УДК 330.47:004.056
DOI https://doi.org/10.32689/maup.it.2022.2.14

Віталій ЧУБАЄВСЬКИЙ
кандидат політичних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, вул. Кіото 19, Київ, Україна, індекс 02157 (chubaievskyi_vi@knute.edu.ua)

ORCID: 0000-0001-8078-2652

Альона ДЕСЯТКО
доктор філософії «Комп'ютерні науки», доцент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, вул. Кіото 19, м. Київ, Україна, індекс 02157 (desyatko@knute.edu.ua)

ORCID: 0000-0002-2284-3418

Олена КРИВОРУЧКО
доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, вул. Кіото 19, м. Київ, Україна, індекс 02156 (kryvoruchko_ev@knute.edu.ua)

ORCID: 0000-0002-7661-9227

Валерій ЛАХНО
доктор технічних наук, професор, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки, Національний університет біоресурсів і природокористування України, вул. Героїв Оборони 16, Київ, Україна, індекс 03041 (lva964@nubip.edu.ua)

ORCID: 0000-0001-5725-5942

Дмитро КАСАТКІН
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, Національний університет біоресурсів і природокористування України, вул. Героїв Оборони 16, Київ, Україна, індекс 03041 (lva964@nubip.edu.ua)

ORCID: 0000-0002-2642-8908

Андрій БЛОЗВА
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, Національний університет біоресурсів і природокористування України, вул. Героїв Оборони 16, Київ, Україна, індекс 03041 (andriy.blozva@nubip.edu.ua)

ORCID: 0000-0002-4377-0916

Максим МІСЮРА
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, Національний університет біоресурсів і природокористування України, вул. Героїв Оборони 16, Київ, Україна, індекс 03041 (mdm@nubip.edu.ua)

ORCID: 0000-0002-9061-3462

Vitaliy CHUBAIEVSKYI
Candidate of Political Sciences, Associate Professor, Associate Professor at the Department of Software Engineering and Cybersecurity, Kyiv National University of Trade and Economics, 19 Kioto str., Kyiv, Ukraine, postal code 02157 (chubaievskyi_vi@knute.edu.ua)

Alona DESIATKO
PhD in Computer Sciences, Associate Professor at the Department of Software Engineering and Cybersecurity, Kyiv National University of Trade and Economics, 19 Kioto str., Kyiv, Ukraine, postal code 02157 (desyatko@knute.edu.ua)

Olena KRYVORUCHKO
Doctor of Technical Sciences, Professor, Head of the Department of Software Engineering and Cybersecurity, Kyiv National University of Trade and Economics, 19 Kioto str., Kyiv, Ukraine, postal code 02156 (kryvoruchko_ev@knute.edu.ua)

Valerii LAKHNO
Doctor of Technical Sciences, Professor, Head of the Department of Computer Systems, Networks and Cyber Security, National University of Life and Environmental Sciences of Ukraine, 16 Heroiv Oborony Str., Kyiv, Ukraine, postal code 03041 (lva964@nubip.edu.ua)

Dmytro KASATKIN
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cyber Security, National University of Life and Environmental Sciences of Ukraine, 16 Heroiv Oborony Str., Kyiv, Ukraine, postal code 03041 (d.kasatkin@nubip.edu.ua)

Andrii BLOZVA
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cyber Security, National University of Life and Environmental Sciences of Ukraine, 16 Heroiv Oborony Str., Kyiv, Ukraine, postal code 03041 (andriy.blozva@nubip.edu.ua)

Maxim MISIURA
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cyber Security, National University of Life and Environmental Sciences of Ukraine, 16 Heroiv Oborony Str., Kyiv, Ukraine, postal code 03041 (mdm@nubip.edu.ua)

Бібліографічний опис статті: Чубаєвський, В., Десятко, А., Криворучко, О., Лахно, В., Касаткін, Д., Блозва, А., Місюра, М. (2022). Застосування СППР у завданнях організаційно-економічного забезпечення захисту інформації. *Інформаційні технології та суспільство*, 2 (4), 100–109. DOI: https://doi.org/10.32689/maup.it.2022.2.14

Bibliographic description of the article: Chubaievskyi, V., Desiatko, A., Kryvoruchko, O., Lakhno, V., Kasatkin, D., Blozva, A., Misiura, M. (2022). Zastosuvaniia SPPR u zavdanniah organizaciyno-economichnogo zabezpechennia zakhystu inphormacii [Application of decision support systems in the task of organizational and economic support of information protection]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 2 (4), 100–109. DOI: https://doi.org/10.32689/maup.it.2022.2.14

ЗАСТОСУВАННЯ СППР У ЗАВДАННЯХ ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Безперервне організаційно-економічне забезпечення процедур інформаційної безпеки (ІБ) компанії може мінімізувати бізнес-ризики, максимізувати віддачу від інвестицій, полегшити можливості для бізнесу, підвищити комерційний імідж та конкурентні переваги компанії. Для забезпечення ефективного захисту інформаційних ресурсів компанії (ІнР) та стабільного управління інформаційною безпекою компанії повинні не тільки періодично виконувати оцінку інформаційної безпеки, а й постійно аналізувати процеси для своїх корпоративних інформаційних систем. Описано модель організаційно-економічного забезпечення ефективного захисту корпоративної інформації шляхом формалізації процедур формалізації завдання оптимізації системи захисту інформації (СЗІ). При цьому, на відміну від існуючих підходів, акцент у запропонованому рішенні робиться на математико-алгоритмічну та комп'ютерну підтримку процедури прийняття рішень у контексті завдань менеджменту інформаційної безпеки компанії. Пропоновані доповнення разом із традиційними підходами дають можливість стороні захисту максимально ефективно, визначати параметри організаційного управління інфраструктурою СЗІ підприємства. Розглянуто контур системи підтримки прийняття рішень (СППР) у процесі розвитку інфраструктури системи захисту інформації компанії. В умовах дефіциту кваліфікованих експертів у галузі інформаційної безпеки компаній, запропоновано доповнення моделі. Дані доповнення дозволяють врахувати вплив кадрових ресурсів експертів у питаннях ІБ на управління інфраструктурою СЗІ компанії. Запропоновано рекомендації та описано відповідне прикладне програмне забезпечення – СППР. Застосування цієї системи підтримки прийняття рішень сприятиме мінімізації ризиків, пов'язаних з відсутністю кваліфікованих експертів з інформаційної безпеки у багатьох компаніях.

Ключові слова: *захист інформації, інформаційна безпека, організаційно-економічне забезпечення, управління інфраструктурою, система підтримки прийняття рішень, мінімізація ризиків.*

APPLICATION OF DSS IN THE TASKS OF ORGANIZATIONAL AND ECONOMIC PROVISION OF INFORMATION PROTECTION

Continuous organizational and economic support of the company's information security procedures (IS) can minimize business risks, maximize return on investment, facilitate business opportunities, increase the company's commercial image and competitive advantage. To ensure effective protection of information resources of the company (IR) and stable management of information security, companies must not only periodically perform information security assessments but also constantly analyze the processes for their corporate information systems. The model of organizational and economic support of effective protection of corporate information by formalizing the procedures of formalizing the task of optimizing the information protection system (IPS) is described. In this case, in contrast to existing approaches, the emphasis in the proposed solution is on mathematical-algorithmic and computer support of the decision-making procedure in the context of the tasks of information security management of the company. The proposed additions, together with traditional approaches, enable the defense party to determine the parameters of organizational management of the IPS infrastructure of the enterprise as effectively as possible. The outline of the decision support system (DSS) in the process of developing the infrastructure of the company's information protection system is considered. In the conditions of shortage of qualified experts in the field of information security of companies, additions to the model are proposed. These additions allow taking into account the impact of human resources of IS experts on the management of the company's IPS infrastructure. Recommendations are offered and the corresponding application software – DSS is described. The application of this decision support system will help minimize the risks associated with the lack of qualified information security experts in many companies.

Key words: *information protection, information security, organizational and economic support, infrastructure management, decision support system, risk minimization.*

В умовах глобалізації, кооперації, конкуренції жодна компанія (незалежно від сфери діяльності) не обходиться без розвиненої структури інформаційних технологій та систем (далі, відповідно, ІТ та ІС), що забезпечують успішність та оперативність, як прийняття окремих управлінських рішень, так і ефективність бізнес процесів компанії загалом.

Динамічний зростання ІТ-інфраструктури компаній давно подолав перший етап традиційного розростання масштабів комплексів апаратно-програмних засобів, задіяних для автоматизації збору, зберігання, обробки, передачі та отримання інформації. У сучасних умовах пріоритетними стали не стільки кількість і якість ІТ та ІС, які використовуються в бізнес-процесах суб'єктів господарської діяльності, скільки достовірність та повнота інформації, що сприяють прийняттю оптимальних управлінських рішень. На зміну традиційним ІС для великих компаній прийшли корпоративні інформаційні системи (далі – КІС). Проте, стрімкий розвиток ІТ та ІС компаній породило таку гостру проблему як забезпечення інформаційної безпеки (далі – ІБ) компаній та збереження їх інформаційних ресурсів (далі – ІнР). Застосування атакуючої стороною все більш складних методів реалізації сценаріїв кібернетичних атак призвело до того, що будь-яка КІС вже на момент початку її функціонування вимагає процесу вживання відповідних заходів, спрямованих на захист корпоративної інформації. Отже, кожне підприємство має забезпечувати високий рівень захисту комерційної інформації, цілісність своїх ІнР [1].

Безперервне організаційно-економічне забезпечення процедур ІБ компанії може мінімізувати бізнес-ризики, максимізувати віддачу від інвестицій, полегшити можливості для бізнесу, підвищити комерційний імідж та конкурентні переваги компанії [1; 2]. Для забезпечення ефективного захисту ІнР та стабільного управління ІБ компанії повинні не тільки періодично виконувати оцінку ІБ, а й постійно аналізувати процеси для своїх КІС.

Світовий досвід незаперечно доводить, що просте збільшення чисельності засобів і заходів захисту інформації (далі – ЗІ) який завжди дають відчутний ефект [2]. Більше того, у низці ситуацій [3] реалізація такого сценарію лише підвищує завантаженість персоналу, який займається питаннями інформаційної безпеки компанії. Більше того, помилки при плануванні ресурсів, які виділяються на забезпечення ІБ компаній, призводять до того, що дорогий захист ІнР з малою цінністю або значущістю для бізнес-процесів фактично виливається на економічну шкоду. Такі збитки можуть бути не завжди фінансово очевидними. У ряді випадків розміри репутаційної шкоди у рази перевищують втрати фінансові від втрати інформації [4]. Те саме можна сказати про недостатньо ефективний захист цінних ІнР компаній. Наприклад, за даними [5] наявність у компанії витоків важливої інформації, яка використовується в бізнес-процесах, обсягах >20 % може призвести до того, що з ймовірністю 60 % компанія стане банкрутом. Більше того, за даними [5; 6] понад 90 % компаній, які були позбавлені доступу до власних ІнР на терміни >10 днів, з високою ймовірністю припиняли свою економічну діяльність.

Резюмуючи вище сказане – існує певна суперечність. Так, з одного боку, суттєві витрати на систему захисту інформації – є обов'язковою складовою витрат практично всіх суб'єктів господарської діяльності. А з іншого боку, так само необхідне і вирішення завдання, пов'язаного з оптимізацією витрат на побудову ефективної СЗІ та організацію ефективних процесів у КІС. Зроблені висновки та визначають

релевантність цього дослідження, спрямованого на вдосконалення методів та моделей організаційної підтримки процесів управління ІТ-інфраструктурою у СЗІ компаній.

Огляд і аналіз літератури. У працях [7; 8] показано, що зростаюча інтенсивність і ускладнення сценаріїв проведення кібернетичних атак роблять актуальними не тільки перманентне вдосконалення апаратно-програмних комплексів СЗІ, але і диктують необхідність вживання інших заходів. До таких заходів, зокрема, належать і заходи, спрямовані на вдосконалення організаційно-економічного забезпечення ефективного захисту корпоративної інформації суб'єктів господарської діяльності. На думку [9; 10] необхідно надати стороні захисту ефективні інтелектуальні системи, здатні полегшити досить рутинну роботу з управління ІБ підприємств.

Необхідність оперативного прийняття рішень, пов'язаних з організаційно-економічним забезпеченням та менеджментом захисту корпоративної інформації, зробила перспективними дослідження з розвитку систем підтримки прийняття рішень (СППР) [11; 12] у цій галузі. У цих працях, а також у працях [13; 14] показано, що в рамках створення подібних СППР відповідний розвиток отримують нові методи, моделі, алгоритми та прикладне програмне забезпечення, що використовується для вирішення подібних завдань. Автори розглянутих праць, однак не наводять вагомих аргументів, що доводять ефективність широкого застосування подібних СППР для більшості суб'єктів господарської діяльності.

Досвід застосування СППР у завданнях менеджменту ІБ окремих компаній розглянуто в [15; 16]. Проте, як зазначено у [16; 17] існуючі комерційні СППР у завданнях забезпечення ІБ компаній мають закритий характер. Автори констатують, що придбання окремими невеликими компаніями такого класу СППР пов'язане із значними фінансовими витратами. Існуючі на ринку прикладного ПЗ некомерційні СППР у завданнях ІБ не володію достатньою функціональністю [17].

Як показано в [18; 19; 20], проблематика комплексного впровадження СППР у завдання організаційно-економічного забезпечення ефективного захисту корпоративної інформації в контексті завдань менеджменту ІБ системно не розглядалися.

Більше половини всіх кібератак націлені на невеликі підприємства та підприємства [21]. Незважаючи на таку гнітючу статистику, як показано в [22], значна частина менеджменту малих та середніх компаній продовжує вважати, що ІБ це зайва стаття витрат. Не менш важливо, що ця думка частково заснована і на тлі дефіциту кваліфікованого кадрового потенціалу, який займається ІБ. Таким чином, невеликі компанії мають більше проблем при моніторингу ефективності ІБ. Як показано [23; 24] звичайною практикою таких невеликих компаній стало застосування формальних та складних процедур, орієнтованих на передбачення та прогнозування інцидентів з ІБ.

Враховуючи висновки, зроблені авторами в [13; 15; 17; 18; 19; 20; 24], залишається невирішеною проблема системної імплементації інтелектуальних СППР у завдання організаційно-економічного забезпечення та менеджменту ІБ компаній. Математико-алгоритмічна та комп'ютерна підтримка процедури прийняття рішень та якісна експертна оцінка дозволяють вирішувати завдання організаційно-економічного забезпечення ефективного захисту корпоративної інформації у контексті завдань менеджменту ІБ найбільш ефективно. Таким чином, концептуально інноваційні підходи можуть базуватись на парадигмі комплексного впровадження СППР у завданнях організаційно-економічного забезпечення ефективного захисту корпоративної інформації у контексті завдань менеджменту ІБ компаній. Вище зазначені причини роблять тематику нашого дослідження актуальним. На наш погляд, доцільно зосередити увагу на питаннях впровадження подібних систем підтримки прийняття рішень у невеликих компаніях, де ситуація з ІБ є найбільш критичною.

Мета роботи та завдання дослідження. Мета роботи – розвиток моделі організаційно-економічного забезпечення та менеджменту ІБ компаній.

Для досягнення мети роботи необхідно вирішити такі завдання:

– розробити модель організаційно-економічного забезпечення та менеджменту інформаційної безпеки компаній з урахуванням мінімізації ризиків, пов'язаних із відсутністю кваліфікованих експертів з інформаційної безпеки;

– розробити та протестувати систем підтримки прийняття рішень для організаційно-економічного забезпечення та менеджменту інформаційної безпеки компаній, які дозволить стороні захисту раціонально використовувати методи та системи захисту інформації.

Методи та моделі. У [25; 26] наголошується, що в умовах глобальної цифровізації економіки багато компаній зіткнулися з дефіцитом кваліфікованих фахівців з кібербезпеки. І якщо більшу частину загроз ІнР вдається блокувати апаратно-технічними системами захисту інформації, то питання організаційно-економічного забезпечення ефективного захисту корпоративної інформації доводиться вирішувати аналітикам з інформаційної безпеки. І тут багато залежить від кваліфікації та досвіду ро-

бота конкретного спеціаліста. На наш погляд, може виявитися досить ефективним напрямок, пов'язаний із широким впровадженням у практику вирішення завдань з організаційно-економічного забезпечення систем захисту корпоративної інформації інтелектуальних систем підтримки прийняття рішень, див. рис. 1.

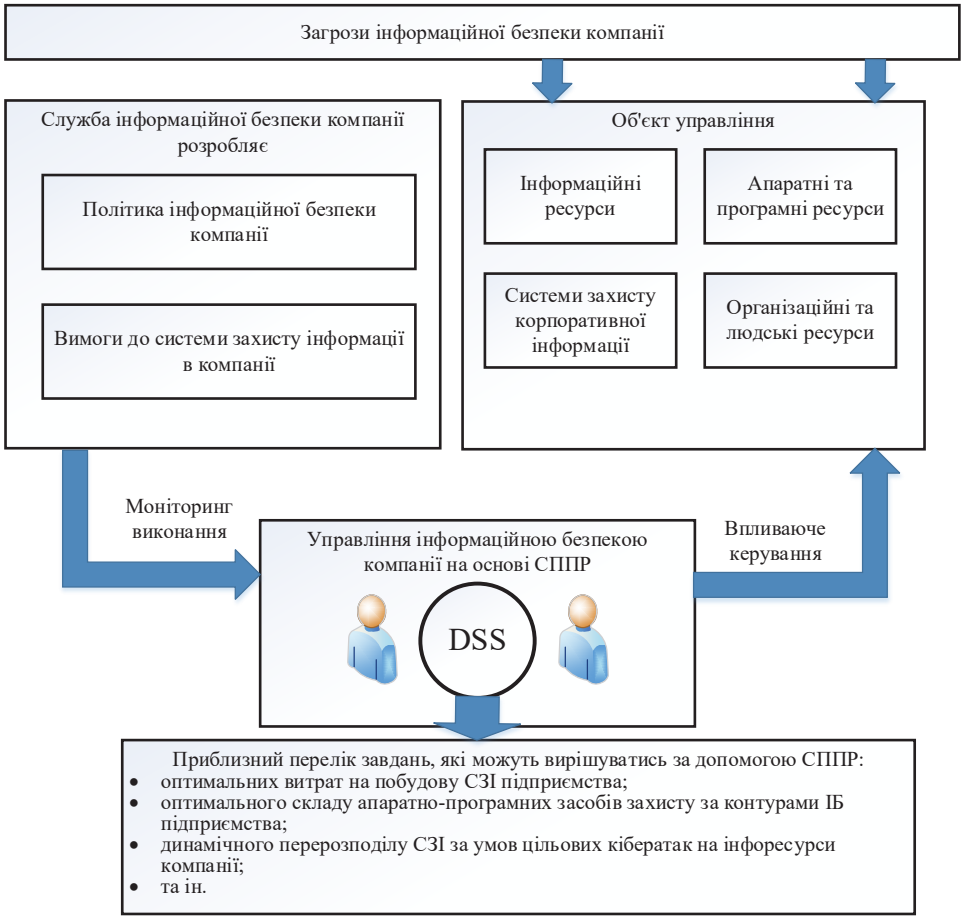

Рис. 1. Структурна схема СППР у задачах забезпечення ІБ компанії

Такі систему здатні взяти на себе виконання досить рутинних та трудомістких розрахунково-аналітичних завдань, пов'язаних, наприклад, з оптимізацією дозволу окремих СЗІ за контурами ІБ компанії. Також такого роду СППР дозволять оперативно приймати рішення при перерозподілі СЗІ за умов динамічного протистояння атакуючій стороні [27; 28; 31–33].

Імплементація СППР, наприклад, структуру моделі ISP 10 × 10M [27; 28], сприятиме ефективнішої реалізації рекомендацій щодо забезпечення ІБ компанії (див. рис. 2). На рис. 2 показані фактори ІБ відповідно до моделі ISP 10 × 10M. Ті фактори, для яких може бути задіяний потенціал СППР, показані із зеленою заливкою.

Загальноприйнятою практикою у системі управління ІБ (далі СУІБ) компаній є делегування частини завдань, які вимагають досить високої кваліфікації, зовнішнім експертам. Однак такий підхід стає не таким ефективним, коли йдеться про необхідність проведення техніко-економічних розрахунків у завданнях забезпечення ІБ підприємства.

Наприклад, до таких завдань можна віднести багатокритеріальні оптимізаційні завдання, пов'язані з пошуком:

- оптимальних витрат на побудову СЗІ компанії;
- оптимального складу апаратно-програмних засобів захисту за контурами ІБ підприємства;
- динамічного перерозподілу СЗІ за умов цільових кібератак на ІнР компанії.

У таких ситуаціях, на наш погляд, доцільно перекласти рутинні розрахунки та пошук математичних рішень, зазначених оптимізаційних завдань, на СППР. При такому підході процеси аналізу даних аудиту ІБ та результатів математико-економічного моделювання за допомогою СППР, а в ряді випадків та прогнозування ризиків, надається керівництву компанії.

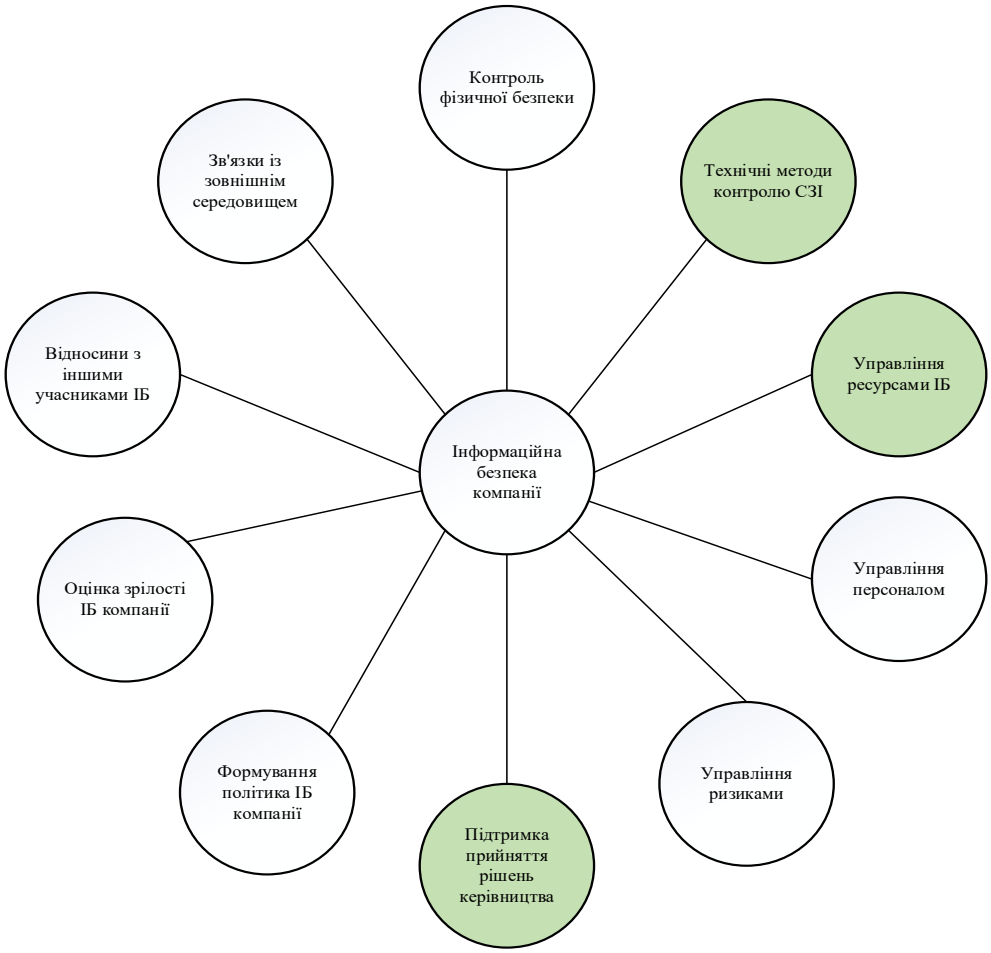

Рис. 2. Структурна схема моделі ISP 10 × 10M
(фактори для яких рекомендується використання СППР, відзначені зеленим кольором)

У міру зростання кількості та ускладнення сценаріїв проведення атак, ІБ стає одним із основних управлінських завдань менеджменту компаній. Це з тим що доводиться розглядати управління складної системою. Причому неправильні рішення щодо ІБ компанії можуть призвести до зниження продуктивності всіх бізнес-процесів. Коли фахівці в галузі ІБ компанії компетентні та здатні забезпечити високий рівень безпеки та захисту інформації, вони здебільшого діють ефективно та при вирішенні завдань планування та інвестиційної діяльності в ІБ. Таким чином, загальна ефективність бізнес-процесів компанії найчастіше залежить від узгодженості між плануванням ІБ та бізнес-плануванням.

Розв'язання задач, пов'язаних з оптимізацією СЗІ компанії включає такі етапи [14; 28]:

1) визначити параметри організаційного управління ІТ-інфраструктурою та СЗІ;
2) мінімізувати витрати на побудову СЗІ;
3) вибрати оптимальний розмір інвестицій СЗІ компанії;
4) виключити (або мінімізувати) можливості витоків інформації у компанії.

Обчислювальне ядро СППР здатне взяти він всі розрахунки з пошуку локальних чи глобальних екстремумів цільових функцій.

Наприклад, пошуку вирішення задачі мінімізації фінансових витрат на СЗІ можна використовувати функцію виду:

$$C = \sum_{i=1}^{n}\sum_{j=1}^{m} C_{ij} \cdot \alpha_{ij} + \sum_{i=1}^{n} C_i \cdot \beta_i \rightarrow \min, \tag{1}$$

$$i = \overline{1,n}; \quad j = \overline{1,m}$$

при дотриманні наступних граничних умов:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} s_j \cdot m_{ij} \cdot \alpha_{ij} \geq PL_{dc}, \sum_{i=1}^{n} \alpha_{ij} = 1, \forall j \in J, \tag{2}$$

$$\sum_{j=1}^{m} k_{ij} = 1,\ \alpha_{ij} \in \{0;1\},\ \beta_{ij} \in \{0;1\},$$

де C_{ij} – розмір витрат на захист j-го ресурсу за допомогою i-го СЗІ; C_i – розмір витрат на безлічі ІнР за допомогою i-го СЗІ; $I=\{i_1, ..., i_n\}$; $J=\{j_1, ..., j_m\}$ – відповідно, безліч СЗІ у компанії та безліч ІнР, які підлягають захисту; m_{ij} – оцінка ефективності захисту j-го ресурсу за допомогою i-го СЗІ; s_j – коефіцієнт важливості j-го ресурсу при комплексній оцінці СЗІ підприємства; α_{ij} – бінарна величина, якщо $\alpha_{ij}=1$ то i-е СЗІ обрано для захисту j-го ресурсу, $\alpha_{ij}=0$, то i-е СЗІ використовується для захисту тільки від потенційних загроз; β_i – двійкове значення, якщо $\beta_i=1$ тоді i-е IPS можна використовувати, якщо $\beta_i=0$, то ні; PL_{cd} – рівень захисту при витратах на СЗІ у розмірі (C) та погрозах (D).

Якщо йдеться про необхідність максимізувати рівень захисту ІнР компанії, то можна використовувати таку цільову функцію:

$$PL_c = \sum_{i=1}^{n}\sum_{j=1}^{m} s_j \cdot m_{ij} \cdot \alpha_{ij} \to \max, \tag{3}$$

при дотриманні наступних граничних умов:

$$C = \sum_{i=1}^{n}\sum_{j=1}^{m} C_{ij} \cdot \alpha_{ij} + \sum_{i=1}^{n} C_i \cdot \beta_i \le C_d,\ \sum_{i=1}^{n} \alpha_{ij} = 1, \forall j \in J, \tag{4}$$

$$\alpha_{ij} \in \{0;1\},\ \beta_{ij} \in \{0;1\}.$$

Висока динаміка зміни ландшафту кібернетичних загроз та зовнішнього середовища для сучасних компаній, що будують багато своїх бізнес-процесів на застосуванні ІТ та ІС, диктує свої особливості у питанні формування кадрової політики щодо фахівців, що займаються ІБ. Метою даного дослідження не є детальне вивчення проблеми ефективності використання кадрового потенціалу ІБ у компаніях. Ми лише хочемо наголосити, що це, як і раніше, залишається маловивченим і вимагає пильної уваги керівників компаній.

У загальному вигляді безліч, що формалізує дефіцит кадрових ресурсів в області ІБ компанії можна так:

$$PE = \{J, \Pr, M, D\}, \tag{5}$$

де J – безліч ІнР компанії які вимагають уваги з боку персоналу в контексті ІБ; Pr – безліч властивостей, якими повинен мати співробітник, який займається питаннями ІБ для конкретних ІнР; M – мотивація до постійного підвищення рівня професійної кваліфікації; D – безліч загроз, що вимагають реагування співробітника, який має високу кваліфікацію.

Зрозуміло, дана формалізація моделі не враховує всі аспекти проблеми дефіциту кадрів фахівців з ІБ компаній, проте вона ілюструє важливість завдання включення до контуру бізнес процесів інтелектуальних СППР, готових прийняти на себе частину досить рутинної роботи, яку доводиться виконувати персоналу у повсякденній практиці забезпечення ІБ компанії. Окремого моделювання та оцінки потребує і процедура розгляду актуальних загроз та ризиків, пов'язаних із реалізацією цих загроз. Описані вище моделі було реалізовано у ряді програмних продуктів. Наприклад, у СППР "DSS investing in cybersecurity" [29; 30].

СППР DSS investing in cybersecurity призначений для вибору в режимі онлайн оптимальних стратегій інвестування в засоби ІБ компанії. Це завдання вирішується в контексті підвищення захищеності КІС компаній за допомогою інноваційних технологій, що ґрунтуються на використанні інтелектуальних систем підтримки прийняття рішення в контурах захисту КІС.

Не ставлячи пріоритетом даного дослідження розвиток комплексу моделей для вирішення багатокритеріальних оптимізаційних завдань, пов'язаних із забезпеченням ІБ компанії, зауважимо, що вирішення цих завдань може бути ефективним лише на основі синергетичного поєднання досвіду експертів і кібернетичного моделювання. Але в сукупності це забезпечує оперативне прийняття рішень щодо забезпечення ІБ компанії.

Обговорення. Якщо покласти на СППР вирішення завдань, пов'язаних з оптимізацією СЗІ, то фахівцям з ІБ усередині компанії можна зосередитись на вирішенні організаційних завдань.

До таких завдань, наприклад, відносяться заходи щодо резервного копіювання даних; ізоляції найбільш чутливих до загроз інформаційних систем; безпечне та надійне знищення пристроїв та даних; централізованого управління системою та управління конфігурацією та ін. Також зауважимо, що спеціалістам з ІБ у самій компанії набагато простіше ніж зовнішнім спеціалістам відстежить персонал, який має зловмисні мотиви. Не потрібна допомога СППР та при вирішенні завдань, пов'язаних з мотивацією та готовністю співробітників брати участь у процесах навчання з ІБ.

СППР також може бути ефективною при аналізі та оцінці ризиків, планів забезпечення безперервності бізнесу та реагування на інциденти, а також для підвищення оперативності процедур відновлення КІС.

Дані математико-економічного моделювання з допомогою СППР передаються менеджменту підприємства прийняття рішень на стратегічному рівні управління ІБ. Основним завданням керівництва у такій ситуації стає забезпечення розумного підходу до формування політики ІБ. Успішність реалізації політики ІБ вимагає безперервної вертикальної та горизонтальної комунікації та координації потреб усіх зацікавлених сторін – фахівців з ІБ, мережевих адміністраторів, менеджменту та ін. Таким чином, організаційно-економічне забезпечення ефективного захисту корпоративної інформації стає невід'ємною частиною процедур управління ІБ. Такий синергетичний підхід демонструє адекватний рівень зрілості ІБ компанії. Застосування СППР можна назвати та розвивати як окрему бізнес-функцію ІБ. Причому ця бізнес функція разом із традиційними підходами дозволить більш оперативно виявляти слабкі ланки ІБ компанії.

Висновки. Набула подальшого розвитку модель, яка описує процедуру формалізації завдання оптимізації системи захисту інформації (СЗІ) суб'єкта господарської діяльності (компанії). На відміну від існуючих підходів, акцент на даному дослідженні, зроблений на математико-алгоритмічну та комп'ютерну підтримку процедури прийняття рішень у питаннях організаційно-економічного забезпечення ефективного захисту корпоративної інформації в контексті завдань менеджменту інформаційної безпеки (ІБ) компаній.

Пропонований підхід дає можливість стороні захисту максимально ефективно, визначати параметри організаційного управління інфраструктурою СЗІ компанії. Розглянуто контур СППР у процесі розвитку інфраструктури СЗІ підприємства. В умовах дефіциту кваліфікованих експертів у галузі ІБ компаній, запропоновано доповнення до існуючих математичних моделей. Запропоновані доповнення дозволяють врахувати вплив кадрових ресурсів експертів у питаннях ІБ на управління інфраструктурою СЗІ компанії. Запропоновано рекомендації та описано відповідне прикладне програмне забезпечення – СППР. Застосування цієї СППР сприятиме мінімізації ризиків, пов'язаних з відсутністю кваліфікованих експертів з ІБ у багатьох компаніях.

Список використаних джерел:

1. Кузнецова Н. В. (2014). Деякі аспекти мінімізації інформаційних ризиків у банківській діяльності. Системні дослідження та інформаційні технології, (1), 7–19.

2. Гордієнко Н., & Дмитро М. (2019). Захист великих даних та мінімізація ризиків втрати інформації. Лóгоσ. Онлайн. https://www.ukrlogos.in.ua/10.11232-2663-4139.04.32.html

3. Al-Moshaigeh A., Dickins D., & Higgs J. L. (2019). Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution? The CPA Journal, 89 (6), 36–41.

4. Amir E., Levi S., & Livne T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, 23 (3), 1177–1206.

5. Erokhin Sergey & Petukhov Andrey & Pilyugin Pavel. (2021). Comparison of Information Security Systems for Asymptotic Information Security Management Critical Information Infrastructures. 89–95. 10.23919/FRUCT50888.2021.9347608

6. Alhayani B., Abbas S. T., Khutar D. Z., & Mohammed H. J. (2021). Best ways computation intelligent of face cyber attacks. Materials Today: Proceedings.

7. Dogaru D. I., & Dumitrache I. (2019). Cyber attacks of a power grid analysis using a deep neural network approach. Journal of Control Engineering and Applied Informatics, 21 (1), 42–50.

8. Krundyshev V., & Kalinin M. (2019, September). Hybrid neural network framework for detection of cyber attacks at smart infrastructures. In Proceedings of the 12th International Conference on Security of Information and Networks (pp. 1–7).

9. Цвілій О. О. (2014). Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою. Телекомунікаційні та інформаційні технології, (2), 73–79.

10. Sarker I. H., Kayes A. S. M., Badsha S., Alqahtani H., Watters P., & Ng A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7 (1), 1–29.

11. Akhmetov B., Lakhno V., Akhmetov B., & Alimseitova Z. (2018, September). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162–171). Springer, Cham.

12. Naseer H., Maynard S. B., & Desouza K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems, 143, 113476.

13. Couce-Vieira A., Insua D. R., & Kosgodagan A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17 (4), 356–374.

14. Adla Abdelkader & Frendi Mohammed. (2021). A Decision Support Systemfor Commercial Lending. 326–331. DOI: 10.1109/DASA53625.2021.9682296

15. Хох В. Д., Мелешко Є. В., & Смірнов О. А. (2017). Дослідження методів аудиту систем управління інформаційною безпекою. Системи управління, навігації та зв'язку, (1), 38–42.

16. Donaldson S. E., Siegel S. G., Williams C. K., & Aslam A. (2015). Measuring a Cybersecurity Program. In Enterprise Cybersecurity (pp. 213–229). Apress, Berkeley, CA.
17. Ekstedt M., Johnson P., Lagerström R., Gorton D., Nydrén J., & Shahzad K. (2015). Securi cad by foreseeti: A cad tool for enterprise cyber security management. In 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop (pp. 152–155). IEEE.
18. Radziwill N. M., & Benton M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. arXiv preprint arXiv: 1707.02653.
19. Al-Dhahri S., Al-Sarti M., & Abdul A. (2017). Information security management system. International Journal of Computer Applications, 158 (7), 29–33.
20. Lakhno V. A. (2017). Development of a support system for managing the cyber security. Radio Electronics, Computer Science, Control, (2), 109–116. https://doi.org/10.15588/1607-3274-2017-2-12
21. Business Advantage. The State of Industrial Cybersecurity 2017. 2017. Available: https://go.kaspersky.com/rs/802-IJN-240/images/ICSWHITE PAPER.pdf
22. Senseon. The State of Cyber Security-SME Report 2019. 2019. Available: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2019/08/
23. Cassar G., & Gibson B. (2007). Forecast rationality in small firms. Journal of Small Business Management, 45 (3), 283–302.
24. Chang S. E., & Ho C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems.
25. Burrell D. N. (2020). An exploration of the cybersecurity workforce shortage. In Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1072–1081). IGI Global.
26. Ohta T., Takenaka M., Katou M., Masuoka R., Kayama K., Fukushima N., & Imai H. (2018). Cybersecurity solutions for major international events. FUJITSU SCIENTIFIC & TECHNICAL JOURNAL, 54 (4), 57–65.
27. Prislan K., Mihelič A., & Bernik I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. PloS one, 15 (9), e0238739.
28. Bernik I., & Prislan K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. PloS one, 11 (9), e0163050.
29. Akhmetov B., Lakhno V., Yagaliyeva B., Kydyralina L., Oshanova N., Adilzhanova S. Conceptual Diagram of an Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems, (2021) Journal of Theoretical and Applied Information Technology, 99 (18), pp. 4297–4310.
30. Lakhno V., Malyukov V., Kasatkin D., Blozva A., Zhyrova T., Kotenko N., Kotova M. Model for Supporting Decisions of Investors, Taking into Consideration Multifactoriality and Turnover, (2021) Communications in Computer and Information Science, 1388 CCIS, pp. 525–535.
31. Bebeshko B., Khorolska K., Kotenko N., Kharchenko O., & Zhyrova T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings,, 2923, 213–223.
32. Lakhno V., Akhmetov B., Ydyryshbayeva M., Bebeshko B., Desiatko A., Khorolska K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber G. W. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol. 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42
33. Khorolska K., Lazorenko V., Bebeshko B., Desiatko A., Kharchenko O., Yaremych V. (2022) Usage of Clustering in Decision Support System. In: Raj J. S., Palanisamy R., Perikos I., Shi Y. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol. 213. Springer, Singapore. https://doi.org/10.1007/978-981-16-2422-3_49

References:

1. Kuznyetsova, N. V. (2014). Deyaki aspekty minimizatsiyi informatsiynykh ryzykiv u bankivskiy diyal'nosti. [Some points of minimizing informational risks in banking]. System research and information technologies, (1), 7–19. [in Ukrainian]
2. Gordienko, N., & Dmitry, M. (2019). Zakhyst velykykh danykh ta minimizatsiya ryzykiv vtraty informatsiyi [Big Data Protection And Minimization of Risks of Loss of Information]. λόροσ. online. (https://www.ukrlogos.in.ua/10.11232-2663-4139.04.32.html). [in Ukrainian]
3. Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution? The CPA Journal, 89 (6), 36–41.
4. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, 23 (3), 1177–1206.
5. Erokhin, Sergey & Petukhov, Andrey & Pilyugin, Pavel. (2021). Comparison of Information Security Systems for Asymptotic Information Security Management Critical Information Infrastructures. 89–95. 10.23919/FRUCT50888.2021.9347608
6. Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. Materials Today: Proceedings.
7. Dogaru, D. I., & Dumitrache, I. (2019). Cyber attacks of a power grid analysis using a deep neural network approach. Journal of Control Engineering and Applied Informatics, 21 (1), 42–50.
8. Krundyshev, V., & Kalinin, M. (2019, September). Hybrid neural network framework for detection of cyber attacks at smart infrastructures. In Proceedings of the 12th International Conference on Security of Information and Networks (pp. 1–7).

9. Tsviliy, O. O. (2014). Bezpeka informatsiynykh tekhnolohiy: suchasnyy stan standartiv ISO27k systemy upravlinnya informatsiynoyu bezpekoyu. [Information security: the current state of ISO27k standards of information security management system]. Telecommunication and Information Technologies, (2), 73–79. [in Ukrainian]

10. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7 (1), 1–29.

11. Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018, September). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162–171). Springer, Cham.

12. Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems, 143, 113476.

13. Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17 (4), 356–374.

14. Adla, Abdelkader & Frendi, Mohammed. (2021). A Decision Support Systemfor Commercial Lending. 326–331. DOI: 10.1109/DASA53625.2021.9682296

15. Hoch, V. D., Meleshko, E. V., & Smirnov, O. A. (2017). Doslidzhennya metodiv audytu system upravlinnya informatsiynoyu bezpekoyu. [Research of methods of audit of information security management systems]. Control, Navigation and Communication Systems, (1), 38–42. [in Ukrainian]

16. Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Measuring a Cybersecurity Program. In Enterprise Cybersecurity (pp. 213–229). Apress, Berkeley, CA.

17. Ekstedt, M., Johnson, P., Lagerström, R., Gorton, D., Nydrén, J., & Shahzad, K. (2015). Securi cad by foreseeti: A cad tool for enterprise cyber security management. In 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop (pp. 152–155). IEEE.

18. Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. arXiv preprint arXiv: 1707.02653.

19. Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information security management system. International Journal of Computer Applications, 158 (7), 29–33.

20. Lakhno, V. A. (2017). Development of a support system for managing the cyber security. Radio Electronics, Computer Science, Control, (2), 109–116. https://doi.org/10.15588/1607-3274-2017-2-12

21. Business Advantage. The State of Industrial Cybersecurity 2017. 2017. Available: https://go.kaspersky.com/rs/802-IJN-240/images/ICSWHITE PAPER.pdf

22. Senseon. The State of Cyber Security-SME Report 2019. 2019. Available: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2019/08/White_paper_1.pdf%0A

23. Cassar, G., & Gibson, B. (2007). Forecast rationality in small firms. Journal of Small Business Management, 45 (3), 283–302.

24. Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems.

25. Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1072–1081). IGI Global.

26. Ohta, T., Takenaka, M., Katou, M., Masuoka, R., Kayama, K., Fukushima, N., & Imai, H. (2018). Cybersecurity solutions for major international events. FUJITSU SCIENTIFIC & TECHNICAL JOURNAL, 54 (4), 57–65.

27. Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. PloS one, 15 (9), e0238739.

28. Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. PloS one, 11 (9), e0163050.

29. Akhmetov, B., Lakhno, V., Yagaliyeva, B., Kydyralina, L., Oshanova, N., Adilzhanova, S. Conceptual Diagram of an Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems, (2021) Journal of Theoretical and Applied Information Technology, 99 (18), pp. 4297–4310.

30. Lakhno, V., Malyukov, V., Kasatkin, D., Blozva, A., Zhyrova, T., Kotenko, N., Kotova, M. Model for Supporting Decisions of Investors, Taking into Consideration Multifactoriality and Turnover, (2021) Communications in Computer and Information Science, 1388 CCIS, pp. 525–535.

31. Bebeshko, B., Khorolska, K., Kotenko, N., Kharchenko, O., & Zhyrova, T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings, 2923, 213–223.

32. Lakhno, V., Akhmetov, B., Ydyryshbayeva, M., Bebeshko, B., Desiatko, A., Khorolska, K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber G. W. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol. 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42

33. Khorolska, K., Lazorenko, V., Bebeshko, B., Desiatko, A., Kharchenko, O., Yaremych, V. (2022) Usage of Clustering in Decision Support System. In: Raj J. S., Palanisamy R., Perikos I., Shi Y. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol. 213. Springer, Singapore. https://doi.org/10.1007/978-981-16-2422-3_49