УДК 336.7004.056.5 DOI: http://dx.doi.org/10.30970/meu.2024.52.0.5216
JEL 004.056.5

ОРГАНІЗАЦІЙНІ ОСОБЛИВОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ В УМОВАХ ВІЙНИ ТА ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

Андрій Денисенко[1], Ростислав Саблук[2]

[1]Приватний вищий навчальний заклад «Європейський університет»
03115, м. Київ, бульвар академіка Вернадського, 16 В
e-mail: andriy.denysenko@e-u.edu.ua
ORCID: 0009-0007-8057-9444
[2]Приватний вищий навчальний заклад «Європейський університет»
03115, м. Київ, бульвар академіка Вернадського, 16 В
e-mail: rostyslav.sabluk@e-u.edu.ua
ORCID: 0009-0002-7085-3028

Анотація. *У статті досліджено організаційні аспекти управління системою інформаційної безпеки підприємств, зокрема в умовах воєнного часу, коли ризики загроз для інформаційних ресурсів значно зростають. Окреслено ключові проблеми, з якими стикаються сучасні підприємства, та запропоновано шляхи їх подолання. Особливу увагу приділено аналізу ключових термінів і понять, пов'язаних із інформаційною безпекою, що дозволяє систематизувати знання у цій сфері. У статті проаналізовано практичне застосування стандарту ISO/IEC 27001:2022 як основи для розробки системи управління інформаційною безпекою. Розглянуто ключові вимоги цього стандарту, які передбачають проведення оцінки ризиків, впровадження політик безпеки, навчання персоналу та регулярний аудит інформаційних систем. Підкреслено важливість інтеграції цих заходів у загальну стратегію управління підприємством для досягнення оптимальних результатів. Окремий акцент зроблено на специфіці управління інформаційною безпекою під час війни, коли підприємства стикаються з новими викликами, такими як кібератаки, порушення ланцюгів поставок та необхідність роботи в умовах обмеженого доступу до ресурсів.*
Ключові слова*: безпека, менеджмент, підприємство, захист інформації, управління, загрози, інформаційна безпека, цифровізація.*

Постановка проблеми. Забезпечення надійної системи управління інформаційною безпекою (СУІБ) є одним із ключових елементів економічної стабільності будь-якого підприємства. У сучасних реаліях, коли інформаційні технології проникають у всі аспекти бізнесу, питання інформаційної безпеки набувають стратегічної важливості. Особливо гостро це питання постає в умовах війни, коли необхідно постійно захищати інформаційні ресурси підприємств, зокрема тих, які беруть активну участь у протидії агресору. Масштабне впровадження цифрових технологій та

використання комп'ютерних систем із застосуванням штучного інтелекту, підкреслює важливість побудови ефективних механізмів захисту від інформаційних загроз. Такий захист покликаний мінімізувати ризики витоку даних, забезпечити стійкість систем до кібератак та запобігти зупинці критичних бізнес-процесів. Це потребує розробки і впровадження продуманих стратегій, що дозволяють оперативно виявляти та ліквідовувати можливі загрози.

СУІБ виступає важливим інструментом забезпечення економічної стійкості підприємств, сприяючи зниженню ризиків, захисту інформаційних активів і підвищенню довіри партнерів та клієнтів. В умовах війни, коли підприємства стикаються з посиленим впливом зовнішніх і внутрішніх загроз, наявність такої системи є критично важливою для стабільності та розвитку їхньої діяльності. Сучасні реалії вимагають обов'язкового впровадження СУІБ як у державних, так і в приватних організаціях. Такий підхід забезпечує комплексний захист інформації та сприяє формуванню стратегії, яка враховує як короткострокові виклики, так і довгострокові перспективи розвитку. Забезпечення інформаційної безпеки стало не лише вимогою часу, але й невід'ємним елементом конкурентоспроможності та успіху підприємств.

Аналіз основних досліджень і публікацій. Теоретичні та практичні аспекти питань інформаційної безпеки розглядаються в працях зарубіжних і вітчизняних дослідників Г. Атаманова, О. Архипова, Е. Бєляєва, М. Бусленка, В. Василюка, С. Гриняєва, О. Додонова, С. Кавуна, І. Маркіна, В. Панченка, Г. Смоляна, О. Турчина та інших.

Одними з найважливіших аспектів питань інформаційної безпеки, на яких акцентувалась увага у наукових публікаціях, були такі, як формування системи управління інформаційною безпекою підприємств [4], [6], [10] та оцінка ризиків для бізнесу під час воєнного стану [1], [14]. При цьому в окремих наукових статтях [5] розроблені комплексні пропозиції з формування моделі системи менеджменту інформаційної безпеки підприємства.

Однак, швидкоплинність бізнес-процесів на підприємствах, непереборна дія факторів зовнішнього середовища, спричинених війною, необхідність оперативно реагувати на виклики зовнішніх факторів впливу, цифровізація економіки, змушують постійно шукати нові підходи в формуванні засобів захисту пов'язаних з менеджментом інформаційних систем підприємства. Виходячи з цього, виникає нагальна потреба у формуванні працюючого управлінського механізму протидії інформаційним загрозам та удосконаленні процесів організації інформаційної безпеки на вітчизняних підприємствах.

Постановка завдання. Метою дослідження є визначення ролі управління інформаційною безпекою підприємства під час війни у загальній системі менеджменту, а також оцінка стану інформаційної безпеки, придатності, результативності та ефективності СУІБ з погляду стандарту ISO/IEC 27001:2022, цілей та планів СУІБ, можливостей удосконалення і визначення потреби у коригувальних та запобіжних діях.

Методи дослідження. У науковій статті використано такі загальнонаукові і специфічні методи дослідження: аналізу й синтезу, узагальнення та класифікацій, наукової абстракції – застосування цих методів дозволило проаналізувати теоретичні джерела, використані під час дослідження; графічні методи використані для візуалізації результатів аналізу статистичної інформації.

Виклад основного матеріалу дослідження. Управління будь-якою соціально-економічною системою нерозривно пов'язане з інформаційними процесами. Інформація виконує роль основного елементу, який забезпечує взаємозв'язок у процесі

управління, адже саме вона містить дані, необхідні для аналізу ситуації та ухвалення управлінських рішень [6, с. 220].

Офіційне визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: «Інформаційна безпека – стан захищеності життєвоважливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [9].

Цифровізація та активний розвиток комп'ютерних технологій стали ключовими чинниками підвищення ефективності та продуктивності сучасної економіки. Водночас прогрес у сфері інформаційних технологій призвів до появи нових викликів у вигляді загроз, пов'язаних із вдосконаленням методів промислового шпигунства, створенням новітніх вірусних програм та використанням кібератак. Такі інструменти дають змогу зловмисникам швидко отримувати доступ до конфіденційної інформації, що зумовлює необхідність впровадження надійних систем захисту даних [11].

Існує потреба в створенні єдиного «інформаційного хабу» підприємства, який був би націлений на систематизацію та поєднання різних видів інформації, що циркулює на підприємстві, включаючи фінансову, технічну, маркетингову, юридичну, безпекову. Створення єдиного інформаційного простору дозволяє реалізувати єдиний безперервний цикл інноваційної діяльності підприємства, що гнучко враховує ринкові сигнали в процесі вдосконалення продукції, дозволяє якнайповніше задовільнити потреби клієнтів [10, с. 348].

Під час повномасштабної війни кількість кібератак та інших інцидентів в Україні значно зросла порівняно з довоєнним періодом. Згідно з даними Державної служби спеціального зв'язку та захисту інформації України, у 2024 році було зафіксовано 4315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році, коли їх було 2541. Основними цілями атак залишаються органи державної влади, медіаресурси, енергетична сфера та логістика. Водночас бізнес України також піддається кібератакам. Великі компанії, впроваджуючи ефективні системи управління інформаційною безпекою (СУІБ), здатні зменшити ризики пошкодження або знищення ключових елементів та ланок діяльності підприємств під час виникнення загроз.

Ключовими змінами, які повинні відбутися на більшості підприємств України, є прагнення до сертифікації за стандартами ISO/IEC 27001:2022 та отримання відповідних міжнародних сертифікатів. Цей стандарт встановлює вимоги до створення, впровадження, підтримки та вдосконалення СУІБ в контексті організації, а також до постійної оцінки інформаційних ризиків і ризик-менеджменту.

ISO/IEC 27001:2022 загалом описує структуру системи управління інформаційною безпекою (СУІБ) для компаній будь-якого розміру та всіх галузей діяльності. Система управління інформаційною безпекою (СУІБ) набуває ключового значення завдяки актуальності для багатьох компаній питань управління ризиками. З майже щоденною появою нових кіберзагроз та постійними змінами, компаніям, які прагнуть захистити свої бізнес-процеси та інформацію, важливо вміти ідентифікувати такі ризики та ефективно керувати ними.

Варто зазначити, що багато компаній мають певні елементи інформаційної безпеки, але вони часто носять формальний характер і не є затвердженою дорожньою картою дій під час війни. Наявність ефективної системи управління інформаційною

безпекою (СУІБ) на підприємстві, її правильне використання та управління є ключовими факторами для забезпечення захисту інформаційних активів та досягнення успіху в умовах сучасних кіберзагроз.

Під час війни підприємства зазнають значних змін. Коли йдеться про ризики воєнного часу, першими на думку спадають майнові втрати. Але є й інші важливі фактори, які бізнес повинен враховувати [14]:

- Законодавство та регуляторні вимоги стали змінюватись швидше, із меншим періодом від ухвалення законів до їх набуття чинності.
- Вимоги фінмоніторингу стали жорсткішими, а також посилилась відповідальність за співпрацю з контрагентами та фізособами російської федерації.
- Кількість ресурсів зменшилась, а ціна менеджерських помилок зросла. Тож для бізнесів є актуальною потреба в оптимізації процесів та управлінні ризиками.
- Щодня збільшується кількість даних та джерел, які потрібно постійно моніторити.

У сучасному бізнес-середовищі ефективне управління ризиками та постійне вдосконалення системи інформаційної безпеки стали глобальними трендами. Ці підходи дозволяють компаніям не лише зберігати стабільність, але й перетворювати виклики на можливості для розвитку. Намагання бізнесу пристосуватися до змін та ризиків відкриває перед ним можливості та перспективи за багатьма напрямами:

- для пошуку інвесторів (компанії, які ефективно управляють ризиками та адаптуються до змін, демонструють стабільність і надійність, що приваблює потенційних інвесторів);
- побудови довіри клієнтів (адаптивні підприємства здатні швидко реагувати на потреби та очікування клієнтів, що сприяє зміцненню довіри та лояльності споживачів);
- виходу на міжнародні ринки (гнучкість у бізнес-процесах дозволяє компаніям ефективно адаптуватися до різних культурних та економічних умов, що полегшує вихід на нові ринки);
- позитивного іміджу та репутації (підприємства, які демонструють здатність адаптуватися та ефективно управляти ризиками, формують позитивний імідж, що підвищує їх конкурентоспроможність та привабливість на ринку).

Таким чином, адаптивність бізнесу є ключовим фактором для досягнення успіху та сталого розвитку в умовах постійних змін та викликів.

Під час війни вплив на інформацію чи інформаційна зброя є достатньо потужним засобом ведення війни, оскільки її технологічна інноваційність, вседоступність та непомітність є дуже загрозливими. В умовах війни набуває вагомого значення інформаційна культури як фактор, що створює протидію інформаційній зброї серед бізнес-середовища та забезпечує сталий розвиток країни.

Під час війни ефективне управління інформаційною безпекою підприємства вимагає проактивного підходу, заснованого на прогнозуванні та передбаченні потенційних загроз. Такий підхід дозволяє з високою ймовірністю уникнути негативних наслідків інцидентів.

У період військових дій, коли час на розробку власних стандартів безпеки обмежений, важливо ефективно адаптувати передові міжнародні стандарти до реалій ведення бізнесу в Україні. Одним із таких стандартів є ISO/IEC 27001, який визначає вимоги до системи управління інформаційною безпекою (СУІБ).

Кращі традиції та практики безпеки підприємств відображаються у стандартах та рекомендаціях найвідомішої у світі асоціації фахівців з безпеки ASIS International

(США). В свою чергу напрямок з управління інформаційною безпекою детально описаний у міжнародному стандарті ISO/IEC 27001:2022 [13].

Згідно базових рекомендацій ASIS International підхід до організації безпеки може значно відрізнятися в залежності від розміру, галузі виробництва, ступеню автоматизації, економічного стану підприємства та інших факторів. Ключовою нормою вважається побудова цілісної, комплексної структури безпеки (рис. 1), що містить сім основних факторів. До цих напрямків безпеки належать:

1) Матеріальні активи;
2) Інформаційні активи;
3) Імідж та репутація;
4) Фінансові активи;
5) Персонал та інтелектуальна власність;
6) Ланцюг поставок;
7) Відповідність нормам.

Рис. 1. Комплексна структура безпеки підприємства [складено автором]

ASIS International пропонує стандарти та рекомендації, які допомагають адаптувати підхід до безпеки відповідно до цих факторів. Наприклад, стандарт "Security Risk Assessment" надає керівництво щодо проведення оцінки ризиків, зокрема фізичних, нефізичних та логічних ризиків, що дозволяє підприємствам розробити ефективні стратегії безпеки, враховуючи їхні унікальні обставини.

Таким чином, підхід до організації безпеки має бути гнучким та адаптованим до конкретних умов кожного підприємства, щоб забезпечити ефективний захист від потенційних загроз.

Система управління інформаційною безпекою підприємства є складовою частиною Системи менеджменту компанії. СУІБ має бути впроваджена за вимогами міжнародного стандарту ISO/IEC 27001 та функціонувати згідно моделі/циклу PDCA (Плануй-Дій-Контролюй-Вдосконалюй) [8]. Даний цикл є ключовим для впровадження та підтримки СУІБ.

Система управління інформаційною безпекою спрямована на досягнення цілей, що стосуються захисту суб'єктів інформаційних відносин (інтереси яких зачіпаються при створенні та функціонуванні паперового та електронного документообігу Підприємства) від можливого нанесення їм відчутного матеріального, фізичного, морального чи іншого збитку за допомогою випадкового або навмисного несанкціонованого втручання в процес функціонування документообігу Підприємства або несанкціонованого доступу до циркулюючої в ньому інформації і її незаконного використання [2, с. 64].

Зазначена мета досягається за допомогою забезпечення і постійної підтримки наступних властивостей інформації та автоматизованої (цифровізованої) системи її обробки:

- доступності оброблюваної інформації для дозволених користувачів (стабільного функціонування документообігу Підприємства, при якому користувачі мають можливість отримання необхідної інформації та результатів вирішення завдань за прийнятний для них час);
- збереження в таємниці (забезпечення конфіденційності) певної частини інформації, що зберігається, оброблюється і надсилається по каналах зв'язку;
- цілісності і автентичності (підтвердження авторства) інформації, що зберігається та обробляється в системі документообігу Підприємства і надсилається по каналах зв'язку.

Для досягнення основної мети захисту і забезпечення вказаних властивостей інформації і системи її обробки система управління інформаційною безпекою документообігу підприємства забезпечує ефективне вирішення таких завдань:

- захист від втручання в процес функціонування паперового та електронного документообігу Підприємства сторонніх осіб;
- розділення доступу користувачів, що зареєстровані до апаратних, програмних і інформаційних ресурсів документообігу підприємства;
- реєстрацію дій користувачів при використанні ресурсів, що захищаються, документообігу підприємства в системних журналах і періодичний контроль коректності дій користувачів системи шляхом аналізу вмісту цих журналів фахівцями компанії;
- контроль цілісності (забезпечення незмінності) середовища здійснення програм і їх відновлення у разі пошкодження;
- захист від несанкціонованої модифікації та контроль цілісності програмних засобів, що використовуються у документообігу Підприємства, а також захист системи від впровадження несанкціонованих програм, включаючи комп'ютерні віруси;
- захист інформації обмеженого користування від витоку через персонал або по технічних каналах при її обробці, зберіганні і передачі;
- захист інформації обмеженого користування, що обробляється, зберігається і надходить від несанкціонованого розголошення чи спотворення;
- забезпечення ідентифікації користувачів, що приймають участь в обміні інформацією;
- своєчасне виявлення джерел загроз безпеці інформації, причин і умов, що сприяють нанесенню збитку зацікавленим суб'єктам інформаційних відносин, створення механізму оперативного реагування на загрози безпеці інформації та негативні тенденції;

• створення умов для мінімізації та локалізації шкоди, що завдається неправомірними діями фізичних та юридичних осіб, ослаблення негативного впливу та ліквідація наслідків порушення безпеки інформації.

На зміни та удосконалення СУІБ впливають:

• зміни регуляторних вимог;

• середовище підприємства, зміни середовища, а також ризики, пов'язані з цим середовищем;

• цілі СУІБ;

• впровадження нових систем та засобів документообігу, нових технологій зберігання та обробки інформації виходячи з цифровізації виробничих процесів;

• зміни в процесах СУІБ та структурі СУІБ;

Основними методами вдосконалення системи управління інформаційною безпекою є проведення коригувальних та запобіжних дій. Причиною впровадження коригувальних та запобіжних дій можуть бути існуючі або потенційні невідповідності, виявлені під час внутрішніх або зовнішніх аудитів СУІБ, аналізу СУІБ зі сторони керівництва, виявлені співробітниками підприємства під час виконання своїх повсякденних задач, виникнення інциденту інформаційної безпеки.

Коригувальні дії спрямовані на усунення причин *виявлених* невідповідностей. Запобіжні ж дії спрямовані на усунення причин *потенційних* невідповідностей.

Для забезпечення ефективної розробки і проведення корегувальних дій, необхідно вирішення наступних питань:

• оперативний розгляд інцидентів інформаційної безпеки, внутрішніх невідповідностей процесів СУІБ;

• дослідження та аналіз причин невідповідностей;

• розробка коригувальних дій, необхідних для усунення причин невідповідностей;

• реалізація коригувальних дій і здійснення контролю їх виконання;

• оцінка результативності проведення коригувальних заходів та внесення змін в документацію СУІБ (при необхідності);

• інформування керівництва підприємства з метою проведення аналізу, виявлення проблем, поліпшення процесів та оцінки результативності СУІБ.

Управління інформаційною безпекою є постійним процесом, який вимагає постійного вдосконалення та адаптації до нових загроз і технологій. Підприємства повинні постійно оцінювати ефективність своїх заходів безпеки та вносити необхідні зміни для підтримки високого рівня захисту.

Отже, інформаційна безпека на підприємстві в умовах війни є ключовою для забезпечення безпеки, стійкості та успішності бізнесу в сучасному цифровому середовищі.

Висновки та перспективи подальших досліджень. За результатами проведеного дослідження, що розкриває проблеми менеджменту інформаційної безпеки підприємства, було проаналізовано основні міжнародні стандарти системи управління інформаційною безпекою підприємств, визначені ключові елементи та підходи в організації системи менеджменту інформаційної безпеки, а також виділено основні властивості інформації та автоматизованої системи її обробки.

Визначені фактори, що впливають на зміни та удосконалення системи управління інформаційною безпекою підприємства, серед яких головні:

• внутрішнє середовище підприємства, зміни середовища, а також ризики, пов'язані з цим середовищем;

- впровадження нових систем та засобів документообігу, нових технологій зберігання та обробки інформації виходячи з цифровізації виробничих процесів;
- зміни в процесах та структурі системи управління інформаційною безпекою підприємства під впливом дії зовнішнього середовища та дії обставин непереборної сили.

Обґрунтовано, що серед основних підходів в організації системи управління інформаційною безпекою підприємств під час війни є підхід, що базується на прогнозуванні та передбачуваності можливих загроз.

В перспективі подальших досліджень може бути практична апробація впровадження системи управління інформаційною безпекою на підприємствах виробничої сфери.

---

1. Актуальні проблеми управління інформаційною безпекою держави. X Всеукраїнська науково-практична конференція [Електронний ресурс]: URL: http://academy.ssu.gov.ua/upload /file/konf_04_04_2019.pdf
2. Архипов О. Є., Архипова Є. О. Положення про інформаційну безпеку в міжнародних стандартах. *Інформаційна безпека людини, суспільства, держави*. Київ, 2010. № 2 (4). С. 62-65.
3. Василюк В. Я., Климчик С. О. Інформаційна безпека держави. Київ: ВД «Скіф», 2008. 136 с.
4. Кавун С.В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2008. 352 с.
5. Маркіна І.А., Дячков Д.В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємства*. 2016. №3 (1). С. 80-88.
6. Панченко В.А. Менеджмент інформаційної безпеки комерційного підприємства. *Центральноукраїнський науковий вісник. Економічні науки*. 2019. вип. 3(36). С. 219-228.
7. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5 липня 1994 року. № 80/94. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
8. Про інформацію. Закон України від 2 жовтня 1992 року № 2657-XII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
9. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 9 січня 2007 року. № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст.102.
10. Турчин О.І. Інформаційна безпека процесів менеджменту інтегрованих систем. *Моделювання регіональної економіки*. 2010. № 2. С. 347-352.
11. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. *Ефективна економіка.* 2014. №5. [Електронний ресурс]: URL : http://www.economy.nayka.com.ua/?op =1&z=3304
12. Что такое цикл PDCA и в чем его преимущества? [Електронний ресурс]: URL : https://bpi-group.com.ua/blog/chto-takoe-czykl-pdca/
13. ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements.
14. 5 найважливіших ризиків для бізнесу під час війни. [Електронний ресурс]: URL: https://biz.ligazakon.net/news/225615_5-nayvazhlivshikh-rizikv-dlya-bznesu-pd-chas-vyni

References

1. Aktual′ni problemy uhliadynnia informatsiynoi bezpeky derzhavy. Vseukrainska naukovo-praktychna konferentsiya. (2019). Retrieved from: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf
2. Arkhipov O. Ye., Arkhipova, Ye. O. (2010). Polozhennia pro informatsiinu bezpeku v mizhnarodnykh standartakh. *Informatsiina bezpeka lyudyny, suspil'stva, derzhavy.* 2(4). Pp. 62-65.
3. Vasiliuk, V. Ya., Klymchyk, S. O. (2008). Informatsiina bezpeka derzhavy. Kyiv: KNT Vydavnytstvo "Skif." 136 p.
4. Kavun, S. V. (2008). Informatsiina bezpeka: Navchalnyi posibnyk. Ch. Vydavnytstvo KhNEU. 352 p.
5. Markina, I. A., Diachkov, D. V. (2016). Osnovy formuvannia systemy menedzhmentu informatsijnoi bezpeky pidpryiemstva. *Problemy i perspektyvy rozvytku pidpryiemnytstva.* 3 (1). Pp. 80-88.
6. Panchenco, V. A. (2019). Menedzhment informatsiinoi zabezpeky komertsiinoho pidpryiemstva. *Tsentralnoukrainskyi naukovyi visnyk. Ekonomichni nauky*. 3(36). Pp. 219-228.
7. Pro zakhyst informatsii v informatsiyno-telekomunikatsiynykh systemakh. Zakon Ukrainy vid 5 lypta 1994 roku № 80/94. Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
8. Pro Informatsiiu. Zakon Ukrainy vid 2 zhovtnia 1992 roku. № 2657-XII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text
9. Pro Osnovni zasady rozvytku informatsiinoho suspil′stva v Ukraini na 2007-2015 roky. Zakon Ukrainy vid 9 sichnia 2007 roku. № 537-V
10. Turchyn, O. I. (2010). Informatsiina bezpeka protsesiv menedzhmentu intehrovanykh system. *Modeliuvannia rehional'noi ekonomiky*. № 2. Pp. 347-352.
11. Cherevko, O. V. (2014). Teoretychni zasady ponyttia informatsiinoi bezpeky ta klasyfikatsiia zahroz systemi informatsiinoho zakhystu. *Efektyvna ekonomika* №5. Retrieved from: http://www.economy.nayka.com.ua/?op= 1&z=3304
12. Chto takoe tsikl PDCA i v chem ego preimushchestva? BPI Group. Retrieved from: https://bpi-group.com.ua/blog/chto-takoe-czykl-pdca/
13. ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements.
14. 5 nayvazhlivshykh ryzykiv dlia biznesu pid chas viyny. Liga Zakon. Retrieved from: https://biz.ligazakon.net/news/225615_5-nayvazhlivshikh-rizikv-dlya-bznesu-pd-chas-vyni

ORGANIZATIONAL FEATURES OF THE INFORMATION SECURITY MANAGEMENT SYSTEM OF ENTERPRISES UNDER THE CONDITIONS OF WAR AND ECONOMY DIGITALIZATION

Andriy Denysenko[1], Rostislav Sabluk[2]

[1, 2] «Private higher educational institution "European University"
03115, Kyiv, Academician Vernadskyi Boulevard, 16 V
[1]e-mail: andriy.denysenko@e-u.edu.ua: ORCID: 0009-0007-8057-9444
[2]e-mail: rostyslav.sabluk@e-u.edu.ua; ORCID: 0009-0002-7085-3028

Abstract. The article examines the organizational aspects of managing information security systems in enterprises, particularly during wartime when risks to information resources significantly increase. It outlines key challenges modern enterprises face and

proposes solutions to them. Emphasis is placed on the importance of a systematic approach to protecting information assets, which includes identifying vulnerabilities, recognizing potential threats, and developing action plans to mitigate their impact. Special attention is given to analyzing key terms and concepts related to information security, facilitating the systematization of knowledge in this field. The article justifies the relevance of implementing an effective information security system amid the digitalization of the economy, where commercial enterprises increasingly rely on information systems and technologies. It is determined that implementing comprehensive protective measures not only reduces risk levels but also enhances the competitiveness of enterprises in the market.

The article analyzes the practical application of the ISO/IEC 27001:2022 standard as a foundation for developing an information security management system. Key requirements of this standard are discussed, including risk assessment, implementation of security policies, staff training, and regular audits of information systems. The importance of integrating these measures into the overall enterprise management strategy to achieve optimal results is emphasized. A particular focus is placed on the specifics of managing information security during wartime, when enterprises face new challenges such as cyberattacks, disruptions in supply chains, and the need to operate under limited resource access. The article offers specific recommendations for adapting the management system to these conditions, including data backup, use of cloud technologies for information storage, implementation of multi-factor authentication, and increasing employee awareness of cyber threats. The study also analyzes the impact of the human factor on the level of information security in enterprises. It is noted that insufficient employee awareness of modern cyber threats can lead to significant data breaches. The authors emphasize the importance of conducting regular training, simulation exercises, and professional development programs to foster a culture of information security within the organization. The research underscores the importance of revising approaches to information security in the context of contemporary challenges. The proposed changes aim to enhance the resilience of enterprises to threats, ensure the continuity of business processes, and maintain customer trust even under challenging conditions. Thus, a systematic approach to managing information security serves as a guarantee of successful enterprise operation amid digitalization and increased risks.

Keywords: security, management, enterprise, information protection, management, threats, information security, digitalization.

Стаття надійшла до редколегії 24.10.2024
Прийнята до друку 25.11.2024