DOI: https://doi.org/10.32836/2521-6643-2019-2-58-5
УДК 004.056:681.518.3

Ю. Л. Поночовний, кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем та технологій Полтавської державної аграрної академії

АНАЛІЗ КОНЦЕПЦІЙ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ РОЗПОДІЛЕНИХ ІТ-ІНФРАСТРУКТУР

Узагальнено актуальні питання управління безпекою організаційно складних систем. Виділено основні принципи визначення концептуальних підходів до управління безпекою в наукових працях та нормативних документах для різних сфер життєдіяльності людини. Приділено увагу як складовим безпеки ІТ-систем (функціональна, інформаційна, кібербезпека), так і якостям складних систем, до яких включено безпеку (гарантоздатність, функціональна надійність). Наведено порівняльний перелік принципів для різних концепцій управління безпекою ІТ-систем та інфраструктур.

Ключові слова: *функціональна та кібербезпека; концепції управління; розподілені ІТ-інфраструктури.*

Обобщены актуальные вопросы управления безопасностью организационно сложных систем. Выделены основные принципы представления концептуальных подходов к управлению безопасностью в научных трудах и нормативных документах для различных сфер жизнедеятельности человека. Уделено внимание как составляющим безопасности ИТ-систем (функциональная, информационная, кибербезопасность), так и качествам сложных систем, в которые включена безопасность (гарантоспособность, функциональная надежность). Приведен сравнительный перечень принципов для различных концепций управления безопасностью ИТ-систем и инфраструктур.

Ключевые слова: *функциональная и кибербезопасность; концепции управления; распределенные ИТ-инфраструктуры.*

The paper summarizes the current issues of security management of organizationally complex systems. Massive introduction of cloud technologies, the Internet of things (IoT), intelligent data processing systems, block chain technologies is not only a fashionable trend, but also dictates the conditions for the development of the information and communication systems industry.

Organization, definition and classification of safety and cybersecurity management concepts in organizationally complex systems are disclosed in the work of researchers in various industries: aviation, economic, information (cybersecurity), administrative, environmental and the like. The article summarizes basic principles of conceptual approaches to safety and cybersecurity management in scientific works and regulatory documents for various spheres of human life.

The purpose of this article is to summarize basic principles for presenting conceptual approaches to managing the cybersecurity of IT-systems and infrastructures in scientific and regulatory documents. To solve the problem, it is necessary to consider the concepts of security management in various spheres of human life, to determine the concept and components of cybersecurity for IT-systems and infrastructures, to consider the basic principles for various conceptual approaches to security management.

Attention is paid both to the components of IT-systems security (functional-, informational-, cybersecurity), and the qualities of complex systems that include security (dependability, functional reliability). Among the main provisions of security management concepts, an important place is given to security policy, both the general and the whole (often as security strategies), and the separation of policies into global and local.

A comparative list of principles for various concepts of managing IT-systems and infrastructures security is given. The security management concepts of distributed IT-systems are analyzed on the example of critical infrastructures, information and telecommunication systems, industrial automation systems, cyberphysical systems and continuous business systems. It is determined that various concepts can use general principles, such as risk management, improvement/ adaptation of the security management system.

Key words: *safety and cybersecurity; management concepts; distributed IT-infrastructures.*

Постановка проблеми. Наразі використання розподілених IT-інфраструктур поширено в усіх галузях життєдіяльності людини, у тому числі й галузі критичного застосування. Масове впровадження хмарних технологій, інтернету речей (IoT), інтелектуальних систем обробки даних, технологій блок-чейн – не тільки модний тренд, але й умова розвитку галузі інформаційно-комунікаційних систем. Проте хронологія аварій і катастроф організаційно складних систем та комплексів авіаційної, ракето-космічної, енергетичної, фінансової та інших галузей вказує на пряму залежність між розмірами і складністю системи й наслідками критичної ситуації в ній. Для запобігання нештатним та критичним ситуаціям, аваріям і катастрофам сучасні організаційно складні системи обов’язково повинні підтримувати безпечний стан (як самої системи, так і навколишнього відносно неї середовища).

Аналіз останніх досліджень і публікацій.

Аналіз джерел інформації щодо способів визначення концепцій управління безпекою у різних галузях життєдіяльності

Питання організації управління безпекою в організаційно складних системах, у тому числі з визначення та класифікації концепцій управління безпекою, розкрито у працях дослідників різних галузей: авіаційної [1], економічної [2; 3], інформаційної (кібербезпека) [4; 5], адміністративної [6], екологічної [7] тощо. Узагальнюючи опрацьований матеріал, слід зазначити, що управління безпекою є комплексом взаємоузгоджених різнопланових заходів, спрямованих на запобігання ризикам різного характеру та мінімізацію їхніх наслідків. Отже, під безпечним розуміють стан системи, за яким ризики завдання шкоди людині, системі чи навколишньому середовищу або зменшуються, або підтримуються нижче від певного рівня.

За енциклопедичним визначенням [8], під концепцією розуміють систему поглядів на явища або процеси. Ця система є первинною, головною, основотвірною. У поданні концепцій та їхніх елементів дослідники зазначають їхній розрізнений характер, оскільки, з одного боку, є наукова складова, а з іншого – необхідно продемонструвати пріоритет своїх концепцій над іншими поглядами.

Наукові дослідження концепцій управління безпекою подаються у вигляді статей, що публікуються у виданнях високого рівня (фахових, міжнародних), монографіях, науково-дослідних працях та проєктах. Завершальним етапом подання концепції можна вважати доведення її положень до рівня нормативних актів, законів чи стандартів певних відомств, держави чи міжнародних організацій.

Для виокремлення чи виділення концепції як авторського результату досліджень їй надається певний ідентифікатор. Таким ідентифікатором може бути назва, наприклад: концепція зон стратегічних ресурсів [9], концепція "об'єкт – загроза – захист" [10], Концепція "безпечна інфраструктура з небезпечних і ненадійних незалежних систем" [11], conception of multilevel complex security system [12]. Для загальновідомих концепцій можливе подання її за прізвищем автора, наприклад: концепція Д. Ф. Неймана [11]. Якщо концепція розглядається як складова методології, то вона може отримати додатковий класифікатор, наприклад: концепція 2.1 структурно-семантичне уявлення профілів [13].

Концепції управління безпекою трактуються різними дослідниками як:

– упорядкована й системна множина принципів, методів і моделей, що входить до складу визначеної методології [11; 13; 14];

– керівний документ (стандарт, закон, нормативний акт) чи їх системна множина [15–18];

– задокументовані взаємозв'язки між нормативно-правовими документами, видами загроз, відповідальними виконавцями та процесами управлін-

ня безпекою; при цьому документи мають у назві ключові слова “стратегія” чи “політика” [6; 7; 19].

Мета статті – узагальнення основних принципів концептуальних підходів до управління безпекою ІТ-систем та інфраструктур у наукових і нормативних документах. Для цього необхідно розглянути концепції управління безпекою у різних сферах життєдіяльності людини, визначитись із поняттям і складовими безпеки для ІТ-систем та інфраструктур, розглянути базові принципи для різних концептуальних підходів до управління безпекою.

Виклад основного матеріалу.

Аналіз наявних підходів до визначення поняття безпеки розподілених ІТ-інфраструктур

У питаннях визначення терміна “безпека” щодо ІТ-інфраструктур наразі можна виділити два головних розгалуження:

– безпека як “safety”;

– безпека як “security”.

“Safety” більшість вітчизняних дослідників перекладає як “функціональна безпека”, таке ж трактування цього слова і в стандартах. Під функціональною безпекою розуміють відсутність неприйнятного ризику за рахунок використання системи управління безпекою та заходів зниження ризику [20]. Це властивість виключати або мінімізувати шкідливі наслідки у разі відмов для користувачів, інших систем та навколишнього середовища [14]. Концептуальні підходи до управління функціональною безпекою доведені до рівня міжнародних стандартів, закріплених за окремими галузями: авіація [21], автомобільна техніка [22], залізничний транспорт [23], атомні електростанції [24], електронні/електричні програмовані компоненти [20].

Термін “security” до певного часу перекладали як “інформаційна безпека”. Але впродовж останнього десятиліття поруч із цим терміном активно використовується інший – “cybersecurity”, що вже отримав чіткий переклад як “кібербезпека”. Інформаційну безпеку розглядають у контексті забезпечення конфіденційності, цілісності та готовності [5; 25] (додатково можуть розглядатися автентичність, неможливість відмови від авторства й надійність, тобто reliability [14; 15; 26]). Кібербезпека трактується як стан безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [19]; чи як дії, необхідні для запобігання несанкціонованому використанню, відмови в обслуговуванні, перетворення, розсекречення, втрати прибутку або пошкодження критичних систем чи інформаційних об’єктів [16; 27].

Концептуальні підходи до управління інформаційною безпекою реалізовані на рівні багатьох міжнародних стандартів, серед яких треба виокремити ISO/IEC15408 (критерії оцінювання ІБ), ISO/IEC2700x (система менеджменту ІБ). Управління кібербезпекою на концептуальному рівні визначено в серії стандартів ISO/IEC 62443 [16; 28].

Слід зазначити, що ряд дослідників приділяє увагу поєднанню властивостей “safety”, “security” (“cybersecurity”) у рамках загального концептуального підходу. Серед вітчизняних дослідників провідне місце належить працям В. С. Харченка [11; 13; 14], в яких узагальнювальною властивістю є “гарантоздатність” (dependabiliyty). Гарантоздатність поєднує групи первинних властивостей (безвідмовність, готовність, обслуговуваність, вірогідність, функціональна безпека, життєздатність, цілісність, конфіденційність) та вторинних властивостей (інформаційна безпека, кібербезпека, автентичність, надійність). Концепція гарантоздатності є хронологічним і послідовним розвитком запропонованої А. Авіженісом, Ж. К. Лапрі та В. Ренделом [29] концепції “Dependability”. У праці І. Б. Шубинського [30] трапляється термін “функціональна надійність”, тобто поєднання готовності, безвідмовності, правильності, безпомилковості, стійкості, цілісності та доступності.

Аналіз концептуальних підходів до управління безпекою багатоелементних систем

Запобігання небезпечним ситуаціям у сучасному діджиталізованому навколишньому середовищі практично неможливе без використання систем управління на всіх етапах життєвого циклу від проєктування до утилізації. У багатьох концепціях процес управління безпекою розглядається відносно багатоелементної, але цілісної системи.

У праці [31] виділяють два підходи до управління безпекою. Традиційний (враховуючи час публікації, його можна трактувати як застарілий) полягає у реагуванні на інциденти після їх виникнення з відпрацюванням корегувальних та відновлювальних заходів. Сучасний підхід додатково передбачає постійний моніторинг ситуації та застосування комплексу моделей для передбачення інцидентів і вживання відповідних заходів щодо запобігання їм, а також інтегрувальної інформаційно-аналітичної системи в складі комплексу управління безпекою.

Також розрізняють два підходи до визначення концепцій безпеки [2]:

а) щодо форми розвитку ресурсів, узгодження конкурентних викликів та діяльності стосовно зовнішнього середовища;

б) як протидію загрозам та забезпечення супутніх показників.

Серед основних положень концепції управління безпекою важливе місце належить політиці безпеки як загальному й цілому [2; 19], а також поділу політик на глобальну та локальні [17; 32; 33].

Аналіз концептуальних підходів до управління безпекою розподілених ІТ-систем

Концептуальні підходи до процесу управління безпекою ІТ-систем як сукупності розподілених елементів висвітлено у низці праць, зафіксованих у стандартах. Типові концепції проаналізовано на основі сукупності ідентифікаторів: (джерело опису, назва, об’єкт захисту, принципи) та зведено у табл. 1.

Таблиця 1

Порівняння концептуальних підходів до управління безпекою розподілених ІТ-систем

№ з/п	Показники	Концептуальні підходи
1	Джерело	Критичні інфраструктури [11]:
	Назва	Концепція: “безпечна інфраструктура з небезпечних і ненадійних незалежних систем”
	Об’єкт	Критична інфраструктура як інтегральна система, що складається з функціонально самостійних (слабо залежних) систем, які можуть функціонувати абсолютно незалежно (слабо залежно) одна від одної
	Принципи	– динамічний аналіз безпеки; – облік емерджентного ризику в критичних інфраструктурах; – інтеграція результатів апріорного і апостеріорного аналізу безпеки; – послідовно-паралельна інтеграція методів оцінки безпеки; – декомпозиція невизначеності; – інфраструктурне резервування і диверсності для забезпечення безпеки критичних інфраструктур
2	Джерело	Кіберфізичні системи [10]:
	Назва	Концепція “об’єкт – загроза – захист”
	Об’єкт	Кіберфізичні багаторівневі системи: – рівень кібернетичної платформи – інформаційні ресурси (ІР), інформаційні системи (ІС), інформаційні процеси (ІП); – рівень комунікаційної платформи – інформаційні мережі та канали (ІМ (К); – рівень фізичної платформи – давачі (Д)
	Принципи	– менеджмент ризику; – зобов’язання; – службові обов’язки і відповідальність; – цілі, стратегії і політика; – управління життєвим циклом
3	Джерело	Системи інформаційних і телекомунікаційних технологій [15]:
	Назва	Концепція менеджменту безпеки інформаційних і телекомунікаційних технологій
	Об’єкт захисту	Активи інформаційних і телекомунікаційних технологій (все, що має цінність для організації). Активи включають в себе таке (але не обмежуються): – матеріальні активи (обчислювальні засоби, засоби зв’язку, будівлі); – інформацію (дані) (документи, бази даних); – програмне забезпечення; – здатність виробляти продукт або надавати послугу; – персонал; – нематеріальні ресурси (престиж фірми, репутацію)
	Принципи	– менеджмент ризику; – зобов’язання; – службові обов’язки і відповідальність; – цілі, стратегія і політика; – управління життєвим циклом

Закінчення табл. 1

4	Джерело	Промислові системи [16]:
	Назва	Концепція безпеки систем промислової автоматики і контролю
	Об’єкт захисту	Майнові об’єкти – фізичні або логічні об’єкти, які належать організації або стосуються її у певний спосіб, являючи собою для неї відчутну або реальну цінність. Такі об’єкти можна поділити на фізичні й логічні, а також кадрові ресурси
	Принципи	У явному вигляді принципи не представлені. Можна розглянути як фундаментальні вимоги до безпеки промислової автоматики: – управління доступом (AC); – контроль за використанням (UC); – цілісність даних (DI); – конфіденційність даних (DC); – обмеження потоку даних (RDF); – своєчасне реагування на подію (TRE); – доступність ресурсів (RA)
5	Джерело	Інформаційні системи [17]:
	Назва	Концепція процесу менеджменту інформаційної безпеки
	Об’єкт захисту	Цінні активи – все, що має цінність для організації
	Принципи	– розуміння вимог інформаційної безпеки організації та необхідності проводити політику і встановлювати цілі інформаційної безпеки; – уведення директив щодо впровадження та експлуатації для управління ризиками інформаційної безпеки організації в контексті сумарних бізнес-ризиків організації; – моніторинг і перевірка якості функціонування та ефективності системи менеджменту інформаційної безпеки; – постійне вдосконалення, що грунтується на реальних оцінках
6	Джерело	Бізнес-системи [34]:
	Назва	Концепція готовності ІКТ до забезпечення безперервності бізнесу (IRBC – ICT readiness for business continuity)
	Об’єкт захисту	Бізнес-операції, бізнес-послуги
	Принципи	– запобігання інцидентам; – виявлення інцидентів; – реагування на інциденти; – відновлення; – удосконалення

Концепція управління безпекою розподілених IT-систем і мінімізація енергоспоживання

Концепція управління безпекою за умови мінімізації енергоспоживання розвивається відповідно до складних систем, побудованих на принципах розподіленої та динамічної архітектури. Вона формулюється як концепція гарантування та управління інформаційною безпекою IT-інфраструктур за фактичним станом під час мінімізації їхнього енергоспоживання.

Методологія управління безпекою розподілених ІТ-інфраструктур

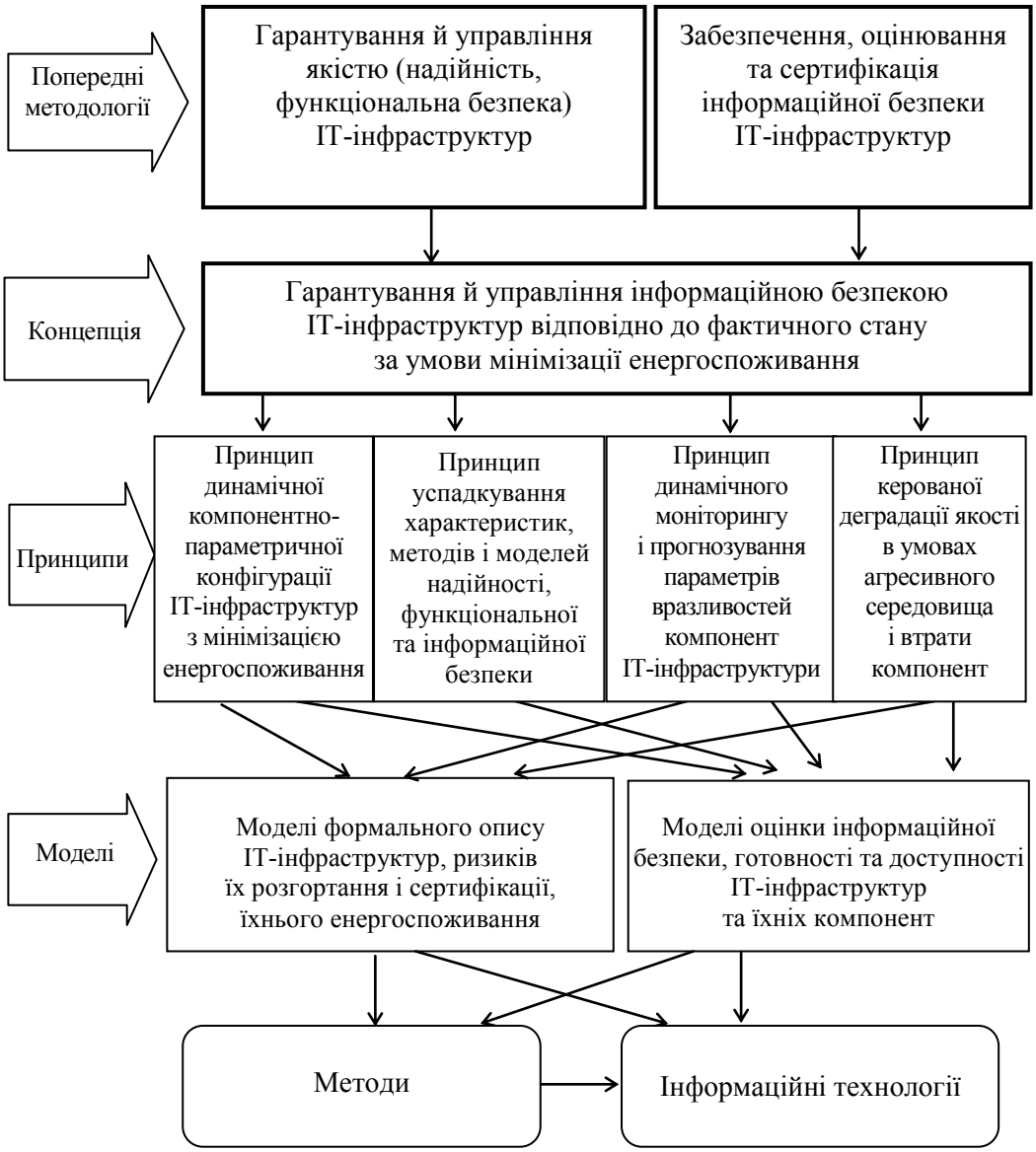

Рис. 1. Концепція управління безпекою та енергоефективністю розподілених ІТ-інфраструктур

Розроблені елементи методології реалізуються за допомогою формулювання (розробки) і використання таких принципів:

1) динамічної компонентно-параметричної конфігурації розподілених ІТ-інфраструктур та їхніх інформаційних систем із мінімізацією енергоспоживання, що реалізується за допомогою формального теоретико-множинного представлення динаміки зміни вхідних і вихідних параметрів ІТ-інфраструктур, їх функціональних характеристик, архітектурних рішень, а також розробки та застосування моделей і методів оцінки ризиків на етапах розгортання та сертифікації;

2) успадкування характеристик, методів і моделей надійності, функціональної та інформаційної безпеки, суть якого полягає в застосуванні оцінних підходів до властивостей інформаційної безпеки і категорування ІТ-інфраструктур на підставі значень оцінених показників, що мають змінний у часі ймовірнісний характер;

3) динамічного моніторингу і прогнозування параметрів вразливостей компонент розподілених ІТ-інфраструктур для оцінювання й мінімізації ризиків атак на них. Для реалізації цього принципу потрібно розробити підхід щодо дослідження впливу зовнішніх факторів на ймовірність проведення атаки, а також до об'єднання інструментаріїв аналітичних апаратів передбачення часових параметрів вияву вразливостей, проведення атак і зміни зовнішніх факторів ІТ-проєкту;

4) принцип керованої деградації якості розподілених ІТ-інфраструктур в умовах агресивного середовища і втрати компонент. Для його реалізації потрібно розробити:

– теоретико-множинний опис стратегії відновлення й тестування компонент із можливим відкатом до попередньої версії;

– модель допустимих втрат якості обслуговування та їхнього впливу на рейтингові показники ІТ-проєкту через проведення оновлення програмного забезпечення, тестування нового функціоналу, аудиту інформаційної та кібербезпеки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Виконано аналіз теоретичних і технологічних напрацювань із концептуальних питань управління безпекою організаційно складних систем різних галузей життєдіяльності. Узагальнено визначення безпеки системи як стану з відсутністю неприйнятного ризику завдання шкоди елементам системи, людям, навколишньому середовищу, бізнесу та ін.

Наразі концепції управління безпекою мають спільну складову, що визначає ризик-орієнтований підхід з елементами планування, прогнозування, запобігання, протидії та адаптації системи управління.

Досліджено дуалізм визначення безпеки як "safety" та "security". Проаналізовано підходи до поєднання цих складових у рамках інтеграційної властивості "гарантоздатність".

Сучасні концепції управління безпекою використовують ієрархічне ранжування властивостей “safety” та “security”, за якого вищою метою є запобігання катастрофічним наслідкам та людським жертвам (складова “safety”), до яких може призвести втручання в інформаційне поле та кіберпростір (складова “security”).

Проаналізовано концепції управління безпекою розподілених ІТ-систем на прикладі критичних інфраструктур, інформаційно-телекомунікаційних систем, систем промислової автоматики, кіберфізичних систем та систем неперервного бізнесу. Визначено, що різні концепції можуть використовувати загальні принципи, такі як управління (менеджмент) ризиком, удосконалення/адаптація системи управління безпекою.

У подальшому необхідно дослідити основні принципи, що входять до складу концепцій управління безпекою розподілених ІТ-інфраструктур.

Список використаних джерел:

1. *Yeun R., Bates P., Murray P.* Aviation safety management systems // World Review of Intermodal Transportation Research. 2014. Vol. 5. № 2. P. 168–196.
2. *Kozachenko G., Lyashenko O., Bezbozhnyy V.* Enterprise economic security management conception // TEKA Kom. Mot. i Energ. Roln. OL PAN. 2010. 10A. P. 263–270.
3. *Череп О. Г., Степаненко О. В.* Концепція управління економічною безпекою машинобудівних підприємств // Сталий розвиток економіки. 2013. № 4. С. 110–114.
4. *Шаньгин В. Ф.* Информационная безопасность компьютерных систем и сетей: учеб. пособие. Москва: ИД “ФОРУМ” : ИНФРА-М, 2017. 416 с.
5. *Raggad B.* Information Security Management: Concepts and Practice. London: CRC Press, 2010. 868 p.
6. Концепция управления безопасностью в администрации города Перми. URL: http://docs.cntd.ru/document/428682486. – 15.10.2019 р.
7. Концепція національної екологічної політики України на період до 2020 року: розпорядження Кабінету Міністрів України від 17 жовтня 2007 р. № 880-р. URL: https://zakon.rada.gov.ua/laws/show/880-2007-%D1%80. – 15.10.2019 р.
8. Концепція // Енциклопедія сучасної України. URL: http://esu.com.ua/search_articles.php?id=3256. – 15.10.2019 р.
9. *Судакова О. І., Медведовська Т. П., Гарбуз Є. В., Лутченко О. В.* Управління безпекою взаємодії підприємства з контрагентами, діючими в загальному життєвому просторі // Глобальні та національні проблеми економіки. 2017. № 19. С. 256–261.

10. *Дудикевич В. Б., Микитин Г. В., Ребець А. І.* До проблеми управління комплексною системою безпеки кіберфізичних систем // Вісник Національного університету "Львівська політехніка". Інформаційні системи та мережі. 2018. № 901. С. 10–21.

11. *Брежнев Е. В., Харченко В. С.* Методология обеспечения безопасности критических инфраструктур в условиях неопределенности: концепция и принципы // Радіоелектронні і комп'ютерні системи. 2015. № 1. С. 25–32.

12. *Dudykevych V., Mykytyn G., Kret T., Rebets A.* Security of Cyber-Physical Systems from Concept to Complex Information Security System // Advances in cyber-physical systems. 2016. Vol. 1. № 2. P. 67–75.

13. *Гордеев А. А., Харченко В. С.* Элементы методологии профиле-ориентированного оценивания качества программного обеспечения информационных систем // Проблеми інформатизації та упр.: зб. наук. пр. 2014. Т. 3. Вип. 47. С. 24–30.

14. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем: монографія / В. С. Харченко, С. В. Яковлев, О. С. Горбачик та ін.; за ред. В. С. Харченка, С. В. Яковлева. Харків: Константа, 2019. 272 с.

15. ISO/IEC 13335-1: 2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. URL: https://www.iso.org/standard/39066.html. – 15.10.2019 p.

16. IEC TS 62443-1-1:2009. Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. URL: https://webstore.iec.ch/publication/7029. – 15.10.2019 p.

17. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: https://www.iso.org/standard/73906.html. – 15.10.2019 p.

18. Концепція забезпечення національної безпеки у фінансовій сфері: розпорядження Кабінету Міністрів України від 15 серпня 2012 р. № 569-р. URL: https://zakon.rada.gov.ua/laws/show/569-2012-%D1%80. – 15.10.2019 p.

19. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 – 15.10.2019 p.

20. IEC 61508-1:2010. Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements. URL: https://webstore.iec.ch/publication/5515. – 15.10.2019 p.

21. ARP 4761. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. URL: https://www.sae.org/standards/content/arp4761. – 15.10.2019 p.

22. ISO 26262-1:2018. Road vehicles – Functional safety – Part 1: Vocabulary. URL: https://www.iso.org/standard/68383.html. – 15.10.2019 p.

23. CENELEC – EN 50159. Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems. URL: https://standards.globalspec.com/std/1285055/EN%2050159. – 15.10.2019 p.

24. IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. URL: https://webstore.iec.ch/publication/5532. – 15.10.2019 p.

25. *Gluschke G.* Cyber security policies and critical infrastructure protection. Potsdam: Institute for Security and Safety (ISS) Press, 2018. 388 p.

26. *Limba T., Plėta T., Agafonov K., Damkus M.* Cyber security management model for critical infrastructure. // Entrepreneurship and Sustainability Issues. 2017. Vol. 4 (4). P. 559–573.

27. Cyber security of critical infrastructures / Maglaras L., Kim K., Janicke H. and oth. // ICT Express. 2018. Vol. 4 (1). P. 42−45.

28. *Dhawan S.* Information and Data Security Concepts, Integrations, Limitations and Future // International Journal of Advanced Information Science and Technology (IJAIST). 2014. Vol. 3 (9). P. 9–13.

29. *Avizienis A., Laprie J.-C., Randell B.* Dependability and its threats: a taxonomy // In Proc. Of the IFIP 18th World Computer Congress, Kluwer Academic Publishers. 2004. P. 91–120.

30. *Шубинский И. Б.* Функциональная надежность информационных систем. Методы анализа. Москва: "Журнал Надежность", 2012. 296 с.

31. *Малыгин В. Б., Нечаев Е. Е.* Обеспечение безопасности полётов при управлении воздушным движением: учебное пособие. Москва: Изд. Московского государственного технического университета гражданской авиации, 2011. 86 с.

32. Концепція глобального управління безпекою. URL: https://ssbb.com.ua/uk/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/koncepciya-globalnogo-upravleniya-bezopasnostu. – 15.10.2019 p.

33. *Carder J.* How to build a SOC with limited resources. Maidenhead: LogRhythm Labs, 2018. 16 p.

34. ISO/IEC 27031:2011. Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. URL://www.iso.org/standard/44374.html (accessed 15.10.2019).

References:

1. Yeun R., Bates P. and Murray P. (2014), "Aviation safety management systems", posted in World Review of Intermodal Transportation Research, vol. 5, No. 2, pp. 168–196.

2. Kozachenko G., Lyashenko O. and Bezbozhnyy V. (2010), Enterprise economic security management conception, TEKA Kom. Mot. i Energ. Roln. OL PAN, 2010. 10A, pp. 263–270.

3. Cherep O. G. and Stepanenko O. V. (2013), "*Kontseptsiya upravlinnya ekonomichnoyu bezpekoyu mashynobudivnykh pidpryyemstv"* ["The concept of economic safety management of machine-building enterprises"], Journal *Stalyy rozvytok ekonomiky* [Sustainable development of economy], vol. 4, pp. 110–114.

4. Shangin V. F. (2017), *Informatsionnaya bezopasnost' komp'yuternykh sistem i setey* [Information Security of Computer Systems and Networks], Moscow, Press Publishing House "FORUM": INFRA-M, 416 p.

5. Raggad B. (2010), Information Security Management, Concepts and Practice, London: CRC Press, 868 p.

6. *Kontseptsiya upravleniya bezopasnost'yu v administratsii goroda Permi.* [Security Management Concept in Perm City Administration], available at: http://docs.cntd.ru/document/428682486 (accessed 15.10.2019).

7. KMU (2007), *Kontseptsiya natsional'noyi ekolohichnoyi polityky Ukrayiny na period do 2020 roku* [The concept of national environmental policy of Ukraine for the period up to 2020Concept of national environmental policy of Ukraine for the period up to 2020], the Decree of the Cabinet of Ministers of Ukraine of October 8, No. 880-p, available at: https://zakon.rada.gov.ua/laws/show/880-2007-%D1%80 (accessed 10.15.2019).

8. *Kontseptsiya* [Concept], *Entsyklopediya Suchasnoyi Ukrayiny* [Encyclopedia of Such Ukraine], available at: http://esu.com.ua/search_articles.php?id=3256 (accessed 15.10.2019).

9. Sudakova O. I., Medvedovskaya T. P., Garbuz E. V. and O. V. Lutchenko et al (2017), *"Upravlinnya bezpekoyu vzayemodiyi pidpryyemstva z kontrahentamy, diyuchymy v zahal'nomu zhyttyevomu prostori"* ["Management of security of interaction of the enterprise with the counterparties operating in the common living space"], Journal *Hlobal'ni ta natsional'ni problemy ekonomiky* [Global and national problems of economy], vol. 19, pp. 256–261.

10. Dudykevych V. B., Mykytin G. V. and Rebetets' A. I. (2018), *"Do problemy upravlinnya kompleksnoyu systemoyu bezpeky kiberfizychnykh system"* ["On the problem of control of complex security system of cyberphysical systems'], Bulletin of the National university "Lviv Polytechnic". Information systems and networks, vol. 901, pp. 10–21.

11. Brezhnev Ye. V. and Kharchenko V. S. (2015), *"Metodologiya obespecheniya bezopasnosti kriticheskikh infrastruktur v usloviyakh neopredelennosti: kontseptsiya i printsipy"* ["Methodology for Critical Infrastructure Safety in Uncertainty: Concept and Principles"], Journal *Radíoyelektronní í komp'yuterní sistemi* [Radioelectronic and Computer Systems], vol. 1, pp. 25–32.

12. Dudykevych V., Mykytyn G., Kret T. and Rebets A. (2016), "Security of Cyber-Physical Systems from Concept to Complex Information Security System", Advances in cyber-physical systems, vol. 1, No. 2, pp. 67–75.

13. Gordeyev A. A. and Kharchenko V. S. (2014), *"Elementy metodologii profileoriyentirovannogo otsenivaniya kachestva programmnogo obespecheniya informatsionnykh sistem"* ["Elements of methodology of profile oriented evaluation of software quality of information systems"], a collection of scientific works *Problemy informatyzatsiyi ta upravlinnya* [Problems of informatization and management], t. 3, vol. 47, pp. 24–30.

14. Kharchenko V.S., Yakovlev S.V., Gorbachik O.S. and oth. (2019), *Zabezpechennya funktsional'noyi bezpeky krytychnykh informatsiyno-keruyuchykh system* [Functional safety of critical information and control systems], monograph. Kharkiv: Constant, 272 p.

15. ISO/IEC 13335–1: 2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, available at: https://www.iso.org/standard/39066.html (accessed 51.10.2019).

16. IEC TS 62443–1–1:2009, Industrial communication networks – Network and system security – Part 1–1: Terminology, concepts and models, available at: https://webstore.iec.ch/publication/7029 (accessed 15.10.2019).

17. ISO/IEC 27000:2018, Information technology − Security techniques – Information security management systems − Overview and vocabulary, available at: https://www.iso.org/standard/73906.html (accessed 15.10.2019).

18. KMU (2012), *Kontseptsiya zabezpechennya natsional'noyi bezpeky u finansoviy sferi* [The concept of ensuring national security in the financial sphere], Ordinance of the Cabinet of Ministers of Ukraine of August 15, No. 569-p. URL: https://zakon.rada.gov.ua/laws/show/569-2012-%D1%80 (accessed 10.15.2019).

19. President of Ukraine (2016), *Stratehiya kiberbezpeky Ukrayiny* [Ukraine's Cybersecurity Strategy], Presidential Decree No. 96/2016 of March 15, available at: https://zakon5.rada.gov.ua/laws/show/96/2016 (accessed 15.10.2019).

20. IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements, available at: https://webstore.iec.ch/publication/5515. (accessed 15.10.2019).

21. ARP 4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, available at: https://www.sae.org/standards/content/arp4761/ (accessed 15.10.2019).

22. ISO 26262-1:2018, Road vehicles – Functional safety – Part 1: Vocabulary, available at: https://www.iso.org/standard/68383.html (accessed 15.10.2019).

23. CENELEC – EN 50159, Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems, available at: https://standards.globalspec.com/std/1285055/ EN%2050159 (accessed 15.10.2019).

24. IEC 61513:2011, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, available at: https://webstore.iec.ch/publication/5532 (accessed 15.10.2019).

25. Gluschke G. (2018), Cyber security policies and critical infrastructure protection. Potsdam: Institute for Security and Safety (ISS) Press, 388 p.

26. Limba T., Plėta T., Agafonov K. and Damkus M. (2017), "Cyber security management model for critical infrastructure.", Journal Entrepreneurship and Sustainability Issues, vol. 4 (4), pp. 559–573.

27. Maglaras L., Kim K. and Janicke H. et al. (2018), "Cyber security of critical infrastructures", Journal ICT Express, vol. 4 (1), pp. 42–45.

28. Dhawan S. (2014), "Information and Data Security Concepts, Integrations, Limitations and Future", International Journal of Advanced Information Science and Technology (IJAIST), vol. 3 (9), pp. 9–13.

29. Avizienis A., Laprie J.-C. and Randell B. (2004), "Dependability and its threats: a taxonomy", In Proc. Of the IFIP 18th World Computer Congress, Kluwer Academic Publishers, pp. 91–120.

30. Shubinskiy I. B. (2012), *Funktsional'naya nadezhnost' informatsionnykh sistem. Metody analiza* [Functional reliability of information systems. Methods of analysis], Moscow, Press Reliability Magazine, 296 p.

31. Malygin V. B. and Nechayev Ye. Ye. (2011), *Obespecheniye bezopasnosti polotov pri upravlenii vozdushnym dvizheniyem* [Flight safety in air traffic control], Tutorial, Moscow, Press Moscow State Technical University of Civil Aviation, 86 p.

32. *Kontseptsiya hlobal'noho upravlinnya bezpekoyu* [Global security management concept, available at: https://ssbb.com.ua/uk/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/koncepciya-globalnogo-upravleniya-bezopasnostu/ (accessed 15.10.2019)

33. Carder J. (2018), How to build a SOC with limited resources. Maidenhead: LogRhythm Labs, 16 p.

34. ISO/IEC 27031:2011, Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity, available at: https://www.iso.org/standard/44374.html (accessed 15.10.2019).