ІНФОРМАЦІЙНІ РЕСУРСИ ТА СИСТЕМИ
INFORMATION RESOURCES AND SYSTEMS

UDC 681.3.06: 519.248.681

Ihor B. Chepkov[1], D. S. (Engineering), Professor
ORCID ID 0000-0002-4294-4152 ***e-mail:*** *i.chepkov@mil.gov.ua*

Valerii V. Zubariev[1], D. S. (Engineering), Professor
ORCID ID 0000-0002-4998-726X ***e-mail:*** *doktorzubarev.2016@gmail.com*

Oleksandr O. Sverhunov[2], PhD, Associate Professor, Leading Researcher
ORCID ID 0000-0002-2158-1532 ***e-mail:*** *asverg@niss.gov.ua*

Oleksandr V. Zubariev[1], PhD, Senior Researcher, Leading Researcher
ORCID ID 0000-0001-5590-7660 ***e-mail:*** *aleksanderzubarev@gmail.com*

[1]Central Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
[2]National Institute for Strategic Studies, Kyiv, Ukraine

ON THE DEVELOPMENT OF DAMAGE OF INFORMATION SYSTEM OPERATIONS AND METHODOLOGICAL ISSUES OF ASSESSMENT OF THE EFFICIENCY OF INFORMATION SECURITY SYSTEMS

Abstract. *The paper analyzes the trends in threats to the functioning of information and telecommunication systems and methodological issues of evaluating the effectiveness of the information security system for protected objects. Based on the results of the analysis, a methodology for assessing the state of the effectiveness of information security systems has been proposed. It is shown that the development of assessment methodologies should be carried out on the basis of statistical and system analysis using expert methods, taking into account the fact that the assessment of the effectiveness of information security systems and its components is assessed with a large number of uncertainties and differences. The approach of assessing the state of the effectiveness of information security systems for an object of protection based on the risk management of business processes has been analyzed. It is substantiated that, depending on the goals and objectives of the assessment, it is possible to change both the main factors and the second level assessment factors and calculate them based on expert assessments of third level factors that affect the level of information security.*
Key words: *information systems; information and communication technologies; information security; information security systems; information systems risk management; information security; methods of assessing the effectiveness of systems; information security*

І.Б. Чепков[1], **В.В. Зубарєв**[1], **О.О. Свергунов**[2], **О.В. Зубарєв**[1]

[1]Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, м. Київ, Україна
[2]Національний інститут стратегічних досліджень, м. Київ, Україна

ЩОДО РОЗВИТКУ ЗАГРОЗ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ І МЕТОДОЛОГІЧНІ ПИТАННЯ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *В роботі проаналізовані тенденції розвитку загроз функціонування інформаційних та телекомунікаційних систем і методологічні питання оцінки ефективності системи забезпечення інформаційної безпеки об'єкта захисту. На основі результатів аналізу запропоновано методику оцінки стану ефективності систем забезпечення інформаційної безпеки. Показано, що розробку методик оцінки необхідно здійснювати на основі статистичного та системного аналізу з використанням експертних методів з урахуванням того, що оцінка стану ефективності систем забезпечення інформаційної безпеки та її складових є багатокритеріальною з великою кількістю невизначеностей та суперечностей. Проаналізовано підхід до оцінки стану ефективності систем забезпечення інформаційної безпеки об'єкта захисту на основі ризик-менеджменту бізнес-процесів. Обґрунтовано, що в залежності від цілей та завдань оцінки можливо змінювати як головні фактори, так і фактори оцінки другого рівня і розраховувати їх на основі експертних оцінок факторів третього рівня, що впливають на рівень інформаційної безпеки.*

Ключові слова: *інформаційні системи; інформаційно-комунікативні технології; інформаційна безпека; системи забезпечення інформаційної безпеки; ризик-менеджмент систем забезпечення інформаційної безпеки; методика оцінки стану ефективності систем забезпечення інформаційної безпеки*

Вступ

Розвиток інформаційно-комунікативних технологій (ІКТ) та інформаційних систем (ІС) у XXI ст. має глобальний характер і став невід'ємною частиною всіх сфер діяльності держав, компаній, суспільства та окремих осіб. Їх ефективне застосування стало фактором прискорення економічного розвитку держав, забезпечення реалізації стратегічних національних пріоритетів, національної безпеки і оборони, формування інформаційного суспільства.

Разом з тим переваги сучасного цифрового світу, розвитку ІКТ та ІС обумовили виникнення нових загроз економіці, національній та міжнародній безпеці, обороні в інформаційній сфері. Застосування ІКТ у якості інструмента політичного та економічного протиборства може призвести до значного збитку для економіки держави і навіть дестабілізувати соціально-політичну обстановку в суспільстві. За таких обставин стійке функціонування інформаційної сфери стає необхідною умовою для ефективного соціально-економічного розвитку країни і забезпечення її безпеки.

В той же час розширення застосування ІКТ та ІС породжує проблеми забезпечення інформаційної безпеки (ІБ) їх функціонування. Поряд із інцидентами природного (ненавмисного) походження таких загроз поширюються випадки незаконного збирання, зберігання, використання,

знищення, поширення інформації, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства, у тому числі й у мережі Інтернет. Зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. За даними Всесвітнього економічного форуму, у 2017 році втрати тільки від кібератак у світі склали порядку трильйона доларів США, і, на думку експертів, якщо не вживати ефективних, результативних заходів щодо захисту інформації, збиток буде ще більшим. І ця тенденція продовжує зростати. Тільки в першому кварталі 2018 року в порівнянні з аналогічним періодом 2017 року число кібератак на російські інформаційні ресурси збільшилося на третину [1].

Проблеми забезпечення ІБ вже сьогодні розглядаються навіть на рівні держав. Наприклад, президент США Д. Трамп 15 травня 2019 року підписав указ про введення режиму надзвичайного стану для захисту інформаційних і комунікаційних мереж США від іноземних загроз. Документ забороняє угоди у сфері інформаційних або комунікаційних технологій або послуг, якщо вони розроблені, вироблені або поставляються іноземними супротивниками США і можуть нести загрозу інформаційним і комунікаційним технологіям США, мати катастрофічний вплив на безпеку критичної інфраструктури США або представляти інші загрози національній безпеці США. Раніше в США заявляли про загрози національній безпеці з боку китайської компанії Huawei. США вважають, що устаткування компанії використовується для шпигунства на користь Китаю. У серпні 2018 року президент США Д. Трамп заборонив урядовим відомствам використовувати устаткування компаній Huawei і ZTE [2, 3]. Міністерство оборони (МО) США включило Росію в список країн, послугами яких заборонено користуватися при комерційних запусках супутників. Виправлення в правилах закупівель в оборонних цілях розміщені на сайті федерального регістру і набудуть чинності з 31 травня 2019 року. У документі відзначається, що нові обмеження вводяться щодо супутників і засобів виведення (супутників) на орбіту для надання послуг супутникового зв'язку. Заборона буде стосуватися випадків, коли виникає ризик у сфері інформаційної безпеки (ІБ), зокрема кібербезпеки [4]. Адміністрація США, включаючи Росію в список країн, у відношенні яких уже діяла аналогічна заборона: КНР, КНДР, Іран, Судан і Сирія, показує, яку велику увагу вони приділяють сфері ІБ. Правило почне діяти з 2023 року. Воно не торкнеться космічних запусків, які відбудуться до 31 грудня 2022 року. МО США також забороняють контракти з іноземними державами на проведення комерційного супутникового обслуговування, оскільки подібні угоди також можуть створити неприйнятний ризик у сфері кібербезпеки для США.

У сучасному цифровому світі кіберзлочинність є ключовою загрозою зростанню світової економіки. Питання ІБ, а також управління критичною інфраструктурою інтернету регулярно обговорюються в міжнародних організаціях. Таким чином, проведений вище аналіз показує, що дослідження проблем ІБ є дуже актуальним питанням.

Постановка наукової проблеми із забезпечення оцінок системи інформаційної безпеки

У міру розвитку ІКТ та ІС, а також їх застосування розширювався та буде розширюватися спектр інформаційних загроз їх функціонування [5, 6, 7, 8 тощо].

Це також обумовило велику увагу до наукових досліджень проблеми різних аспектів ІБ як функціонування ІКТ та ІС, так і об'єктів (компаній, організацій тощо) захисту [9, 10 тощо].

В той же час ряд досліджень показують наявність нових проблем в цій сфері. Так, *«Глобальне дослідження з питань інформаційної безпеки. Перспективи на 2014 рік»* (The Global State of Information Security. Survey 2014), яке проведено фірмою PWC і журналами CIO і CSO, показує, що стратегії інформаційної безпеки, які традиційно були засновані на дотриманні нормативно-правових вимог і обмежувалися лише інформаційним захистом периметра, не встигають за зростаючим рівнем ризиків у сфері ІБ [11, 12]. Тому у сфері ІБ формується нова модель, в якій інформаційні загрози для ІС та ТКС є бізнес-ризиками. Ризики, пов'язані з безпекою інформації, слід розглядати як загрози для самої організації. Наприклад, у липні 2017 року стався один з найбільших витоків персональних даних у бюро кредитної історії Equifax у США. У руки зловмисників потрапили особисті відомості більш ніж 143 млн споживачів, 209 000 номерів кредитних карт. У результаті, за даними на 8 вересня 2017 року, акції бюро впали на 13% [13].

Надзвичайно важливо прогнозувати такі загрози, розуміти вразливі місця організації, уміти виявляти пов'язані з ними ризики і управляти такими ризиками [8].

Інформаційні процеси більше не можуть бути відділені від бізнес-процесів організації. Інформація стає органічною складовою практично всіх аспектів діяльності організації, як основної, так і допоміжної. З позицій економічного аналізу, з одного боку, інформація є товаром, який має специфічні властивості. З іншого боку, інформація є стратегічним ресурсом суб'єкта економічної діяльності. Однак в обох випадках цієї діяльності проявляється фундаментальна потреба – забезпечити її безпеку.

Застосування цієї нової моделі ІБ припускає, що в основі будь-якої діяльності та інвестиційних рішень повинне бути чітке розуміння того, що являють собою наявні в організації інформаційні ресурси, які існують загрози від функціонування ІС та ТКС для системи бізнесу, які ділянки бізнесу з використанням ІС та ТКС найбільш уразливі, а також мати результати моніторингу інформаційної діяльності організації, щоб вона охоплювала не тільки ІС та ТКС, а й всіх співробітників, починаючи з вищих посадових осіб, що ухвалюють для себе зобов'язання з організації і забезпечення інформаційної безпеки, і закінчуючи кожним співробітником і всіма третіми особами. При цьому необхідно співробітничати з державними установами і приватними компаніями для більш ефективного обміну інформацією про виникаючі загрози ІБ. Вищезгадана модель ІБ потребує формування нових методичних підходів з оцінки системи забезпечення ІБ для всієї організації.

Тому **метою статті є** дослідження методичних підходів з формування методів оцінки системи забезпечення ІБ організації на основі експертних методів та системних поглядів на процеси ІБ. Такі методики в подальшому можливо використати в оцінках управління ризиками бізнес-процесів з урахуванням проблем ІБ.

Характеристика проблеми інформаційної безпеки

Нині питання забезпечення інформаційної безпеки держав, міністерств, окремих компаній та інших державних і приватних установ, суспільства і осіб стали розглядатись як в контексті забезпечення національної безпеки держав, так і як окремий напрям діяльності, що впливає на оборону, безпеку економічної і фінансової діяльності соціально-економічних систем тощо. Наприклад, на питаннях забезпечення інформаційної безпеки США в рамках міждержавної стратегічної конкуренції акцентується увага в Стратегії національної безпеки США (National Security Strategy, NSS) [14], яку затвердив президент та оприлюднив 18 грудня 2017 року, та в Національній оборонній стратегії США (National Defense Strategy, NDS), яку підписав Міністр оборони і яку частково оприлюднено 19 січня 2018 року [15]. Ця NDS – перша після 2008 року.

Голова ОКНШ генерал армії США М. Демпсі в червні 2015 року підписав Національну військову стратегію (The National Military Strategy, NMS), попередня версія якої була випущена в 2011 році. У цій військовій стратегії особлива увага приділяється переважаючій в цей час тактиці гібридних війн, в рамках яких застосовуються нові технології, інформаційні війни та забезпечується ІБ існуючих ІС та ТКС [16].

В Національній стратегії кібербезпеки (The National Cyber Strategy, NCS), яку президент США Д. Трамп підписав та оприлюднив у вересні 2018 року, також акцентується увага на посиленні інформаційних загроз національній безпеці США [17]. Згідно з цим документом Міністерству внутрішньої безпеки (Department of Homeland Security, DHS) надані повноваження на забезпечення інформаційної безпеки федеральних міністерських і відомчих мереж, за винятком ІС національної безпеки Міністерства оборони (Department of Defense, DOD) та ІС розвідувального співтовариства (Intelligence Community).

В новій національній кіберстратегії США проголошено настання «нової ери стратегічного суперництва» в інформаційній сфері. У США заявили, що вони можуть розпочати наступальні кібероперації у відповідь на зловмисні дії держав, злочинних та терористичних організацій, які прагнуть викрасти у США інтелектуальну власність, персональні дані, заподіяти шкоду їхній інфраструктурі та навіть підірвати їх демократію за допомогою кіберінструментів. Для подолання цих викликів і забезпечення кібербезпеки в США поставлені завдання щодо вдосконалення інформаційних технологій, процвітання сектору сучасних технологій і підвищення ефективності серед представників співтовариства інформаційних технологій. Стратегія пропонує федеральному уряду вживати заходів для забезпечення довгострокового поліпшення стану безпеки в кіберпросторі для всіх американців.

У Стратегії кібербезпеки України також акцентується увага на тому, що кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства, бізнесу і держави [18].

У Доктрині інформаційної безпеки України [19] зафіксовано, що «комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації», а Міністерство оборони України має організовувати і забезпечувати супроводження інформаційними засобами

виконання завдань оборони України. Тому розробка методологічних підходів до оцінки інформаційної безпеки, у тому числі у сфері оборони, є дуже актуальним питанням.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [20]. Згідно із цим Законом (ст. 8) національна система кібербезпеки України є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Функціонування національної системи кібербезпеки забезпечується шляхом (серед іншого):

– впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.

Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

В 2016 році в РФ була затверджена нова Доктрина інформаційної безпеки РФ, в якій представлена система офіційних поглядів на забезпечення національної безпеки РФ в інформаційній сфері. Під інформаційною сферою розуміється сукупність інформації, об'єктів інформатизації, інформаційних систем, сайтів в інформаційно-телекомунікаційній мережі «Інтернет», мереж зв'язку, інформаційних технологій, суб'єктів, діяльність яких пов'язана з формуванням і обробкою інформації, розвитком і використанням названих технологій, забезпеченням інформаційної безпеки, а також сукупність механізмів регулювання відповідних суспільних відносин. Вищезазначена Доктрина стала основою в РФ для: формування державної політики в області забезпечення ІБ РФ; підготовки пропозицій з удосконалювання правового,

методичного, науково-технічного і організаційного забезпечення ІБ РФ; розробки цільових програм забезпечення ІБ РФ [21].

В РФ існує закон «Про інформацію, інформаційні технології і про захист інформації» (Федеральный закон «Об информации, информационных технологиях и о защите информации»). Цей закон визначає і закріплює права на захист інформації та інформаційну безпеку громадян і організацій в ЕОМ і в інформаційних системах, а також питання інформаційної безпеки громадян, організацій, суспільства і держави. У законі дане правове визначення поняття «інформація»: «інформація – відомості (повідомлення, дані) незалежно від форми їх представлення» [22].

В РФ закон «О безопасности критической информационной инфраструктуры» [23] регулює відносини у сфері забезпечення безпеки критичної інформаційної інфраструктури РФ із метою її стійкого функціонування при проведенні у відношенні її комп'ютерних атак. Критична інформаційна інфраструктура (КІІ) являє собою сукупність об'єктів КІІ, а також мережі електрозв'язку, які використовуються для організації взаємодії таких об'єктів. У цьому законі безпека критичної інформаційної інфраструктури розуміється як стан захищеності КІІ, що забезпечує її стійке функціонування при проведенні у відношенні її комп'ютерних атак. Об'єктами КІІ є інформаційні системи, інформаційно-телекомунікаційні мережі, автоматизовані системи управління суб'єктів КІІ. Суб'єктами КІІ є державні органі, державні установи, російські юридичні особи і (або) індивідуальні підприємці, яким на праві власності, оренди або на іншій законній підставі належать інформаційні системи, інформаційно-телекомунікаційні мережі, автоматизовані системи управління, що функціонують у сфері охорони здоров'я, науки, транспорту, зв'язку, енергетики, банківській сфері та інших сферах фінансового ринку, паливно-енергетичного комплексу, в області атомної енергії, оборонної, ракетно-космічної, гірничодобувної, металургійної і хімічної промисловості, російські юридичні особи і (або) індивідуальні підприємці, які забезпечують взаємодію зазначених систем або мереж. Під автоматизованою системою управління (АСУ) розуміється комплекс програмних і програмно-апаратних засобів, призначених для контролю над технологічним і (або) виробничим устаткуванням (виконавчими пристроями) і виробленими ними процесами, а також для управління такими устаткуванням і процесами. У вищезазначеному законі комп'ютерна атака розглядається як цілеспрямований вплив програмних і (або) програмно-апаратних коштів на об'єкти КІІ, мережі електрозв'язку, використовувані для організації взаємодії таких об'єктів, з метою порушення і (або) припинення їх функціонування і (або) створення загрози безпеці оброблюваної такими об'єктами інформації. Комп'ютерний інцидент розглядається як факт порушення і (або) припинення функціонування об'єкта КІІ, мережі електрозв'язку, яка використовується для організації взаємодії таких об'єктів, і (або) порушення безпеки оброблюваної таким об'єктом інформації, у тому числі що відбувся в результаті комп'ютерної атаки.

Значимий об'єкт КІІ розглядається як об'єкт КІІ, якому привласнено одну з категорій значимості і який включений до реєстру значимих об'єктів КІІ.

Аналіз нормативно-правової бази деяких країн з питань ІБ, включаючи кібернетичну безпеку, показує, що ІБ нині приділяється дуже велика увага на різних рівнях.

Характеристика державних структур провідних країн з проблем інформаційної безпеки

З 90-х років XX ст. по мірі зростання загроз ІБ провідні країни почали формувати спеціальні державні структури з питань ІБ. Основними завданнями таких структур були: оцінка загроз державам у сферах інформаційної безпеки або кібербезпеки; розробка пропозицій для урядів та приватного бізнесу зі зменшення таких загроз тощо.

Кібербезпека розглядається одним із напрямів ІБ, у рамках якого вивчають процеси формування, функціонування і еволюції кібероб'єктів, для виявлення джерел кіберзагроз, що утворюються при цьому, визначення їх характеристик, а також їх класифікацію і формування нормативних документів, виконання яких повинне гарантувати захист кібероб'єктів від усіх виявлених і вивчених джерел загроз кібербезпеки. Кібербезпека – це процес використання заходів безпеки для забезпечення конфіденційності, цілісності і доступності даних у кібернетичному просторі.

У жовтні 2016 року почав функціонувати національний центр кібербезпеки Великобританії (англ. National Cybersecurity Center, NCSC), який є організацією уряду Великобританії, щоб допомогти британським організаціям краще захищатися від нападу хакерів і реагувати на інциденти (своєчасне виявлення кібератак і їх швидке усунення), пов'язані з кібернетичною безпекою [24].

NCSC є частиною британського агентства з електронної розвідки, інформації та урядового зв'язку GCHQ (англ. Government Communications Headquarters). GCHQ за своїми функціями співставно з Агентством національної безпеки (АНБ) США.

Національний центр кібернетичної безпеки NCSC почав роботу в рамках п'ятирічної стратегії з бюджетом в £1.9 млрд. Згідно з офіційними заявами центр є першою «кіберсилою» країни, якій доручено займатися великими кібернетичними інцидентами. Завдяки роботі GCHQ, NCSC може виявити кібератаки з усього світу.

За повідомленнями ЗМІ, в завдання Національного центру кібернетичної безпеки Великобританії стали входити завдання активної відповіді на кібератаки.

Національний центр кібербезпеки (нім. Nationales Cyber-Abwehrzentrum, NCAZ) Федеративної Республіки Німеччини – міжвідомче урядове агентство, створене для захисту від кібератак критично значимих об'єктів національної IT-інфраструктури і економіки. У відповідності до «Стратегії кібербезпеки для Німеччини» кібератака – це дія, яка спрямована проти однієї або декількох IT-систем з метою злому їх систем безпеки. BSI відносить до різновидів кібератак, зокрема, крадіжки особистих даних, хакерські атаки, поширення комп'ютерних вірусів, Dos-атаки, атаки на інфраструктуру Інтернету тощо.

Національний центр кібербезпеки створений на підставі рішення уряду Німеччини від 23 лютого 2011 року та вступив у дію 1 квітня 2011 року. Офіційне відкриття NCAZ відбулося 16 червня 2011 року. NCAZ перебуває в головному офісі Федерального управління з інформаційної безпеки (BSI) у Бонні. Необхідність створення NCAZ була пов'язана з ростом з 2005 року числа хакерських атак на комп'ютерні системи органів влади та комерційних підприємств у Німеччині, у тому числі появою комп'ютерних вірусів Ghostnet

і Stuxnet. У відповідності з рекомендаціями BSI, NCAZ веде, зокрема, збір інформації про терористичні загрози, виявлення уразливостей в IT-продуктах і IT-інцидентах і аналіз цих даних. NCAZ веде свою діяльність в інтересах цивільних організацій. Питаннями кібербезпеки у військовій сфері в Німеччині з 2002 року займається аналогічна організація – Команда стратегічної розвідки.

NCAZ поєднує засоби кібербезпеки BSI, Федерального відомства із захисту Конституції, Федеральної розвідувальної служби (BND), Федеральної поліції, слідчого управління митниці Німеччини, Бундесверу, Федерального управління цивільного захисту і допомоги при стихійних лихах і Федерального відомства карної поліції, а також співробітничає з наглядовими органами операторів критично важливої інфраструктури, у межах своїх статутних обов'язків і повноважень. Основою взаємодії є «угоди про співробітництво» відповідних органів і відомств Німеччини.

NCAZ також співробітничає з інститутами ЄС, з використанням ресурсів існуючих органів країн ЄС, що займаються питаннями кібербезпеки. BSI також співробітничає з Європейським агентством із мережевої і інформаційної безпеки (англ. – ENISA).

У рамках ЄС створений Центр електронної кіберзлочинності під егідою Європола.

Найбільш розвинена інфраструктура щодо забезпечення ІБ розгорнута у США у різних відомствах. Наприклад, Національний центр кібербезпеки (англ. National Cybersecurity Center, NCSC) – підрозділ міністерства внутрішньої безпеки США, створений в березні 2008 року відповідно до Директив NSPD-54/HSPD−23, перебуває в прямому підпорядкуванні міністра внутрішньої безпеки. На Центр покладений кібернетичний захист мереж зв'язку уряду США, включаючи моніторинг, збір і обмін інформацією про системи, що належать АНБ, ФБР, МО та міністерству внутрішньої безпеки.

Характеристика національних і міжнародних стандартів з питань інформаційної безпеки

У міру розвитку ІС і ТКС відбувається розвиток систем їх ІБ і стандартів з класифікації, сертифікації, аудиту, побудови та іншим аспектів як самих ІС і ТКС, так і систем забезпечення їх ІБ. Використання стандартів ІБ сприяє вирішенню наступних завдань:

– строго визначаються цілі забезпечення ІБ інформаційних і телекомунікаційних систем;

– створюється ефективна система управління ІБ;

– забезпечуються розрахунки сукупності деталізованих не тільки якісних, але й кількісних показників для оцінки відповідності ІБ заявленим цілям;

– створюються умови застосування наявного інструментарію (програмних і апаратних засобів) забезпечення ІБ і оцінки її поточного стану;

– відкривається можливість використання методик управління безпекою з обґрунтованою системою метрик і заходів забезпечення розробників інформаційних систем.

Станом на 2019 рік створені та діють ряд національних і міжнародних стандартів у сфері ІБ, які певною мірою доповнюють один одного. Найбільш відомими серед них є: Стандарт «Критерії оцінки надійності комп'ютерних систем». «Оранжева книга» (США); Гармонізовані критерії європейських країн; Німецький стандарт BSI; Британський стандарт BS7799; Міжнародний стандарт ISO17799; Міжнародний стандарт ISO/IEC 15408 «Загальні критерії»; Стандарт COBIT та інші.

Ці стандарти можна розділити на два види:

1) стандарти для оцінки, спрямовані на класифікацію інформаційних систем і засобів захисту відносно вимог безпеки;

2) технічні специфікації, що регламентують різні аспекти реалізації засобів захисту.

Стандарти для оцінки виділяють найважливіші, з погляду ІБ, аспекти ІС, відіграючи роль архітектурних специфікацій. Інші технічні специфікації визначають, як будувати ІС запропонованої архітектури.

Наприклад, у травні 2018 року на території ЄС набули чинності оновлені правила (стандарти) з ІБ щодо обробки персональних даних, установлені «Загальним регламентом по захисту даних» (Регламент ЄС 2016/679 від 27 квітня 2016 року або GDPR – General Data Protection Regulation).

Даний регламент замінить рамкову Директиву про захист персональних даних 95/46/ЄС від 24 жовтня 1995 року. Важливим нюансом GDPR є екстериторіальний принцип дії нових європейських правил обробки персональних даних.

Новий регламент надає резидентам ЄС інструменти для повного контролю над своїми персональними даними. Із травня 2018 року посилюється відповідальність за порушення правил обробки персональних даних: по GDPR штрафи досягають 20 мільйонів євро або 4% річного глобального доходу компанії.

Це означає, що компанії інших країн, які обробляють персональні дані країн ЄС, підпадають під дію GDPR і зобов'язані дотримуватися нових європейських правил обробки персональних даних (перевезення, медичні послуги, страховки європейців тощо) щодо їх ІБ і забезпечити функціонування своїх ІС та ТКС відповідно до GDPR.

Важливою установою з питань стандартизації у сфері ІБ у США є Національний інститут стандартів і технологій (англ. The National Institute of Standards and Technology, NIST). Цей інститут разом з Американським національним інститутом стандартів (ANSI) бере участь у розробці стандартів і специфікацій до програмних рішень у сфері ІБ, які використовуються як у державному секторі США, так і у комерційній сфері. NIST є підрозділом управління технологіями США, у складі одного з агентств Міністерства торгівлі США. Штаб-квартира – Гейтерсберг. З 1901 по 1988 роки NIST називався Національне бюро стандартів США. Місією інституту визначено: просувати інноваційну та індустріальну конкурентоспроможність США.

Методологічні питання оцінки ефективності системи забезпечення інформаційної безпеки

В роботі для подальшого аналізу і розробки методик термін інформаційна безпека (англ. Information Security, Infosec) буде використовуватись як

практика запобігання несанкціонованому доступу, використання, розкриття, викривлення, зміни, дослідження, запису або знищення інформації. Це універсальне поняття застосовується незалежно від форми, в якій представлені дані (електронна або, наприклад, фізична) [25].

В основі інформаційної безпеки (ІБ) лежить діяльність із захисту інформації за категоріями: забезпечення її конфіденційності, доступності і цілісності, а також недопущення якої-небудь компрометації в критичних ситуаціях. До таких ситуацій відносяться природні, техногенні і соціальні катастрофи, комп'ютерні збої, фізичне викрадення інформації і тому подібні явища. Навіть коли діловодство організацій засноване на паперових документах, потрібні відповідні заходи забезпечення ІБ. Під конфіденційністю (англ. Confidentiality) розуміється властивість інформації бути недоступною або закритою для неавторизованих осіб, сутностей або процесів; доступністю (англ. Availability) – властивість інформації бути доступною і готовою до використання по запиту авторизованого суб'єкта; цілісністю (англ. Integrity) – властивість збереження правильності й повноти активів. У сукупності ці три ключові категорії інформаційної безпеки йменуються тріадою CIA. В 1998 році Д. Паркер доповнив класичну тріаду CIA ще трьома категоріями: володіння або контроль (англ. Possession or Control), автентичність (англ. Authenticity) і корисність (англ. Utility). В 1996 році американський NIST сформулював вісім основних принципів, які засвідчують, що комп'ютерна безпека «підтримує місію організації», «є невід'ємною складовою раціонального менеджменту», «повинна бути економічно ефективною», «вимагає всеосяжного і комплексного підходу», «обмежується соціальними факторами», «повинна періодично зазнати перегляду», «обов'язки і відповідальність за комп'ютерну безпеку повинні бути чітко сформульовані», а «власники систем відповідають за безпеку за межами своєї організації». На основі цієї моделі в 2004 році NIST опублікував 33 принципи інженерного проектування систем забезпечення інформаційної безпеки, для кожного з яких були розроблені практичні керівництва і рекомендації, які донині постійно доповнюються і підтримуються в актуальному стані [26].

В 2009 році міністерство оборони США опублікувало «Три основні принципи комп'ютерної безпеки»: схильність системи [до ризику] (англ. System Susceptibility), доступність уразливості (англ. Access to the Flaw) і здатність експлуатувати уразливість (англ. Capability to Exploit the Flaw). В 2011 році міжнародний консорціум The Open Group опублікував стандарт управління інформаційною безпекою O-ISM3. Згідно із цим стандартом для кожної організації можливо ідентифікувати індивідуальний набір цілей безпеки, що ставляться до однієї з п'яти категорій, які відповідають тому або іншому компоненту тріади CIA: пріоритетні цілі безпеки (конфіденційність), довгострокові цілі безпеки (цілісність), цілі якості інформації (цілісність), цілі контролю доступу (доступність) і технічні цілі безпеки [26].

Із усіх згаданих вище категорій ІБ класична тріада CIA як і раніше залишається найбільш визнаною та розповсюдженою в міжнародному професійному співтоваристві. Вона зафіксована в національних і міжнародних стандартах і ввійшла в основні освітні та сертифікаційні програми з ІБ.

Основне завдання інформаційної безпеки – це збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням вимог її застосування без якого-небудь збитку продуктивності організації.

Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, які дозволяють ідентифікувати основні засоби і нематеріальні активи, джерела загроз, уразливості, потенційний ступінь впливу і можливості керування ризиками. Цей процес супроводжується оцінкою ефективності плану з управління ризиками.

Нині об'єкти інформаційного захисту можуть мати дуже різну та складну структуру, різний обсяг інформаційних ресурсів, різне територіальне розміщення, різні інформаційні загрози функціонування ІС та телекомунікаційних систем. Наприклад, ІС критичної інфраструктури держави будуть суттєво відрізнятися від ІС автоматизованих систем управління технологічними процесами. Тому для розробки та оцінки ефективності системи забезпечення інформаційної безпеки (СЗІБ) необхідний системний підхід. Методологічні питання оцінки ефективності СЗІБ об'єкта (підрозділу, компанії, установи і т. д.), що має у своєму складі інформаційні ресурси, ІС або телекомунікаційні системи, потребують визначення факторів (показників) та критеріїв, за якими буде проводитись оцінка.

При виборі критерію необхідно, щоб виконувалася наступна умова: критерії, які використані для вирішення завдань нижчого рівня, мають логічно збігатися із критеріями, які використовуються на наступному, більш високому рівні [27].

Основними принципами вибору показників і критеріїв мають бути:

– необхідність строгої відповідності цілі (задачі), яка поставлена перед системою;

– критичність до цілей дослідження (мають відповідати масштабу досліджень – незначна зміна процесу має викликати помітну зміну значення критерію);

– можливість повного урахування всіх факторів, які визначають ефективність системи;

– вибір таких критеріїв, при яких показники ефективності системи легко визначаються та обчислюються;

– простота, наочність, ясний фізичний зміст;

– відсутність протиріччя окремих показників загальному.

В якості інтегрального критерію оцінки стану ефективності системи забезпечення ІБ визначимо ефективність за сукупністю комплексних показників (факторів), які зумовлюють в цілому оцінку ефективності складових СЗІБ. Оцінку стану ефективності СЗІБ визначимо за формулою

$$S = \sum_{i=1}^{N} L_i E_i \ , \qquad (1)$$

де Li – вагові коефіцієнти комплексних факторів, Ei – значення i-го комплексного фактору складової СЗІБ, N – кількість комплексних факторів складових СЗІБ. Вагові коефіцієнти комплексних факторів складових СЗІБ визначаються на експертному рівні. Сума вагових коефіцієнтів повинна дорівнювати одиниці.

Визначимо шкалу оцінки стану ефективності СЗІБ наступним чином (таблиця 1).

Таблиця 1

Оцінка стану ефективності СЗІБ	Значення показника *S*
Дуже ефективна	*S > 0,8*
Ефективна	*0,6 < S < 0,8*
Недостатньо ефективна	*0,4 < S < 0,6*
Неефективна	*0,2 < S < 0,4*
Дуже неефективна	*0,2 < S*

Враховуючи, що оцінка стану ефективності СЗІБ та її складових є багатокритеріальною з великою кількістю невизначеностей та суперечностей, розробку методик оцінки необхідно здійснювати на основі статистичного та системного аналізу з використанням експертних методів.

На основі статистичної, нормативно-правової, наукової та експертної інформації, що необхідна для належної підготовки методичних та аналітичних матеріалів у галузі ІБ, проблему необхідно аналізувати в різних площинах, які включають нормативно-правові, інформаційні, політичні, економічні, інноваційні, наукові та інші аспекти. Значення вагових коефіцієнтів комплексних факторів на перших етапах проведення експертних опитувань можна визначити рівнозначними. У подальшому їх значення можуть уточнюватись, але у будь-якому разі їх сума повинна дорівнювати одиниці.

Для оцінки ефективності СЗІБ необхідно враховувати наступні головні фактори (таблиця 2):

– наявність інформаційних ресурсів, телекомунікаційних систем (ТКС) і ІС об’єкта захисту. З оцінки майна починається процес забезпечення інформаційної безпеки, визначення інформаційних активів об’єкта захисту, цілей та завдань забезпечення ІБ, факторів, що загрожують цій інформації і її уразливості, значимості загального ризику для об’єкта захисту. Залежно від майна й буде складатися політика безпеки (інформації в організації /об’єкті захисту) (англ. Organization alsecurity policy) – як сукупність документованих правил, процедур, практичних рішень або керівних принципів в області безпеки інформації, якими керується організація у своїй діяльності;

– наявність інформаційних загроз об’єкту захисту. Це забезпечить виявлення безлічі потенційно можливих загроз і каналів витоку інформації; оцінки уразливості і ризиків інформації при наявній безлічі загроз і каналів витоку; визначення вимог до системи захисту; її організаційної структури, здійснення вибору засобів захисту інформації і їх характеристик;

– структури і завдання органів (підрозділів) у СЗІБ, що забезпечують ІБ. Це забезпечить впровадження і організацію використання обраних неформальних заходів, способів і засобів захисту;

– програмно-технічні способи і засоби забезпечення інформаційної безпеки ТКС та ІС в СЗІБ;

– ефективність функціонування системи менеджменту (керування) інформаційною безпекою (СМІБ) об’єкта захисту.

Таблиця 2

Позначення основних факторів	Найменування основних факторів
E_1	Оцінка наявності інформаційних ресурсів, ТКС і ІС на об'єкті захисту
E_2	Оцінка наявності інформаційних загроз об'єкту захисту
E_3	Оцінка структури і завдань органів (підрозділів) у СЗІБ, що забезпечують ІБ на об'єкті захисту
E_4	Оцінка програмно-технічних способів і засобів забезпечення інформаційної безпеки ТКС та ІС в СЗІБ
E_5	Оцінка ефективності функціонування СМІБ

Проаналізуємо перший головний фактор оцінки наявності інформаційних ресурсів, телекомунікаційних систем і ІС об'єкта захисту у формулі (1).

Значення 1-го комплексного фактору складової СЗІБ позначимо E_1. Оцінку цього фактору також можливо провести через фактори (показники) другого рівня за формулою

$$E_1 = \sum_{i=1}^{K} M_i D_i , \qquad (2)$$

де K – кількість факторів другого рівня, що використовуються для розрахунку E_1 (таблиця 3), M_i – вагові коефіцієнти комплексних факторів другого рівня, D_i – значення i-го комплексного фактору другого рівня. Вагові коефіцієнти комплексних факторів складових СЗІБ визначаються на експертному рівні. Сума вагових коефіцієнтів другого рівня також повинна дорівнювати одиниці. В таблиці 3 для характеристики об'єкта захисту для прикладу вибрані 3 фактори другого рівня.

Таблиця 3

Позначення факторів другого рівня	Найменування факторів другого рівня
D_1	Оцінка наявних інформаційних ресурсів об'єкта захисту
D_2	Оцінка наявних ІС
D_3	Оцінка наявних ТКС

Проаналізуємо другий головний фактор у формулі (1) щодо оцінки наявності інформаційних загроз об'єкту захисту E_2. Оцінку цього фактору також можливо провести через фактори (показники) другого рівня за формулою

$$E_2 = \sum_{i=1}^{P} G_i F_i , \qquad (3)$$

де P – кількість факторів другого рівня, що використовуються для розрахунку E_2 (таблиця 4), G_i – вагові коефіцієнти комплексних факторів другого рівня,

F_i – значення i-го комплексного фактору другого рівня. Вагові коефіцієнти комплексних факторів складових СЗІБ визначаються на експертному рівні. Сума вагових коефіцієнтів другого рівня також повинна дорівнювати одиниці

$$\sum_{i=1}^{P} G_i = 1 . \tag{4}$$

В залежності від характеристики об'єкта захисту, категорії інформації, яка знаходиться в ІС та ТКС, кількість факторів другого рівня, що використовуються для розрахунку E_2, може суттєво змінюватись. В таблиці 4 для характеристики інформаційних загроз об'єкту захисту вибрані 4 фактори другого рівня.

Таблиця 4

Позначення факторів другого рівня	Найменування факторів другого рівня
F_1	Оцінка кібернетичних загроз об'єкту захисту
F_2	Оцінка фізичних загроз ІБ об'єкту захисту
F_3	Оцінка інформаційних загроз ІБ ТКС та ІС
F_4	Оцінка загроз ІБ ТКС та ІС щодо їх знищення або виведення з ладу за допомогою систем РЕБ, оптико-електронних систем тощо

В таблиці 4 розглядаються фактори другого рівня, які характеризують інформаційні загрози, що можуть виникати: через процеси, процедури, програми обробки, передачі, зберігання інформації (кібернетичні загрози); через фізичне знищення ІС та ТК її носіїв (паперових, пристроїв пам'яті, дисків) тощо; через канали зв'язку (акустичні, інфрачервоні, провідні, радіоканали та ін.), через побічні випромінювання; знищення або тимчасове виведення з ладу ТКС та ІС за допомогою систем РЕБ, оптико-електронних засобів /лазерних/ тощо.

Проаналізуємо третій головний фактор E_3 оцінки структури і завдань органів (підрозділів) у СЗІБ, що забезпечують ІБ на об'єкті захисту у формулі (1). Оцінку цього фактору також можливо провести через фактори (показники) другого рівня за формулою

$$E_3 = \sum_{i=1}^{T} R_i H_i , \tag{5}$$

де T – кількість факторів другого рівня, що використовуються для розрахунку E_3 (таблиця 3), R_i – вагові коефіцієнти комплексних факторів другого рівня, H_i – значення i-го комплексного фактору другого рівня. Вагові коефіцієнти R_i факторів другого рівня визначаються на експертному рівні. Сума вагових коефіцієнтів другого рівня також повинна дорівнювати одиниці. В таблиці 5 для характеристики оцінки структури і завдань органів (підрозділів) у СЗІБ, що забезпечують ІБ на об'єкті захисту, вибрані 3 фактори другого рівня.

Таблиця 5

Позначення факторів другого рівня	Найменування факторів другого рівня
H_1	Оцінка організації фізичного захисту об'єкта
H_2	Оцінка організації доступу до ІС
H_3	Оцінка організації доступу до ТКС

Фактично головний фактор E_3 оцінює організаційний аспект забезпечення ІБ завдяки регламентації виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво утрудняє неправомірне оволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз. До системи організації фізичного захисту об'єкта, як правило, входять служба економічної безпеки; служба безпеки персоналу (режимний відділ); кадрова служба; служба інформаційної безпеки тощо. Організаційний захист забезпечує організацію:

– режиму і охорони з метою виключення можливості таємного проникнення сторонніх осіб на територію об'єкта захисту або у приміщення, де здійснюється робота з конфіденційною інформацією;

– роботи зі співробітниками, яка передбачає набір і розміщення персоналу, включаючи ознайомлення зі співробітниками, навчання правилам роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил захисту інформації тощо;

– роботи з документами і документованою інформацією, роботи з ІС та ТКС, включаючи організацію розробки і використання документів і носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;

– використання технічних засобів збору, обробки, нагромадження і зберігання конфіденційної інформації;

– роботи з аналізу внутрішніх і зовнішніх загроз конфіденційній інформації і вироблення заходів щодо забезпечення її захисту;

– використання технічних засобів безпеки з виявлення внутрішніх і зовнішніх загроз інформаційній діяльності;

– організацію роботи із проведення систематичного контролю над роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання і знищення документів і технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і утримування, спрямовані на забезпечення безпеки інформації в конкретних умовах.

Проаналізуємо четвертий головний фактор E_4 оцінки програмно-технічних способів і засобів забезпечення інформаційної безпеки ТКС та ІС в СЗІБ, що забезпечують ІБ на об'єкті захисту у формулі (1). Оцінку цього фактору також можливо провести через фактори (показники) другого рівня за формулою

$$E_4 = \sum_{i=1}^{X} V_i B_i , \qquad (6)$$

де X – кількість факторів другого рівня, що використовуються для розрахунку E_4 (таблиця 6), V_i – вагові коефіцієнти комплексних факторів другого рівня,

B_i – значення i-го комплексного фактору другого рівня. Вагові коефіцієнти V_i факторів другого рівня визначаються на експертному рівні. Сума вагових коефіцієнтів другого рівня також повинна дорівнювати одиниці. В таблиці 6 для характеристики оцінки програмно-технічних способів і засобів забезпечення інформаційної безпеки ТКС та ІС в СЗІБ, що забезпечують ІБ на об'єкті захисту, вибрані 10 факторів другого рівня.

Таблиця 6

Позначення факторів другого рівня	Найменування факторів другого рівня
B_1	Оцінка можливості перерозподіляти ресурси мережі у випадках порушення працездатності окремих елементів
B_2	Оцінка системи аналізу і моделювання інформаційних потоків (Case-Системи)
B_3	Оцінка системи моніторингу мереж (*Системи виявлення і запобігання вторгненню (IDS/IPS). Системи запобігання витокам конфіденційної інформації /DLP-системи/).*
B_4	Оцінка антивірусних засобів
B_5	Оцінка міжмережевих екранів
B_6	Оцінка криптографічних засобів
B_7	Оцінка систем резервного копіювання
B_8	Оцінка систем безперебійного електроживлення
B_9	Оцінка систем аутентифікації і ідентифікації
B_{10}	Оцінка комплексу технічних заходів щодо контролю об'єктів ІС та ТКС (облаштування приміщення камерами спостереження, сигналізацією тощо)

Група програмно-технічних способів і засобів забезпечення інформаційної безпеки ТКС та ІС в СЗІБ включає велику кількість апаратних та програмних засобів. Основними з них є:

– резервне копіювання і окреме зберігання найбільш важливих масивів даних у ІС або ТКС – на регулярній основі;

– дублювання і резервування всіх підсистем мереж, які мають значення для збереження даних;

– створення можливості перерозподіляти ресурси мережі у випадках порушення працездатності окремих елементів;

– забезпечення можливості використовувати резервні системи електроживлення;

– забезпечення безпеки від пожежі або ушкодження устаткування водою;

– установка програмного забезпечення, яке забезпечує захист баз даних та іншої інформації від несанкціонованого доступу;

– установлення комплексу технічних заходів щодо забезпечення контролю об'єктів комп'ютерних мереж, наприклад, облаштування приміщення камерами спостереження і сигналізацією;

– аутентифікація і ідентифікація.

Щоб виключити неправомірний доступ до інформації, застосовують такі способи, як ідентифікація та аутентифікація. Ідентифікація – це механізм присвоєння власного унікального імені або образа користувачеві, який

взаємодіє з інформацією. Аутентифікація – це система способів перевірки збігу користувача з тим образом, якому дозволений допуск. Ці засоби спрямовані на те, щоб надати або, навпаки, заборонити допуск до даних. Реально, як правило, це визначається трьома способами: програмою, апаратом, людиною. При цьому об'єктом аутентифікації може бути не тільки людина, а й технічні коштзасоби (комп'ютер, монітор, носії) або дані. Найпростіший спосіб захисту – пароль.

Для контролю витоків інформації використовують DLP-системи (Data Leak Prevention). Під DLP-системами (Data Leak Prevention) прийнято розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю вихідну, а в ряді випадків і вхідну інформацію. Контрольованою інформацією може бути не тільки інтернет-трафік, але й ряд інших інформаційних потоків: документи, які виносяться за межі контуру, що захищається, контроль документів ІБ на зовнішніх носіях, що роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і т. д. Оскільки DLP-система повинна перешкоджати витокам конфіденційної інформації, то вона в обов'язковому порядку має вбудовані механізми визначення ступеня конфіденційності документа, виявленого в перехопленому трафіку.

Проаналізуємо п'ятий головний фактор E_5 оцінки ефективності функціонування СМІБ, що забезпечують ІБ на об'єкті захисту у формулі (1). Оцінку цього фактору також можливо провести через фактори (показники) другого рівня за формулою

$$E_5 = \sum_{i=1}^{Z} W_i Q_i \,, \tag{7}$$

де Z – кількість факторів другого рівня, що використовуються для розрахунку E_5 (таблиця 7), W_i – вагові коефіцієнти комплексних факторів другого рівня, Q_i – значення i-го комплексного фактору другого рівня. Вагові коефіцієнти W_i факторів другого рівня визначаються на експертному рівні. Сума вагових коефіцієнтів другого рівня також повинна дорівнювати одиниці. В таблиці 7 для характеристики оцінки ефективності функціонування СМІБ, що забезпечують ІБ на об'єкті захисту, вибрані 3 фактори другого рівня.

Таблиця 7

Позначення факторів другого рівня	Найменування факторів другого рівня
Q_1	Оцінка моніторингу ефективності функціонування СМІБ
Q_2	Оцінка системи управління ризиками функціонування СМІБ
Q_3	Оцінка системи впровадження змін з СЗІБ

Для оцінки ефективності функціонування СМІБ, що забезпечують ІБ на об'єкті захисту, нині використовують різні методи. В деяких випадках ці методи базуються на міжнародних стандартах. Наприклад, Міжнародною комісією зі стандартизації (ISO) та Міжнародною енергетичною комісією

(IEC) розроблена група стандартів ISO/IEC 27000, в яких міститься ряд рекомендацій і практичних порад для впровадження системи менеджменту інформаційної безпеки (СМІБ).

Крім стандартів серії ISO/IEC 27000, європейські держави розробляють і впроваджують власні нормативні документи, що визначають вимоги до забезпечення ІБ. Найчастіше національні стандарти, розроблені для внутрішньодержавного застосування, використовуються іншими державами. Наприклад, розроблені у Великобританії Практичні правила керування інформаційною безпекою BS 7799 вийшли за межі національного рівня. Вищезазначені правила використані у міжнародному стандарті ISO17799.

Ряд компаній для захисту власної конфіденційної інформації і сертифікації товарів, послуг і контролю СМІБ використовують стандарт ISO 9001. Згідно з моделлю менеджменту стандарту ISO 9001, процес створення, впровадження та контролю СМІБ включає чотири етапи, які позначаються абревіатурою PDCA (табл. 8).

При впровадженні СМІБ шляхом PDCA система буде відповідати вимогам міжнародних стандартів сертифікації.

Слід зазначити, що методичний підхід PDCA є постійним циклічним процесом, завдяки якому СМІБ постійно удосконалюється.

Таким чином, використовуючи дані оцінок з таблиць 3–7 факторів другого рівня, можливо за формулами (2–7) здійснити розрахунок головних факторів оцінки ефективності СЗІБ, що визначені в таблиці 2. Використовуючи ці значення головних факторів за формулою (1), можливо розрахувати оцінку ефективності СЗІБ. Порівнюючи цю оцінку з даними таблиці 1, можливо оцінити рівень ефективності СЗІБ.

Таблиця 8

Етап	Назва етапу	Характеристика етапу
Plan	Плануй	На етапі Plan розробляють внутрішню нормативну документацію, проводять аудит систем, інвентаризацію можливих ризиків або критичних активів, розробляють систему технічних заходів.
Do	Роби	На етапі Do впроваджують розроблену систему і засоби оцінки ефективності вжитих заходів.
Check	Визначай	На етапі Check оцінюють якість роботи системи, причому оцінка повинна носити цільовий і регулярний характер.
Act	Дій	На етапі Act здійснюють доробку і усунення виявлених недоліків.

У запропонованій методиці оцінки рівня ефективності СЗІБ в залежності від цілей оцінки можливо змінювати як головні фактори в таблиці 2, так і фактори оцінки другого рівня. Фактори другого рівня також можливо розраховувати на основі експертних оцінок на основі факторів третього рівня, як це запропоновано в роботі [27].

Висновки

1. По мірі розвитку ІС та ТКС і їх використання в економічному розвитку держав, національній безпеці, компаніях, суспільстві і окремими особами, кіберзлочинність стає ключовою загрозою розвитку світової економіки, а проблема забезпечення інформаційної безпеки буде ставати все актуальнішою. Тому провідні країни світу проблемі ІБ приділяють все більше уваги, а для її забезпечення формують відповідну нормативну базу і спеціальні інститути.

2. Проблема ІБ нині зачіпає не тільки окремі ІС та ТКС, окремі організації та компанії, а й в цілому держави та міждержавні відносини, з формуванням відповідних міждержавних угод у сфері ІБ. Питання ІБ регулярно обговорюються на зустрічах «Великої двадцятки», на майданчику ООН, на зустрічах міністрів телекомунікацій і інформаційних технологій країн різних союзів та блоків.

3. Вже сьогодні сформовані та продовжують удосконалюватись державні (національні) та міждержавні стандарти у сфері ІБ, зокрема стандарт «Критерії оцінки надійності комп'ютерних систем». «Оранжева книга» (США); Гармонізовані критерії європейських країн; Міжнародний стандарт ISO17799; Міжнародний стандарт ISO/IEC 15408 «Загальні критерії»; Стандарт COBIT; Регламент ЄС 2016/679 від 27 квітня 2016 року або GDPR – General Data Protection Regulation та інші.

4. По мірі розширення застосування ІС та ТКС у різних сферах економічної, політичної, екологічної, воєнної, наукової діяльності та інших галузях ІБ стала розглядатись як певний ризик для основної діяльності. При цьому для створення, аналізу та оцінки ефективності СЗІБ необхідна розробка методів оцінки ефективності СЗІБ, які необхідні для систем управління ризиками основної діяльності з включенням в цю систему проблеми ІБ. Тому запропонована методика оцінки ефективності СЗІБ з використанням міждержавних стандартів у сфері ІБ, експертних методів та системного аналізу, що реально дозволяє оцінити конкретні об'єкти інформаційного захисту (компанії, окремі підприємства, установи тощо) як з урахуванням ІС та ТКС на цих об'єктах, так і інших організаційних заходів.

5. Використання запропонованої методики оцінки ефективності СЗІБ в системі ризик-менеджменту бізнес-процесів дозволить більш ефективно управляти ризиками об'єктів інформаційного захисту (компаній, окремих підприємств, організацій тощо).

СПИСОК ЛІТЕРАТУРИ

1. Международный конгресс по кибербезопасности 5-6 июля 2018 года. Пленарное заседание. 06.07.2018. [Електронний ресурс] – Режим доступу : http://kremlin.ru/events/president/news/57957.
2. Statement from the Press Secretary. Whitehouse. 15.05.2019. [Електронний ресурс] – Режим доступу : https://www.whitehouse.gov/briefings-statements/statement-press-secretary-56/.
3. Трамп ввел чрезвычайное положение в США для защиты коммуникационных сетей. Ведомости. 16.05.2019. [Електронний ресурс] – Режим доступу : https://www.vedomosti.ru/politics/news/2019/05/16/801521-tramp.

4. Пентагон запретил контракты с РФ на запуск коммерческих спутников с 2023 года. Interfax.ru. 30.05.2019. [Електронний ресурс] – Режим доступу : https://www.interfax.ru/world/663107.
5. Пять проблем и тенденций информационной безопасности: чего ожидать в 2018 году. Компанія GlobalSign. 09.02.2018. [Електронний ресурс] – Режим доступу : https://habr.com/ru/company/globalsign/blog/348690/.
6. Прогнозы по информационной безопасности на 2018 год. RVision. 01.06.2019. [Електронний ресурс] – Режим доступу : https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/.
7. Прогнозы по информационной безопасности на 2019 год. RVision. 01.06.2019. [Електронний ресурс] – Режим доступу : https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2019-god/.
8. Информационная безопасность (тренды). 2019: Топ-10 трендов в сфере кибербезопасности интернета вещей – Counterpoint Technology. Tadviser. 08.02.2019. [Електронний ресурс] – Режим доступу : http://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации.
9. Статьи по информационной безопасности за 2016 год. МИРЭА. 01.06.2019. [Електронний ресурс] – Режим доступу : https://www.mirea.ru/umo/scientific-activities/articles-on-information-security-for-2016/.
10. Шерстюк В.П. МГУ: научные исследования в области информационной безопасности. МГУ. 01.06.2019. [Електронний ресурс] – Режим доступу : http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/892ea7cb332e596cc32571cb00319141.
11. Вопросы информационной безопасности. 09.09.2014. [Електронний ресурс] – Режим доступу : https://www.marketing.spb.ru/mr/it/giss.htm.
12. Скляров Д. Как менялась информационная безопасность за последние 20 лет. Центр стратегических оценок и прогнозов. 06.05.2019. [Електронний ресурс] – Режим доступу : http://csef.ru/ru/oborona-i-bezopasnost/272/kak-menyalas-informaczionnaya-bezopasnost-za-poslednie-20-let-8881.
13. Информационная безопасность предприятия: ключевые угрозы и средства защиты. КР. 01.06.2019. [Електронний ресурс] – Режим доступу : https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html.
14. A New National Security Strategy for a New Era. Whitehouse. 18.12.2019. [Електронний ресурс] – Режим доступу : https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.
15. The National Defense Strategy. DOD/ 19.01.2018. [Електронний ресурс] – Режим доступу : https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
16. The National Military Strategy of the United States of America. 2015. JCS.mil. 15.05.2019. [Електронний ресурс] – Режим доступу : https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
17. The National Cyber Strategy, (NCS). Whitehouse. 28.09.2018. [Електронний ресурс] – Режим доступу : https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
18. Стратегія кібербезпеки України. Указ Президента України № 96/2016 від 15 березня 2016 року. 2019. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016#n11.
19. Доктрина інформаційної безпеки України. Указ Президента України № 47/2017 від 25 лютого 2017 року 2019. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017.
20. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 із змінами. 2019. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19.

21. Доктрина информационной безопасности РФ, 2016. [Електронний ресурс] – Режим доступу : http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1.
22. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ. Консультант плюс. 27.05.2019. [Електронний ресурс] – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_61798/.
23. Федеральный закон РФ «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 N 187-ФЗ. Консультант плюс. 27.05.2019. [Електронний ресурс] – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_220885/.
24. Центр национальной компьютерной безопасности Великобритании. 01.06.2019. [Електронний ресурс] – Режим доступу : https://ru.wikipedia.org/wiki/Центр_национальной_компьютерной_безопасности_Великобритании.
25. ISO/IEC 27000 - серия международных стандартов, включающая стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссией (IEC).
26. Информационная безопасность. Википедия. 01.06.2019. [Електронний ресурс] – Режим доступу : https://ru.wikipedia.org/wiki/Информационная_безопасность.
27. Методологічні аспекти оцінки стану військово-технічної політики та її складових : наук.-метод. видання. / В.П. Горбулін (кер. авт. кол.), В.В. Зубарєв, О.П. Кутовий; О.О. Свергунов; С.М. Химченко. – К.: Інтертехнологія, 2009. – 208 с.

Стаття надійшла до редакції 21.05.2019 і прийнята до друку після рецензування 10.06.2019

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Plenarnoe zasedanie Mezhdunarodnogo kongressa po kiberbezopasnosti. (2018, July 06). Retrieved from http://kremlin.ru/events/president/news/57957 (in Russian).
2. Statement from the Press Secretary. Whitehouse. (2019, May 15). Retrieved from https://www.whitehouse.gov/briefings-statements/statement-press-secretary-56/.
3. Vedomosti. (2019, May 16). Tramp vvel chrezvychajnoe polozhenie v SShA dlya zaschity kommunikacionnyh setej. Retrieved from https://www.vedomosti.ru/politics/news/2019/05/16/801521-tramp (in Russian).
4. Interfax.ru. (2019, May 30). Pentagon zapretil kontrakty s RF na zapusk kommercheskih sputnikov s 2023 goda. Retrieved from https://www.interfax.ru/world/663107 (in Russian).
5. Kompaniya GlobalSign. (2018, February 09). Pyat' problem i tendencij informacionnoj bezopasnosti: chego ozhidat' v 2018 godu. Retrieved from https://habr.com/ru/company/globalsign/blog/348690/ (in Russian).
6. Prognozy po informacionnoj bezopasnosti na 2018 god | R-Vision. (n.d.). Retrieved June 1, 2019 from https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/ (in Russian).
7. Prognozy po informacionnoj bezopasnosti na 2019 god | R-Vision. (n.d.). Retrieved June 1, 2019 from https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2019-god/ (in Russian).
8. Informacionnaya bezopasnost' (trendy). 2019: Top-10 trendov v sfere kiberbezopasnosti interneta veschej. (2019, February 8). Retrieved from http://www.tadviser.ru/index.php/ (in Russian).
9. MIREA. (n.d.). Stat'i po informacionnoj bezopasnosti za 2016 god. Retrieved June 1, 2019 from https://www.mirea.ru/umo/scientific-activities/articles-on-information-security-for-2016/ (in Russian).

10. Sherstyuk, V. P. (n.d.). MGU: Nauchnye issledovaniya v oblasti informacionnoj bezopasnosti. Retrieved June 1, 2019, from http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/892ea7cb332e596cc32571cb00319141 (in Russian).
11. Voprosy informacionnoj bezopasnosti. (2014, September 9). Retrieved from https://www.marketing.spb.ru/mr/it/giss.htm (in Russian).
12. Sklyarov, D. (2019, May 6). Kak menyalas' informacionnaya bezopasnost' za poslednie 20 let. Retrieved from http://csef.ru/ru/oborona-i-bezopasnost/272/kak-menyalas-informaczionnaya-bezopasnost-za-poslednie-20-let-8881 (in Russian).
13. Informacionnaya bezopasnost' predpriyatiya: Klyuchevye ugrozy i sredstva zaschity. (n.d.). Retrieved June 1, 2019, from https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (in Russian).
14. A New National Security Strategy for a New Era. Whitehouse. (2017, December 19). Retrieved from https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/
15. The National Defense Strategy. DOD. (2018, January 19). Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
16. The National Military Strategy of the United States of America. 2015. JCS.mil. (n.d.). Retrieved May 15, 2019, from https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
17. The National Cyber Strategy, (NCS). Whitehouse. (2018, September 28). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
18. Strategiya Kiberbezpeki Ukrai'ny. (2016, March 15). *Ukaz Prezidenta Ukrai'ny № 96/2016*. Retrieved from https://zakon.rada.gov.ua/laws/show/96/2016#n11 (in Ukrainian).
19. Doktrina informacijnoï bezpeki Ukrai'ny. (2017, February 25). *Ukaz Prezidenta Ukrai'ny № 47/2017*. Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017 (in Ukrainian).
20. Verhovna Rada Ukrai'ny. (2017, October 5). *Zakon Ukrai'ny «Pro Osnovni Zasadi Zabezpechennya Kiberbezpeki Ukrai'ny» № 2163-VIII* (Vidomosti Verhovnoï Radi (VVR), 2017, № 45, st.403 iz zminami). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian).
21. Doktrina informacionnoj bezopasnosti RF, 2016. (n.d.). Retrieved from http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1 (in Russian).
22. Federal'nyj Zakon RF «Ob Informacii, Informacionnyh Tehnologiyah i o Zaschite Informacii» (2006, July 27). Retrieved May 27, 2019, from http://www.consultant.ru/document/cons_doc_LAW_61798/ (in Russian).
23. Federal'nyj zakon RF «O bezopasnosti kriticheskoj informacionnoj infrastruktury RF» N 187-FZ (2017, July 26). Retrieved May 27, 2019, from http://www.consultant.ru/document/cons_doc_LAW_220885/ (in Russian).
24. Centr nacional'noj komp'yuternoj bezopasnosti Velikobritanii. Retrieved June 1, 2019, from https://ru.wikipedia.org/wiki/Centr_nacional'noj_komp'yuternoj_bezopasnosti_Velikobritanii (in Russian).
25. ISO/IEC 27000 – seriya mezhdunarodnyh standartov, vklyuchayuschaya standarty po informacionnoj bezopasnosti, opublikovannye sovmestno Mezhdunarodnoj Organizaciej po Standartizacii (ISO) i Mezhdunarodnoj `Elektrotehnicheskoj Komissiej (IEC).
26. Informacionnaya bezopasnost'. Vikipediya. (n.d.). Retrieved June 1, 2019, from https://ru.wikipedia.org/wiki/Informacionnaya_bezopasnost' (in Russian).
27. Zubarev, V. V., Kutovij, O. P., Svergunov, O. O., & Himchenko, S. M. (2009). *Metodologichni aspekti ocinki stanu vijs'kovo-tehnichnoï politiki ta ïï skladovih : Nauk.-metod. vidannya* (V. P. Gorbulin, Ed.). Kyiv: Intertehnologiya (in Ukrainian).

The article was received 21.05.2019 and was accepted after revision 10.06.2019

Чепков Ігор Борисович
доктор технічних наук, професор, ЦНДІ ОВТ ЗС України
Адреса робоча: 03049 Україна, м. Київ, Повітрофлотський проспект, 28
e-mail: *i.chepkov@mil.gov.ua*
ORCID ID 0000-0002-4294-4152

Зубарєв Валерій Володимирович
доктор технічних наук, професор, ЦНДІ ОВТ ЗС України
Адреса робоча: 03049 Україна, м. Київ, Повітрофлотський проспект, 28
e-mail: *doktorzubarev.2016@gmail.com*
ORCID ID 0000-0002-4998-726X

Свергунов Олександр Олексійович
кандидат технічних наук, доцент, провідний науковий співробітник НІСД
Адреса робоча: 01030 Україна, м. Київ, вул. Пирогова, 7А
e-mail: *asverg@niss.gov.ua*
ORCID ID 0000-0002-2158-1532

Зубарєв Олександр Валерійович
кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник ЦНДІ ОВТ ЗС України
Адреса робоча: 03049 Україна, м. Київ, Повітрофлотський проспект, 28
e-mail: *aleksanderzubarev@gmail.com*
ORCID ID 0000-0001-5590-7660