти засобів захисту від загроз безпеці. Вартість реалізації засобів захисту обрано на основі припущення про наявність у компанії 200 робочих станцій та 5 файлових серверів. Можливість запобігання загроз вибрана на основі експертних оцінок.

Таблиця 1. Можливі загрози безпеці та можливі збитки від їхньої реалізації на інтервалі часу один рік

Загроза	Ймовірність реалізації	Можливі збитки від реалізації, грн.	Ризик від реалізації, грн.
Несанкціоноване вторгнення в мережу (загроза 1)	0,6	2000000	1200000
Вірусна атака (загроза 2)	0,9	400000	360000
Витік конфіденційної інформації (загроза 3)	0,8	3000000	2400000

Таблиця 2. Засоби захисту від загроз безпеки, вартості їхньої реалізації та можливості запобігання загрозам на інтервалі часу один рік

Засіб захисту	Вартість реалізації, грн.	Можливість запобігання загрозі		
		несанкціонованого вторгнення в мережу	вірусної атаки	витоку конфіденційної інформації
ESET NOD32 Antivirus (засіб 1)	325680	0	0,8	0
Fortinet FortiGate 100F (засіб 2)	258375	0,7	0,4	0
Symantec Antivirus Enterprise (засіб 3)	580000	0	0,9	0,7
Outpost Network Security (засіб 4)	364122	0,8	0,5	0,6
Kerio WinRoute Firewall (засіб 5)	158000	0,7	0,3	0,7

Таблиця 3. Результати розрахунків для загрози 1 (C=2000000 грн.)

Засіб захисту	$S(X)$, грн	$U(X)$	P_1	$P_1(X)$	R_1, грн	$R_1(X)$, грн	$E_1(X)$, %
Засіб 1	325680	0	0,6	0,6	1200000	1200000	-27,14
Засіб 2	258375	0,7	0,6	0,18	1200000	360000	48,469
Засіб 3	580000	0	0,6	0,6	1200000	1200000	-48,333
Засіб 4	364122	0,8	0,6	0,12	1200000	240000	49,657
Засіб 5	158000	0,7	0,6	0,18	1200000	360000	56,833

Таблиця 4. Результати розрахунків для загрози 2 (С=400000 грн.)

Засіб захисту	$S(X)$, грн.	$U(X)$	P_2	$P_2(X)$	R_2, грн	$R_2(X)$, грн	$E_2(X)$, %
Засіб 1	325680	0,8	0,9	0,18	360000	72000	-10,467
Засіб 2	258375	0,4	0,9	0,54	360000	216000	-31,771
Засіб 3	580000	0,9	0,9	0,09	360000	36000	-71,111
Засіб 4	364122	0,5	0,9	0,45	360000	180000	-51,145
Засіб 5	158000	0,3	0,9	0,63	360000	252000	-13,889

Таблиця 5. Результати розрахунків для загрози 3 (С=3000000 грн.)

Засіб захисту	$S(X)$, грн.	$U(X)$	P_3	$P_3(X)$	R_3, грн	$R_3(X)$, грн	$E_3(X)$, %
Засіб 1	325680	0	0,8	0,8	2400000	2400000	-13,57
Засіб 2	258375	0	0,8	0,8	2400000	2400000	-10,766
Засіб 3	580000	0,7	0,8	0,24	2400000	720000	45,833
Засіб 4	364122	0,6	0,8	0,32	2400000	960000	44,828
Засіб 5	158000	0,7	0,8	0,24	2400000	720000	63,417

Аналіз результатів розрахунків (табл. 3) показує, що для запобігання першої загрози оптимальним є засіб захисту 5. Із табл. 4 видно, що для другої загрози показники ефективності для всіх наявних засобів мають негативні значення. Це говорить про перевищення витрат на засоби захисту для запобігання цій загрозі та необхідності пошуку більш дешевших засобів. Тим не менш, серед наявних засобів оптимальним є засіб захисту 1. Із табл. 5 видно, що для запобігання загрози 3 оптимальним є засіб захисту 5. Таким чином, даний засіб захисту є оптимальним для запобігання відразу двох загроз – загрози 1 і загрози 3.

Це враховується при розрахунку інтегрального показника ефективності КЗЗ (11). Вартість засобу 3 згідно з (9) повторно не враховується ($A_3 = 0$). Інтегральний показник ефективності (11) для КЗЗ, що складається з двох засобів (засіб 1 і засіб 5) приймає максимальне значення і дорівнює $E(X)$ = 116,366%.

Висновки

У статті розглянуто математичну модель вирішення завдання оптимального вибору засобів захисту від загроз на об'єкті інформатизації. Основними етапами її вирішення є:

– інвентаризація інформаційних ресурсів на ОІ;

– аналіз загроз інформаційній безпеці;

– аналіз ринку засобів захисту від загроз;

– збирання та обробка інформації про характеристики загроз (ймовірності реалізації та збитки від їх незапобігання);

– збирання та обробка інформації про можливість запобігання загроз різними засобами захисту;

– оптимальний вибір варіанту КЗЗ з використанням запропонованого показника ефективності (9), алгоритму та критерія оптимізації.

У результаті знаходяться засоби забезпечення інформаційної безпеки, які дозволять оптимально захистити інформаційні ресурси об'єкта інформатизації на підприємстві. Адекватність запропонованої моделі підтверджується проведеними розрахунками. Результати моделювання залежать від повноти та якості вихідних даних.

Запропонована математична модель оптимального вибору засобів захисту від загроз для кожного інформаційного ресурсу на ОІ надає можливість економічно обґрунтувати склад комплексу спеціальних технічних засобів для КСЗІ в цілому. Критерій оптимальності цієї композиції враховує суму середніх втрат від реалізації загроз та витрат на систему захисту. Згідно з цим критерієм оптимальний КЗЗ повинен забезпечувати максимальне зменшення ризику при мінімальних витратах на його впровадження та експлуатацію.

Новизна цієї моделі визначається тим, що для оцінювання ефективності засобів захисту був запропонований новий показник ефективності (9). На його основі був запропонований критерій оптимальності вибору засобу для запобігання загрози (10), показник ефективності КЗЗ (11) та критерій оптимальності складу КЗЗ для КСЗІ (12). Запропонована математична модель дозволяє поряд із вартістю сучасних засобів захисту врахувати їхні можливості щодо одночасної протидії довільній кількості загроз, що сприяє оптимальному вибору складу КЗЗ на етапі проектування КСЗІ.

Список літератури

1. НД ТЗІ 2.5-007-07, (2007), Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1, Державна служба спеціального зв'язку України, 9 с.

2. НД ТЗІ 2.5-004-99, (1999), Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, Державна служба спеціального зв'язку України, 60 с.

3. *Домарев, В. В.* (2002), Безопасность информационных технологий: Методология создания систем защиты, Диасофт, 688 с.

4. *Козюра, В. Д., Хорошко, В.О., Шелест, М. Є., Ткач, Ю. М., Усов, Я. Ю.* (2019), Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах, ТПК «Орхідея», 144 с.

5. *Яремчук, Ю. Є., Павловський, П. В., Катаєв, В. С., Сінюгін, В. В.* (2018), Комплексні системи захисту інформації: навчальний посібник, ВНТУ, 118 с.

6. *Богуш, В. М., Богуш, Б. М., Довидьков, О. А., Кривуца, В. Г.* (2010), Теоретичні основи захищених інформаційних технологій: навчальний посібник, ДУІКТ, 454 с.

7. *Юдін, О. К., Корченко, О. Г., Конахович, Г. Ф.* (2009), Захист інформації в мережах передачі даних, ТОВ «НВП» ІНТЕРСЕРВІС», 716 с.

8. Аналітичний звіт Державної служби спеціального зв'язку та захисту інформації України «Російські Кібероперації». **URL**: https://cip.gov.ua/services/cm/api/attachment/download?id=60201.

9. *Остапов, С. Е., Євсеєв, С. П., Король, О. Г.* (2020), Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів, Новий Світ-2000, 678 с.

10. *Грайворонський, М. В., Новіков, О. М.* (2009), Безпека інформаційно-комунікаційних систем, Видавнича група BHV, 608с.

11. *Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., Толюпа, С. В.* (2015), Інформаційна та кібербезпека: соціотехнічний аспект: підручник, ДУТ, 288 с.

12. *Корченко, О. Г., Шелест, М. С., Казмірчук, С. В., Ткач, Ю. М., Іванченко, Є. В.* (2019), Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 «Кібербезпека», ТПК «Орхідея», 408 с.

13. *Замула, О. А., Горбенко, Ю. І., Шумов, О. І.* (2010), Нормативно–правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: навч. посібник, ХНУРЕ, 248 с.

14. *Домарев, В. В., Домарев, Д. В.* (2012), Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Велстар, 146 с.

15. *Домарєв, В. В., Домарев, Д. В., Гордієнко, С. Б.* (2012), «Обґрунтування основних функцій системи управління інформаційною безпекою», Вісник Державного університету інформаційно-комунікаційних технологій, № 10(2), С. 102–104.