му за потреби можна добавити більше правил, які будуть детальніше описувати роботу системи та дії, що вона має виконувати у конкретних ситуаціях.

Висновки. Дослідивши альтернативні моделі управлінні крановими установками, встановлено, що використання нечітких систем управління є найкращим способом реалізації такої складної системи, як кранові установки. Нечіткі системи управління використовують нечіткі правила, які базуються на лінгвістичних змінних.

Використання лінгвістичних змінних у багатьох застосуваннях зменшує загальну складність обчислень програми, що є особливо корисним у складних нелінійних застосуваннях. Таким чином, природною мовою можна описати ті операції та дії, які виконує оператор крана під час управління крановою установкою. Можна використати досвід та знання оператора крана в автоматизованому процесі управління краном для забезпечення якісного та безпечного перевезення вантажу без його розгойдування.

Література

1. Popadic T. A fuzzy control scheme for the gantry crane position and load swing control / T. Popadic, F. Kolonic, A. Poljugan // University of Zagreb. – 6 p.

2. Burul I. The control system design of a gantry crane based on H_∞ control theory / I. Burul, F. Kolonić, J. Matuško // MIPRO 2010. – Croatia. – 183-188 p.

3. Practical Fuzzy Logic Design. [Electronic resource]. – Mode of access http://www.fuzzytech.com/e/e_a_pfd.html

4. Banks W. Linguistic Variables: Clear Thinking with Fuzzy Logic / W. Banks. [Electronic resource]. – Mode of access http://www.phaedsys.com/principals/bytecraft/bytecraftdata/Linguistic Variables .pdf.

5. Zadeh L.A. The concept of a Linguistic Variable and its Application to Appproximate Reasoning – I / L.A. Zadeh. [Electronic resource]. – Mode of access http://www.cs.berkeley.edu/ ~zadeh/papers/The Concept of a Linguistic Variable and its Applications to Approximate Reasoning I-1975.pdf.

Ткаченко Р.А., Вербенко И.О. **Лингвистическая стратегия управления крановыми установками**

Проведен анализ традиционных моделей управления такими крановыми установками: на основе ПИД регуляторов; на основе использования математической модели крана в основе модели контроллера; на основе нечеткой логики. Исследовано, что классические методы управления хорошо работают при полностью описанном и определенном объекте управления и известной среде, а для систем, таких как крановые установки, с неполной информацией и высокой сложностью объекта управления, оптимальными являются нечеткие методы управления. Проанализировано использование лингвистических переменных для создания лингвистической стратегии управления портальными кранами на основе знаний и опыта оператора крана, которая будет использоваться в разработке производительных правил. Полученные результаты применяются в разработке автоматизированной системы нечеткого управления крановыми установками для контроля колебания груза при его перевозке.

Ключевые слова: крановая установка, портальный кран, ПИД регуляторы, нечеткая логика, нечеткие системы управления, нечеткие правила, лингвистическая переменная, лингвистическая стратегия управления.

Tkachenko R.O., Verbenko I.O. **Linguistic Strategy for Managing Crane Systems**

Traditional models for managing crane systems such as a model based on the use of PID controllers, a model based on the use of mathematical model in the crane model-based controller, and a model based on fuzzy logic were analyzed. It was investigated that classical management methods work well when the object is fully described and defined and the environment is known. However, for managing systems such as crane installation with incomplete information and high complexity of management object the best way is to use fuzzy logic. The use of linguistic variables for creating gantry cranes linguistic strategy based on knowledge and experience of crane operator and its further usage for the development of production rules was analyzed. The results obtained are used in designing the automated fuzzy crane management system to control load position during its transporting.

Keywords: crane system, gantry crane, PID controllers, fuzzy logic, fuzzy control systems, fuzzy rules, linguistic variable, linguistic management strategy.

УДК 34.03:004.056.5

Проф. Ю.І. Грицюк, д-р техн. наук –
НУ "Львівська політехніка"

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПРИНЦИПУ РОЗУМНОЇ ДОСТАТНОСТІ ФУНКЦІОНУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Розглядаються питання обґрунтування особливостей реалізації принципу розумної достатності та економічної ефективності функціонування комплексної системи захисту інформації (КСЗІ) на підприємстві, які дають змогу встановити його номінальні величини, а також оцінювати якість роботи системи захисту та здійснювати налаштування параметрів експлуатації. Виявлено, що на сьогодні розробити і впровадити абсолютно неперебірну КСЗІ принципово неможливо. При достатньому обсягу часу і наявності сучасних програмно-технічних засобів можна подолати будь-який опір системи захист. Тому йдеться про достатній рівень якості роботи КСЗІ, при якому фінансові витрати на її побудову та експлуатацію, ризик успішної реалізації інформаційних атак і розмір можливого збитку від них були б співвимірними між собою та прийнятними для підприємства.

Ключові слова: інформаційна безпека (ІБ), комплексна система захисту інформації (КСЗІ), інформаційні ресурси (ІР), організаційна та математична модель ІБ підприємства.

Вступ. Відомо, що інформаційні ресурси (ІР) будь-якого підприємства є одним з головних джерел його ефективної економічної діяльності [4]. Фактично існує тенденція, коли всі сфери діяльності підприємства стають залежними від інформаційного розвитку, в процесі якого вони самі породжують інформацію та самі ж її споживають [17]. Тому використання ефективної системи зберігання, накопичення та використання ІР є самостійною складовою загальної діяльності підприємства, значення якої з кожним роком зростає [9].

Стрімкий розвиток ІТ призводить до різкого накопичення ІР підприємства [1, 16], які постійно піддаються різним інформаційним атакам з боку конкурентів, зловмисників чи просто хакерів [5]. Наслідками успішного проведення таких атак можуть стати компрометація конфіденційної або спотворення цілісної інформації, нав'язування керівництву помилкової інформації, порушення встановленого регламенту доступу до достовірної інформації, а також відмови і збої в роботі програмно-технічних систем [2]. Все це також пов'язано з навмисними і випадковими діями як з боку працівників підприємства [13, 14, 19, 23, 30], так і з боку потенційних конкурентів чи злочинних організацій [32]. Реалії ж сьогодення свідчать про те, що кількість зловмисних дій стосовно певного виду інформації не тільки не зменшується, але й має достатньо стійку тенденцію до зростання [8, 18, 28]. Розуміючи це, керівники підприємств вимушені запроваджувати різні організаційні та програмно-технічні заходи щодо захисту ІР, важливих для них [7, 11, 17].

Для вирішення завдань захисту ІР підприємства створюється комплексна система захисту інформації (КСЗІ) [20], головною метою роботи якої є забезпечення безперервності бізнес-процесів підприємства, стійкого його перебігу та запобігання потенційним загрозам і небезпекам [12]. Загалом КСЗІ направлена на недопущення [1]: 1) несанкціонованого використання фінансових і матеріально-технічних цінностей; 2) спотворення цілісної інформації та перешкоджання електронному документообігу; 3) розголошення конфіденційної та витоку службової інформації, а також несанкціонованого доступу до неї; 4) порушення роботи програмно-технічних засобів забезпечення виробничої діяльності підприємства, в т.ч. інформаційно-комунікаційних систем [5, 18].

Оскільки часто доводиться впроваджувати КСЗІ за умови деякої невизначеності середовища її функціонування, тому прийняті заходи і встановлені засоби захисту ІР, особливо в початковий період її експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захищеності ІР підприємства [15, 26, 32]. Для забезпечення можливості варіювання рівнем захищеності ІР потрібно, щоб використовувані засоби КСЗІ володіли певною гнучкістю [22, 24]. Ця властивість є особливо важливою в тих випадках, коли виникає потреба встановлювати нові засоби захисту на наявну КСЗІ, не порушуючи процесу її нормального функціонування. Окрім цього, зовнішні умови перебігу інформаційної злочинності [8, 28] та вимоги до рівня захищеності ІР підприємства з часом міняються. У таких ситуаціях властивість гнучкості КСЗІ часто рятує власників наявних АСУ від потреби впровадження кардинальних заходів з повної заміни деяких засобів захисту на нові, більш досконалі та ефективні [25].

В роботі [10, ст. 12] зазначено, що забезпечення інформаційної безпеки (ІБ) підприємства ґрунтується на таких основних принципах: системності; комплексності; своєчасності; безперервності захисту; розумній достатності; гнучкості; спеціалізації; взаємодії та координації (плануванні); вдосконаленні; централізації та управлінні; активності; економічній ефективності; простоті впровадження організаційних заходів і захисних засобів.

Зі всіх перерахованих принципів особливої уваги заслуговує *принцип розумної достатності*, який враховує той факт, що розробити і впровадити абсолютно неперебороную КСЗІ на підприємстві принципово неможливо [3, 24]. При достатньому обсягу часу і кількості сучасних програмно-технічних засобів можна подолати будь-який захист ІР підприємства, тому йдеться тільки про деякий прийнятний рівень їхньої захищеності [27]. Водночас, високоефективна КСЗІ, попри свою високу вартість впровадження та експлуатації, ще й використовує при роботі істотну частину потужності та ресурсів наявної АСУ підприємства і, зазвичай, створює відчутні додаткові незручності роботи як у обслуговувального персоналу, так і у потенційних клієнтів [25]. Тому важливо правильно вибрати той достатній рівень якості роботи КСЗІ [22], при якому фінансові витрати на її побудову та експлуатацію, ризик успішного проведення інформаційних атак зловмисників і розмір можливого збитку від них були б співвимірними між собою та прийнятними для підприємства.

Однак, у доступній науковій літературі [1, 3, 7, 11, 18, 26, 28] не повністю з'ясовано основні особливості процесу реалізації принципу розумної достатності та економічної ефективності роботи КСЗІ на підприємстві: не виявлено недоліки та переваги наявної організаційної моделі ІБ підприємства; немає рекомендацій

щодо використання найбільш придатних математичних моделей для відбору раціональної системи ЗІ; не синтезовано нові знання, придатні для встановлення достатнього рівня якості роботи системи ЗІ. Тому обґрунтування особливостей реалізації принципу розумної достатності та економічної ефективності функціонування КСЗІ на підприємстві є актуальним науковим завданням, сприяло виконанню цієї роботи та вимагає реалізації подальших досліджень.

Об'єкт дослідження – ефективність роботи КСЗІ на підприємстві.

Предмет дослідження – підходи та механізми реалізації принципу розумної достатності та економічної ефективності роботи КСЗІ на підприємстві.

Мета роботи полягає в обґрунтуванні особливостей реалізації принципу розумної достатності та економічної ефективності функціонування КСЗІ на підприємстві, які дадуть змогу встановити його номінальні величини, а також оцінювати якість роботи та здійснювати налаштування параметрів експлуатації.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) проаналізувати організаційну модель ІБ підприємства, виявити її недоліки та переваги з огляду на сучасні умови інформаційного розвитку;
2) синтезувати нові знання, придатні для встановлення розумної достатності та економічної ефективності функціонування КСЗІ на підприємстві;
3) зробити відповідні висновки та надати рекомендації щодо використання.

1. Організаційна модель інформаційної безпеки підприємства

Відомо [1; 3; 25, ст. 36], що будь-яка організаційна модель ІБ підприємства має ієрархічну структуру, що складається з багатьох елементів, механізмів захисту ІР, логічних, адміністративних і фізичних компонент, процедур реалізації бізнес-процесів і їх конфігурацій, які працюють спільно, забезпечуючи потрібний рівень реалізації бізнес-цілей діяльності підприємства. Кожна модель може мати свої відмінності у структурі [1, ст. 87], але всі вони мають певні ієрархічні рівні, кожен з яких підтримує вищий і захищає нижчий рівень. Оскільки організаційна модель ІБ може мати складну ієрархічну структуру (рис. 1), то різні підприємства можуть наповнювати її різними технологіями захисту своїх ІР, адекватними методами і процедурами їх підтримки для досягнення потрібного рівня захищеності [24].

Реалізація ефективної організаційної моделі ІБ підприємства вимагає зваженого підходу і застосування всіх компонент і процедур для забезпечення безперервності бізнес-процесів підприємства, стійкого його перебігу та запобігання потенційним загрозам і небезпекам [12]. Деякі компоненти моделі (наприклад, списки контролю доступу, методи шифрування) є програмно-технічними, а інші – фізичними і адміністративними (наприклад, розроблення політики ІБ підприємства і забезпечення її відповідності нормативним документам), але кожен має важливе місце в рамках загальної мети діяльності підприємства [1, 7, 11]. Якщо одна компонента відсутня або реалізується не повною мірою, то це може негативно вплинути на всю ієрархічну структуру ІБ підприємства.

Оскільки організаційна модель ІБ підприємства складається з різних ієрархічних рівнів [3], то кожен з них має забезпечити виконання різні функціональні цілі захисту ІР [11], які мають досягатися в різні терміни та за різні проміжки часу. Цілі можуть бути щоденними (*операційними*), середньо-терміновими (*тактичними*) і довготерміновими (*стратегічними*). Те ж саме відбувається і

у сфері планування ІБ підприємства [1]. Щоденні (операційні) цілі пов'язані з продуктивністю роботи АСУ підприємством і виконанням поточних завдань, що забезпечують передбачене функціонування відповідних бізнес-процесів. Середньо-термінові (тактичні) цілі стосуються, наприклад, об'єднання всіх робочих станцій АСУ та відповідних ІР у один домен, щоб забезпечити можливість їхнього централізованого контролю. Прикладом довготермінових (стратегічних) цілей може бути переведення всіх філій на зв'язок з головним офісом за допомогою VPN-з'єднань, об'єднання всіх безпровідних технологій для отримання єдиного підходу до забезпечення ІБ підприємства.

Рис. 1. Організаційна модель ІБ підприємства та її компоненти

Стратегічне планування передбачає роботу з планами, які знаходяться на одному рівні з бізнес-цілями діяльності підприємства і цілями захищеності його ІР. Оскільки цілі такого планування довготермінові, тому вони мають як широкий горизонт реалізації, так і достатню глибину прогнозування подальшої діяльності. Стратегічне планування, зазвичай, містить такі цілі [25, ст. 138]:

- забезпечити правильне розуміння допустимих ризиків проведення інформаційних атак зловмисниками, організувати їх прогнозування та здійснити облік;
- забезпечити відповідність КСЗІ вимогам чинного законодавства та регуляторів ІБ;
- інтегрувати обов'язки працівників підприємства щодо забезпечення ІБ в їх безпосередню та повсякденну діяльність;
- розробити модель компетентності працівників підприємства для забезпечення можливості реалізації бізнес-цілей його діяльності та поліпшення його ІБ;
- використовувати ІБ підприємства як бізнес-перевагу над конкурентами, щоб привернути більше клієнтів і закріпити свій стан на ринку товаровиробників.

Тактичне планування належить до діяльності менеджерів підприємства та підтримки їхніх дій, які необхідні для досягнення широких цілей, висунутих у

процесі стратегічного планування. Загалом, тактичні плани мають дещо коротші терміни планування, набагато вужчий горизонт реалізації та значно меншу глибину прогнозування порівняно із стратегічними планами.

Оперативне планування – це конкретні плани і прогнози, терміни і цілі, припускає вказання дієвих заходів, встановлення жорстких термінів і графіків виконання робіт [25, ст. 141]. Це конкретні дії реалізації тактичних і стратегічних планів, які потрібно зробити для досягнення бізнес-цілей діяльності підприємства. Зазвичай оперативне планування зводиться до [28]:

- оцінювання ризиків успішного проведення інформаційних атак зловмисниками, а також нанесення потенційних збитків підприємству від них;
- усунення негативного впливу змін у системі ЗІ на продуктивність роботи працівників підприємства;
- підтримка і впровадження захисних заходів з поліпшення ІБ підприємства;
- постійне сканування вразливостей і встановлення програмних оновлень;
- контроль відповідності дій працівників підприємства та потенційних клієнтів встановленій політиці ІБ.

Такий підхід до планування називається *горизонтом планування* (planning horizon). При цьому політика ІБ підприємства працює краще тоді, якщо оперативні, тактичні та стратегічні бізнес-цілі діяльності підприємства конкретно визначені та взаємодіють між собою, підтримуючи одне одного.

2. Розумна достатність і економічна ефективність функціонування КСЗІ на підприємстві

Наповнення рівнів ієрархічної структури КСЗІ на підприємстві визначає його керівництво [24], виходячи зі свого уявлення про ІБ підприємства та методи її оцінювання, а також з виділених засобів на захист ІР, з перспектив розвитку підприємства та інших чинників. В цьому випадку йдеться про використовувані заходи щодо нейтралізації потенційних загроз і небезпек [28]. Вважається, що стан захищеності ІР буде достатнім, якщо реалізовані заходи щодо їх захисту будуть адекватними характеру і діям потенційних загроз і небезпек [27].

Організація системи захисту ІР підприємства є процесом, що містить процедуру оцінювання двох протиборних і ворогуючих між собою сторін [10, ст. 16]: з одного боку – це загрози і небезпеки, а з іншого – заходи і засоби КСЗІ. Критерієм взаємодії між потенційними загрозами і наявними чи впроваджуваними засобами системи захисту є стан захищеності ІР підприємства [1], який залежить від:

- стану економічного розвитку підприємства;
- рівня забезпеченості системи захисту ІР підприємства матеріальними, технічними, людськими і іншими засобами;
- рівня компетенції працівників підприємства та ступеню підготовленості кадрів служби ІБ для протидії інформаційним атакам;
- стану та рівня розвитку інформаційної злочинності в регіоні й державі, і ін.

На рис. 2 наведена схема забезпечення розумної достатності та економічної ефективності функціонування КСЗІ на підприємстві [11]. Тут крива 1 характеризує залежність стану захищеності ІР підприємства (R) від рівня його економічного розвитку (E). Згідно з принципом захищеності, крива 1 направлена вгору позаяк із збільшенням рівня економічного розвитку підприємства захищеність ІР

має збільшуватися. Крива 2 вказує на ступінь реалізації інформаційних атак (*W*), тобто характеризує залежність нанесеного збитку підприємству при їх реалізації від рівня його економічного розвитку (*E*). Тенденція зміни кривої 2 вибрана за умови, що динаміка появи потенційних загроз і небезпек у процесі економічного розвитку підприємства залишається постійною. Особливістю графіка, наведеного на рис. 2, є те, що осі *R* і *W* позитивно направлені, але в протилежні сторони, що дає змогу наочно відобразити відповідні тенденції зміни кривих.

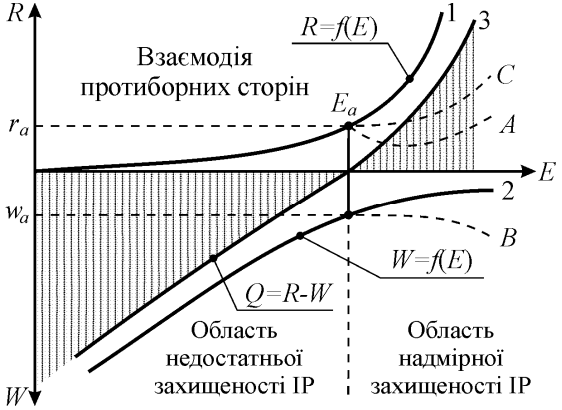

Рис. 2. Розумна достатність рівня захищеності ІР підприємства [10]: *вісь R – захищеність ІР; вісь W – реалізація інформаційних атак; вісь E – економічний розвиток підприємства; E_a – стан, при якому встановлений захист r_a протидіє певним інформаційним атакам w_a; крива 1 характеризує рівень захищеності ІР підприємства; крива 2 – рівень нанесення збитку підприємству; крива 3 – рівень очікуваного економічного ефекту*

Крива 3 – отриманий результат, який відображає різницю взаємодії сторін $Q = R – W$ і вказує на ступінь розумної достатності рівня захищеності ІР підприємства та рівень економічної ефективності роботи КСЗІ. З рис. 2 видно, що в точці рівноваги (E_a) протиборних між собою сторін витрати на захищеність ІР дорівнюють втратам від реалізації інформаційних атак $r_a = w_a$, а тому різниця їхньої взаємодії $Q = 0$. Цей стан рівноваги для підприємства є економічно вигідним, оскільки при цьому забезпечується відповідна (адекватна) потенційним загрозам захищеності ІР підприємства.

На ділянці $[0, E_a]$ втрати підприємства від реалізації інформаційних атак значно перевищують захищеність його ІР, тобто $W > R$, а тому $Q < 0$. Заштрихована область вказує на переважання можливостей потенційних загроз і небезпек над здатністю КСЗІ їм протидіяти. Ця ділянка відповідає області недостатньої захищеності ІР і характеризується часто великими втратами прибутку підприємства через низьку якість роботи КСЗІ. Для цієї області характерні: низький рівень економічного розвитку підприємства та захищеності його ІР; недостатня оцінка керівництвом підприємства потенційних загроз і небезпек; сприяння появі значної кількості інформаційних атак через низький рівень захисту.

На ділянці $[E_a, + \infty]$ втрати підприємства від реалізації інформаційних атак є меншими порівняно з захищеністю ІР підприємства, тобто $W < R$, тому $Q > 0$. Заштрихована область вказує на перевагу заходів і засобів КСЗІ над можли-

востями потенційних загроз і небезпек. Ця ділянка відповідає області надмірної захищеності ІР і характеризується незначними втратами прибутку підприємства через високу якість роботи КСЗІ. Для цієї області характерні: високий рівень економічного розвитку підприємства та захищеності його ІР; належна оцінка керівництвом підприємства потенційних загроз і небезпек; зменшення у зловмисників бажання до інформаційних атак через високий рівень захисту.

Отже, тільки в стані рівноваги протиборних сторін (при $Q = 0$) достатність рівня захищеності ІР є тим мінімально потрібним, при якій витрати на забезпечення такого захисту будуть мінімальними. Такий стан рівноваги вказує на достатню якість роботи КСЗІ на підприємстві, яка відповідає нанесеним збиткам від реалізації потенційних загроз і небезпек, тобто буде їм адекватною.

В процесі управління ІБ підприємства зберегти стан рівноваги можна в одному з двох випадків. Перший, коли тенденція залежності нанесеного збитку підприємству від реалізації інформаційних атак (крива 2) після точки рівноваги E_a не зміниться. В цьому випадку стан захищеності ІР підприємства (крива 1) має змінитися в напрямі *A*.

У другому випадку із зростанням економічного розвитку підприємства після точки рівноваги E_a зловмисники прагнутимуть збільшити свої можливості. В цьому випадку крива 2 змінить свій первинний напрям у бік збільшення нанесеного збитку підприємству від реалізації інформаційних атак (крива В). Для утримання рівноважного, економічно ефективного стану діяльності підприємству потрібно змінити стан захищеності ІР підприємства у бік його збільшення (крива *C*).

Отже, принцип розумної достатності рівня захищеності ІР підприємства вказує на те, що тільки шляхом прогнозування та своєчасного оцінювання як потенційних загроз і небезпек, так і можливостей впроваджених заходів і засобів КСЗІ можна ефективно управляти ІБ підприємства, забезпечуючи при цьому адекватну динаміку захищеності ІР при мінімальних економічних витратах.

На сьогодні будь-яке підприємство при значному обмеженні фінансових ресурсів має широкі можливості для залучення потенційних інвесторів, тому виникає постановка задачі оптимізації інвестиційного портфеля системи захисту ІР підприємства. Однак для її розв'язання потрібно правильно оцінювати ефективність інвестиційних проектів. Насамперед йдеться про впровадження інформаційних технологій (ІТ), коли менеджери, що приймають управлінські рішення, розглядають їх передусім як засіб вирішення завдань бізнес-процесу діяльності підприємства: зниження виробничих витрат, підвищення ефективності виконання бізнес-операцій, критичних для даного виду діяльності, і т.д. Проте стосовно ІБ підприємства, то тут існує виняток, позаяк цілі інвестицій в КСЗІ відрізняються від стандартних цілей ІТ-інвестицій, оскільки потенційний інвестор не очікує їх безпосереднього повернення.

Як правило, основний ефект від впровадження, наприклад, офісних ІС – зростання продуктивності праці певних працівників підприємства [29], що сприяє:

- значній економії робочого часу певних менеджерів системи управління;
- ефективному використанню людських ресурсів підприємства;
- скороченню вартості здійснення операцій в електронному документообігу.

Водночас, інвестиції в КСЗІ з економічної точки зору:

- мають запобігти (знизити) збитки від можливого порушення ІБ підприємства, а не отримання додаткових економічних вигод;
- вважаються специфічним економічним збитком для підприємства під час експлуатації КСЗІ чи її модернізації;
- вважаються доцільними для впровадження нових засобів захисту, якщо їх розмір не перевищує обсягу можливого збитку від дії потенційних загроз і небезпек.

Ці ідеї визначають основні напрями інвестиційного аналізу КСЗІ при її побудові чи модернізації, а саме: оцінювання збитку підприємства в разі реалізації потенційних загроз і небезпек; оцінювання витрат на впровадження нових хаодів і засобів системи захисту ІР; обґрунтування економічно ефективної роботи КСЗІ.

Методи оцінювання збитку (ризиків) від реалізації потенційних загроз і небезпек розглянуті в роботах [18, 26]. Тут тільки відзначимо, що в найпростішому випадку цей аналіз можна не проводити, а використовувати якийсь базовий загальновідомий набір загроз і небезпек. Для протидії цим загрозам приймається типовий набір рішень з реалізації певних засобів ІБ і організаційних заходів у КСЗІ незалежно від ймовірності їх появи та вразливості ІР підприємства. Такий підхід є прийнятним, якщо вартість ІР підприємства є незначною. В цьому випадку витрати на програмно-технічні засоби системи захисту ІР і організаційні заходи забезпечення ІБ, потрібні для відповідності КСЗІ базовим специфікаціям, є обов'язковими. Як правило, витрати на засоби ІБ не перевищують 15-20% засобів, що витрачаються на ІТ-інвестиції. Зазвичай, проводиться аналіз декількох варіантів проектних рішень за критерієм вартості побудови КСЗІ чи ефективності її роботи.

Залежно від ступеня готовності підприємства до впровадження КСЗІ і характеру його основної бізнес-діяльності процес обґрунтування нормативного рівня ризику від реалізації інформаційних атак може проводитися різними способами. В даний час поширений аналіз різних варіантів забезпечення ІБ підприємства за критерієм, який характеризує вартість побудови чи ефективність функціонування КСЗІ. Загалом підприємство може реалізувати два граничні інвестиційні рішення:

1) не вкладати інвестицій у впровадження КСЗІ, допускаючи можливість несення будь-якого збитку від реалізації інформаційних атак;
2) вкладати максимально можливі інвестиції, які реально обмежені тільки його платоспроможністю.

Друге рішення дає змогу комплексно реалізувати правові, організаційні, технічні та морально-етичні заходи у впровадження КСЗІ, що забезпечують значне підвищення надійності та ефективності її роботи. Однак, таке управлінське рішення дуже дорого обходиться підприємству.

Очевидно, що підприємство, з одного боку, в жодному випадку немає дотримуватися першої стратегії поведінки, а з іншого боку – не завжди має можливість реалізувати другу стратегію. Компромісом може бути одне з можливих проектних рішень, яке, як наслідок, зводяться до одного з таких варіантів:

1) вартість побудови КСЗІ немає перевищувати певну суму, наприклад, більше 20 % вартості офісної ІС. В цьому випадку потрібно знайти такий варіант забезпечення ІБ підприємства, який мінімізує рівень інтегральних ризиків;
2) рівень інтегральних ризиків немає перевищувати деяку межу, наприклад, "дуже низький рівень". В цьому випадку потрібно знайти такий варіант забезпечення ІБ підприємства, який мінімізує вартість побудови КСЗІ.

Варто мати на увазі, що збиток від порушення ІБ підприємства може бути значно нижчим за вартість побудови КСЗІ, тобто йдеться про надмірно надійну її роботу. Отже, основний збиток підприємства пов'язаний не з втратами від порушення його ІБ, а з надмірно високою вартістю побудови КСЗІ. Тому інвестиції в її розроблення та експлуатацію мають бути збалансованими і відповідати масштабу появи збитків підприємства при реалізації потенційних загроз і небезпек.

Такий якісний аналіз показує, що в інвестиційному діапазоні існує оптимальне значення інвестицій в побудову КСЗІ, яке мінімізує загальний збиток підприємства при порушеннях його ІБ. Саме у цьому сенсі має розглядатися задача розроблення технічно ефективної та економічно оптимальної КСЗІ.

Типова залежність величини збитку підприємства ($З$) від вартості побудови КСЗІ ($В$) наведена на рис. 3. Тут показано, що із зростанням вартості побудови КСЗІ на підприємстві спостерігатиметься значне зменшення ймовірності нанесеного збитку підприємства $Р_{зб}$ (зменшення вразливості ІР). З рисунку також видно, що застосування навіть недорогих заходів і засобів на забезпечення ІБ підприємства ($V_{ек}$) різко знижує сумарний збиток підприємства ($В_\Sigma$). Тому інвестиції в побудову КСЗІ дуже ефективні навіть в порівняно невеликих розмірах, а крива збитку ($В_\Sigma$) в деякій точці має найменше значення, яке можна вважати оптимальним.

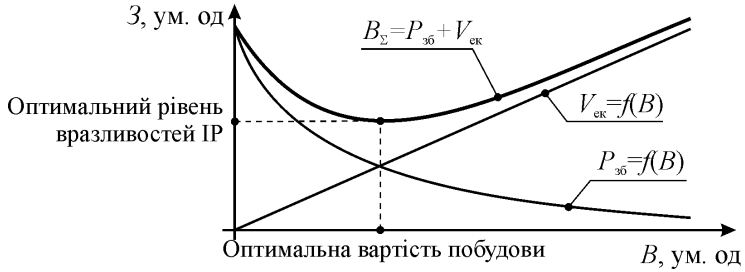

Рис. 3. Залежність збитку підприємства від вартості побудови КСЗІ

Зростання інвестицій в побудову КСЗІ вище за оптимальне значення веде до збільшення сумарних витрат підприємства. В цьому випадку підвищення надійності роботи КСЗІ і відповідне зниження ймовірності появи збитку підприємства нівелюються надмірно високою вартістю забезпечення ІБ підприємства.

Тому якнайкращою стратегією, мабуть, є використання КСЗІ, що забезпечує мінімум сумарних витрат на її впровадження та експлуатацію. Ефективність цього рішення підтверджена різними експериментальними дослідженнями: економічно оптимальна КСЗІ знижує сумарні втрати на її побудову приблизно на порядок порівняно з базовими рішеннями. При цьому така система не є найбезпечнішою. Понад це, ймовірність появи збитку підприємства від порушення його ІБ в цій системі може в рази бути меншою від максимально можливого значення.

У разі, коли основною вимогою до КСЗІ є гарантоване забезпечення ІБ підприємства на заданому рівні, реалізація концепції економічно оптимальної КСЗІ неможлива. Це стосується, наприклад, захисту відомостей, які становлять державну таємницю. Оптимальні КСЗІ найбільш цікаві для економічно самостійних приватних підприємств, для яких спостерігається критичний баланс між витратами на систему ІБ підприємства і можливим збитком від порушення його

ІБ. В цьому випадку оцінювання економічно оптимальних параметрів функціонування КСЗІ є основою формування конкретної її техніко-організаційної структури та рівня захищеності ІР підприємства.

Отже, викладені принципи організації менеджменту з забезпечення ІБ підприємства дають змогу здійснити аналіз наявних КСЗІ або новостворюваних у плані забезпечення економічно ефективної безпеки підприємницької діяльності. Результати такого аналізу дають змогу найбільш ефективно розробити узгоджений комплекс заходів, направлений на вирішення науково-технічних, соціально-економічних і інших проблем відповідно до вимог, встановлених у чинних стандартах і нормативних документах.

Висновки

1. З'ясовано, що для вирішення завдань захисту ІР підприємства впроваджується КСЗІ, головною метою роботи якої є забезпечення безперервності бізнес-процесів підприємства, стійкого його функціонування та запобігання потенційним збиткам підприємства від реалізації інформаційних атак.

2. Виявлено, що на сьогодні розробити і впровадити абсолютно неперебірну КСЗІ на підприємстві принципово неможливо. При достатньому обсягу часу і кількості сучасних програмно-технічних засобів можна подолати будь-який захист ІР підприємства. Тому йдеться про достатній рівень якості роботи КСЗІ, при якому фінансові витрати на її побудову та експлуатацію, ризик успішної реалізації інформаційних атак і розмір можливого збитку від них були б співвимірними між собою та прийнятними для підприємства.

3. Проаналізовано організаційну модель ІБ підприємства, виявлено її недоліки та переваги з огляду на сучасні умови інформаційного розвитку. Встановлено, що кожна організаційна модель ІБ, маючи різні ієрархічні рівні, може наповнюватися різними технологіями захисту ІР, адекватними методами і процедурами їх підтримки, внаслідок чого кожен рівень має різні цілі забезпечення ІБ, які можуть досягатися в різні терміни та за різні проміжки часу.

4. Синтезовано нові знання, придатні для встановлення розумної достатності та економічної ефективності функціонування КСЗІ на підприємстві. Встановлено, що організація системи захисту ІР підприємства є процесом, що містить процедуру оцінювання двох протиборних і ворогуючих між собою сторін: з одного боку – це загрози і небезпеки, а з іншого – заходи і засоби КСЗІ. Критерієм взаємодії між потенційними загрозами і наявними чи впроваджуваними засобами системи захисту є стан захищеності ІР підприємства.

Література

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http:// nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf
2. Бармута Андрей. Утечка информации в корпоративной сети: угроза виртуальная, защита реальная / Андрей Бармута. [Электронный ресурс]. – Доступный с http://www.itsec.ru/articles2/inch-sec/ytechka-informacii-v-korporativnoi-seti-ygroza-virtyalnaya-zashita-realnaya
3. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К. : Вид-во КНЕУ, 2008. – 280 с.
4. Бойчик І.М. Економіка підприємства : навч. посіб. [для студ. ВНЗ] / І.М. Бойчик. – К. : Вид-во "Атіка", 2004. – 480 с.
5. Галицкий А.В. Защита информации в сети: анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М. : Изд-во "ДМК Пресс", 2004. – 616 с.

6. Гатчин Ю.А. Математические модели оценки инфраструктуры системы защиты информации на предприятии / Ю.А. Гатчин, И.О. Жаринов, А.Г. Коробейников // Научно-технический вестник информационных технологий, механики и оптики. – СПб. : Изд-во Университета ИТМО. – 2012. – Т. 12, № 2(78). – С. 92-05.
7. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О.В. Герасименко, А.В. Козак. [Електронний ресурс]. – Доступний з http:// intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/
8. Глобальное исследование информационной безопасности. [Электронный ресурс]. – Доступный с http://www.gosbook.ru/node/64161
9. Глобальное исследование инцидентов внутренней информационной безопасности. [Электронный ресурс]. – Доступный с http://www.securitylab.ru/analytics/291018.php
10. Грибунин В.Г. Комплексные системы защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский. – М. : Изд. центр "Академия", 2009. – 416 с.
11. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf
12. Жора Виктор. Комплексные системы защиты информации: быть или не быть? / Виктор Жора. [Электронный ресурс]. – Доступный с http://infosafe.ua/articles/article-6.html
13. Защита информации от внутренних угроз. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/informationnaya_bezopasnost.php
14. Защита от инсайдеров и утечки информации // ISO27000.RU Искусство управления информационной безопасностью. [Электронный ресурс]. – Доступный с http://www.iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov
15. Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. [Электронный ресурс]. – Доступный с http://profession-konspect.org/?content=3377
16. Корпоративная информационная безопасность: виды IT-угроз. [Электронный ресурс]. – Доступный с http://www.razumny.ru/stat/it-ugrozy.html
17. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.
18. Мальцев А. Методика оценки состояния инженерно-технической защищенности объектов / А. Мальцев // Технологии защиты. – 2010. – № 4. – С. 15-21.
19. Надо ли следить за персоналом?. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/monitiring-personal.php
20. НД ТЗИ 3.7-003-05 "Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електронний ресурс]. – Доступний з http:// www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835
21. Ногин В.Д. Проблема сужения множества Парето: подходы к решению / В.Д. Ногин // Искусственный интеллект и принятие решений. – 2008. – № 1. – С. 98-112.
22. ООО "Дата Лоджик" Комплексные системы защиты информации. [Электронный ресурс]. – Доступный с http://datalogic.ua/kszi/
23. Перехват сообщений и скрытое наблюдение за сотрудниками. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/perehvat_soobshniy_skrytoe_nablyudenie.php
24. Петраков А.В. Основы практической защиты информации : учеб. пособ. – М. : Изд-во "Радио и Связь", 2012. – 384 с.
25. Петров В.А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах : учебн. пособ. / В.А. Петров, А.С. Пискарев, А.В. Шеин. – М. : Изд-во МИФИ, 2005. – 396 с.
26. Радаев Н.Н. Приближенные оценки защищенности объектов от террористических действий / Н.Н. Радаев // Безопасность – Достоверность – Информация. – 2007. – №3(72). – С. 28-32.
27. Скляров Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб. : Изд-во "БХВ – Петербург", 2004. – 288 с.
28. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf
29. Тупкало В.Н. Совершенствование системы управления предприятием на основе реализации принципа "Структура следует за стратегией" / В.Н. Тупкало, С.В. Тупкало // Das Management. – 2009. – № 1 (11-12). – С. 66-71.

30. Утечка информации – угроза корпоративной безопасности. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/Information_leakage.php

31. Черноруцкий И.Г. Методы принятия решений / И.Г. Черноруцкий. – СПб. : Изд-во "БХВ – Петербург", 2005. – 416 с.

32. Ющук Евгений. Брешь в конфиденциальности (Практика использования сети Интернет в конкурентной разведке) / Евгений Ющук. [Электронный ресурс]. – Доступный с http://citcity.ru/17017/

Грыцюк Ю.І. **Особенности реализации принципа разумной достаточности функционирования комплексной системы защиты информации на предприятии**

Рассматриваются вопросы обоснования особенностей реализации принципа разумной достаточности и экономической эффективности функционирования комплексной системы защиты информации (КСЗИ) на предприятии, позволяющие установить его номинальные величины, а также оценивать качество работы системы защиты и осуществлять настройку параметров эксплуатации. Выявлено, что на данный момент разработать и внедрить абсолютно непреодолимую КСЗИ практически невозможно. При достаточном количестве времени и наличии современных программно-технических средств можно преодолеть любое сопротивление системы защиты. Поэтому речь идет о достаточном уровне качества работы КСЗИ, при котором финансовые затраты на ее построение и эксплуатацию, риск успешной реализации информационных атак и размер возможного ущерба от их реализации были бы соразмерны между собой и приемлемыми для предприятия.

Ключевые слова: информационная безопасность (ИБ), комплексная система защиты информации (КСЗИ), информационные ресурсы (ИР), организационная и математическая модель ИБ предприятия.

Gryciuk Yu.I. **Features of the principle of reasonable sufficiency of functioning of complex system of information security in the enterprise**

The issues of study characteristics of the principle of reasonable sufficiency and economic effectiveness of the complex system of information security (CSIS) in the enterprise, allowing it to set the nominal value and assess the quality of the protection system and to adjust operating parameters. It was revealed that at the moment to develop and implement an absolutely irresistible CSIS almost impossible. Given enough time and the presence of modern software and hardware you can overcome any resistance protection system. Therefore, it is a sufficient level of quality of work CSIS in which the financial costs of its construction and operation, the risk of the successful implementation of information attacks, and the size of possible damage from implementation would be proportionate to each other and appropriate for the company.

Keywords: information security (IS), complex system of information security (CSIS), information resources (IR), organizational and mathematical model of enterprise information security.

УДК 356.05.01

Здобувач О.Ю. Антипцева[1] **–**
Українська інженерно педагогічна академія, м. Харків

МОДЕЛЮВАННЯ ВПЛИВУ МОТИВАЦІЙНИХ ФАКТОРІВ НА РІВЕНЬ ФІНАНСОВОГО РОЗВИТКУ МАШИНОБУДІВНИХ ПІДПРИЄМСТВ

Обґрунтовано потребу встановлення впливу мотиваційних факторів на фінансовий розвиток машинобудівних підприємств для ефективного мотиваційно орієнтованого управління ним. Побудовано ієрархічну модель фінансового розвитку машинобудівних підприємств для відображення функціональних складових його забезпечення. Запропоновано структурно-системну модель на основі мотиваційно орієнтованого управління, яка за допомогою виділення та обґрунтування шляхів формування окремих підсистем відображає вплив мотиваційних факторів на результативне значення рівня фінансового розвитку. Для визначення впливу якісних мотиваційних факторів, визначених унаслідок застосування експертних методів, на рівень фінансового розвитку машинобудівних підприємств застосовано метод імітаційного моделювання. На основі побудованої кореляційно-регресійної моделі виділено найбільш впливові кількісні показники ефективності мотиваційних факторів.

Ключові слова: управління, розвиток, фінансовий розвиток, мотиваційно орієнтоване управління, мотиваційні фактори, моделювання, модель, вплив.

Вступ. Процеси інтеграції до світового простору, як виклики сьогодення, притаманні сучасним машинобудівним підприємствам України. Управління на стратегічному рівні набуває соціально орієнтованого спрямування, внаслідок чого вмотивованість людини у високих результатах власної праці та зацікавленість у фінансовому розвитку розглядають як основну рушійну силу соціально-економічного розвитку суспільства.

Адже зацікавленість у підвищенні власного інтелектуального рівня, у набутті відповідних компетентностей зможе забезпечити сталі конкурентні переваги підприємства на шляху до власного фінансового розвитку, оскільки фінансовий розвиток – це безпосередньо результат праці високоосвічених, кваліфікованих, зацікавлених у результатах праці кадрів. Особливим чином підвищення уваги до зазначених шляхів удосконалення діяльності та розвитку сучасних підприємств зумовлено вимогами економіки знань.

Деякі аспекти мотивації розкрито у працях як вітчизняних, так і зарубіжних економістів, зокрема: О.О. Митрофанова **[**1**]**, С. Сардак **[**2**]**, О.О. Хандій **[**3**]**, Л.В. Стрижеус **[**4**]**, А.Н. Леонтьєв **[**5**]**, Б.Ф. Ломов **[**6**]** та ін. Проблеми забезпечення максимального рівня фінансового розвитку машинобудівних підприємств дослідили такі вчені, як В.В. Прохорова **[**7**]**, Т.В. Швед **[**8**]** та ін. Однак треба зауважити, що сучасні умови розвитку економіки знань вимагають поряд з фінансовими пріоритетами висувати мотиваційно орієнтовані інтереси, які здатні спонукати до власного організаційно-управлінського, компетентністного та інтелектуального розвитку як запоруки комплексного фінансового розвитку.

Мета роботи – науково-теоретичне обґрунтування методичних положень здійснення моделювання впливу мотиваційних факторів на рівень фінансового розвитку машинобудівних підприємств України в умовах економіки знань.

Виклад основного матеріалу дослідження. У сучасних умовах розвитку машинобудівних підприємств беззаперечної уваги потребує дослідження тенденцій змін рівня їх фінансового розвитку з урахуванням функціональних особливостей його окремих специфічних напрямків. Це спричинено тим, що існує діалектичний зв'язок між функціональною специфікою та загальним рівнем розвитку. В.В. Прохорова зазначає, що функціонування стримує розвиток і водночас є основою його здійснення. Розвиток руйнує багато процесів функціонування, але при цьому створює умови для його більш сталого здійснення **[**5**]**. У ході дослідження для чіткого розуміння взаємодії рівня фінансового розвитку та його функціональних напрямків використано прийоми ієрархічного моделювання. Принциповий опис змісту процесу фінансового розвитку представлено у виді ієрархічної моделі, що має виражені зв'язки між елементами, що характеризують об'єкт мотиваційно орієнтованого управління на машинобудівних підприємствах (рис. 1). Наявність зв'язків у цій моделі виявляється у використанні відносин між

[1] Наук. керівник: проф. В.В. Прохорова, д-р екон. наук