Міністерство освіти і науки України

Системні технології

System technologies

4 (141) 2022

Регіональний міжвузівський збірник наукових праць

Засновано у січні 1997 року.

У випуску:

– ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ОРГАНІЗАЦІЯ СУЧАСНОГО ВИРОБНИЦТВА

– МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

– СИСТЕМНІ ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

DOI 10.34185/1562-9945-4-141-2022-13
УДК 004.056.5

Ю.С.Тарасенко, В.Ю.Клим

БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ПОЗИЦІЙ ЗНИЖЕННЯ РЕЗУЛЬТАТИВНОСТІ РИЗИКІВ

Аннотація. Запропонована структурно-лінгвістична схема методології побудови системи захисту та безпеки об'єктів критичної інфраструктури (ОКІ) з позицій зниження результативності ризиків. Виконано аналіз Системи оцінювання ризику безпеки сукупності ОКІ та доступу до неї. Вона фактично має універсальну структуру та може бути використана в будь-якій організованій сфері діяльності соціуму незалежно від виду галузі, розмірів організації, рівня професіоналізму штатного персоналу, відповідального за безпеку. Обґрунтована доцільність підвищених зобов`язань щодо метрологічної надійності засобів вимірювання з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації принципу невизначеності при забезпеченні достовірності вимірювань.
Ключові слова: системи захисту та безпеки, системи оцінювання ризику безпеки.

Постановка проблеми. В основі штатної працездатності об'єктів критичної інфраструктури (ОКІ), відповідно до методології побудови пізнавальної моделі їх захисту та безпеки [1], лежала процедура перевірки справжності доступу до них – аутентифікації. Реалізація останньої була розглянута з позицій стандартів України, які мають аналоги у межах ISO щодо оцінювання супутніх ризиків згідно фізичної та інформаційної безпеки. Саме з цих позицій менеджмента ризику (risk management) [2] – «скоординированных действий по руководству и управлению организацией в области риска» – продовжено аналіз запропонованої Системи оцінювання ризику безпеки сукупності об'єктів критичної інфраструктури (СОКІ) та доступу до неї з позицій зниження результативності ризиків. При цьому, із врахуванням вибору критеріїв ризику та «ступеню реалізації запланованих робіт і досягнення запланованих результатів» (тобто результативності [3. п.3.7.11]) доцільно розглянути наступні підсистеми: стандартів України [2,4-6] загального оцінювання ризику, які є аналоги у межах ISO; методів загального оцінювання ризику згідно IEC/ISO 31010 2013 (Додаток В) [4]; оцінювання втрат безпеки згідно ДСТУ ISO/IEC 27000:2019 (конфіденційності, цілісності, доступності, спостережності, автентичності, на-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

дійності [7] та стійкості рубежів захисту [8]); фільтрації даних ризиків, згідно ДСТУ ISO/IEC 27001:2013 та підтримки прийняття рішень (ПсППР) доступа до СОКІ [9, Ст.1, п.1, поз.9].

Аналіз останніх досліджень і публікацій. Слід звернути увагу, що в цих стандартах аспекти безпеки мають інформативний характер, де від провадження загального оцінювання ризику маємо деякі основні вигоди [4, с.2], а саме: розуміння ризику та його потенційного впливу на досягнення цілей; надання інформації особам, які приймають рішення; поліпшення розуміння ризиків з тим, щоб допомогти у вибиранні варіантів їх обробляння; ідентифікування важливих чинників, що сприяють ризикам, і слабких ланок у системах та організаціях; порівняння з ризиками в альтернативних системах, технологіях або підходах; обмінювання інформацією про ризики та невизначеності; допомога в установленні пріоритетів; запобігання інцидентам на основі розслідування їхніх причин та наслідків; вибирання різних форм обробляння ризику; задоволення регуляторних вимог; забезпечування інформацією, яка дає змогу оцінити, наскільки ризик потрібно прийняти, якщо брати до уваги попередньо визначені критерії; загальне оцінювання ризиків, пов’язаних з утилізацією продукції після закінчення строку її служби.

З наданих в стандарті [2, с.4,5] формулювань випливає, що загальне оцінювання ризику – це спільний процес: *ідентифікування ризику*, *аналізування ризику та оцінювання ризику*. Причому загальне оцінювання ризику повинно відповідати його (ризику) критеріям, які встановлюють на початку процесу оцінки ризику, а у разі потреби обов'язково переглядають та коригують. Більш того, необхідно враховувати умови для вибору критеріїв ризику, виходячи з оцінки їх значущості за підтримки процесів прийняття рішень, які мають бути узгоджені зі структурою управління ризиками та адаптовані до конкретних цілей та обсягів аналізованої діяльності згідно ДСТУ ISO 31000:2018 [5, п.6.3.4] (табл. 1).

Отже, оцінка ризику – це фактично процес, спрямований на досягнення цілей як за змістом (у різних галузях життєдіяльності соціуму), так і за призначенням (наприклад, як розробки проектів, технологій, продукції тощо), який, забезпечуючи ідентифікацію ризику, аналіз ризику та порівняльну оцінку ризику [5, п.6.4.1], має використовувати сучасну методологію побудови, у даному випадку СОКІ, з оптимізацією відомих та створенням нових систем контролю та управління доступу (СКУД) до них.

Таблиця 1

Умови для вибору критеріїв ризику (їх залежністі)

Позначення	Зміст залежності умов від наступних чинників:
ВК.1	характеру та типу невизначеностей, які можуть вплинути на результати та досягнення цілей (як матеріальні, так і нематеріальні)
ВК.2	способу визначення та оцінки наслідків (як позитивних, так і негативних) та їх ймовірність
ВК.3	факторів, пов'язаних з часом
ВК.4	коректності та узгодженості застосовуваних методів вимірювань
ВК.5	порядку визначення рівня ризику
ВК.6	способу обліку комбінації та послідовності множинних ризиків
ВК.7	масштабу організації, підприємства, офісу та ін.

З метою запобігання несанкціонованому фізичному доступу, будь-яким пошкодженням та втручанню зі втратою (частковою або повною) конфіденційності, цілісності, доступності, спостережності, автентичності та надійності як службової інформації організації, так і цілісності виробничої системи організації з її засобами отримання, обробки та зберігання інформації необхідно виконати вибір методу оцінювання ризику та реалізації відповідного захисту, які суттєво залежать від наступних чинників: внутрішнього та зовнішнього середовища організації [5, п.5.4.1]; стійкості рубежів захисту зон безпеки і безпеки обладнання [8, п.А.11]; професіоналізму співробітників [5, п.5.4.2,3] у процесі прийняття рішень та змісту методів згідно [4, Додаток В (довідковий) с. 18-71] ДСТУ IEC/ISO 31010:2013 у межах (IEC/ISO 31010:2009, IDT), які викладено в таблиці 2.

Мета роботи полягає в обґрунтуванні та аналізі запропонованої пізнавальної структурно-лінгвістичної схеми (СЛС) методології побудови Системи захисту та безпеки об’єктів критичної інфраструктури (ОКІ) з позицій зниження результативності ризиків, згідно рекомендацій ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) відносно п.3.12.4 [3] (рис.1).

Викладення основного матеріалу дослідження. Очевидно, що підвищення рівня захисту СОКІ, оцінювання втрат безпеки (згідно з гіпотетичним кіберінцидентам, які мають ймовірнісний характер), – це динамічний процес залучення ресурсів (методів, способів та алгоритмів) мультисервісної мережі зв'язку (криптографічних, канальних та інших) з її кореляційними пристроями, що фільтрують, реалізованими під конкретні вимоги (завдання) користувачів для передачі інформації, що захищається. Отже, вибір рівнів спрацьовування

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

кінцевих порогових блоків має багатопрофільний характер і залежить від задекларованих ймовірностей правильного виявлення чи пропуску кібератак чи кіберзагроз [1].

Таблиця 2

Методи загального оцінювання ризику

Позначення	Зміст методів
B.1	Мозкова атака
B.2	Структуроване чи напівструктуроване опитування
B.3	Метод Дельфі
B.4	Переліки контрольних запитань
B.5	Попереднє аналізування небезпечних чинників (PHA)
B.6	Метод HAZOP (HAZard and Operability study) – дослідження небезпечних чинників і працездатності
B.7	Аналізування небезпечних чинників і критичні точки контролю
B.8	Загальне оцінювання екологічного ризику
B.9	Структурований метод «Що – якщо» (SWIFT)
B.10	Аналізування сценарію
B.11	Аналізування впливу на діяльність (BIA)
B.12	Аналізування першопричин (RCA)
B.13	Аналізування видів і наслідків відмов (FMEA) і аналізування видів, наслідків і критичності відмов (FMECA)
B.14	Аналізування дерева відмов (FTA)
B.15	Аналізування дерева подій (ETA)
B.16	Аналізування причин і наслідків
B.17	Аналізування причинно-наслідкових зв’язків
B.18	Аналізування рівнів захисту (LOPA)
B.19	Аналізування дерева рішень
B.20	Загальне оцінювання надійності людини (HRA)
B.21	Аналізування діаграми «краватка-метелик»
B.22	Технічне обслуговування, зорієнтоване на забезпечення безвідмовності
B.23	Аналізування паразитних впливів (SA) і аналізування паразитних схем (SCA)
B.24	Марковське аналізування
B.25	Імітаційне моделювання методом Монте-Карло
B.26	Байєсівська статистика та мережі Байєса
B.27	Криві FN
B.28	Індекси ризику
B.29	Матриця наслідків/імовірностей
B.30	Аналізування витрат і вигод (CBA)
B.31	Багатокритерійне аналізування рішень (MCDA)

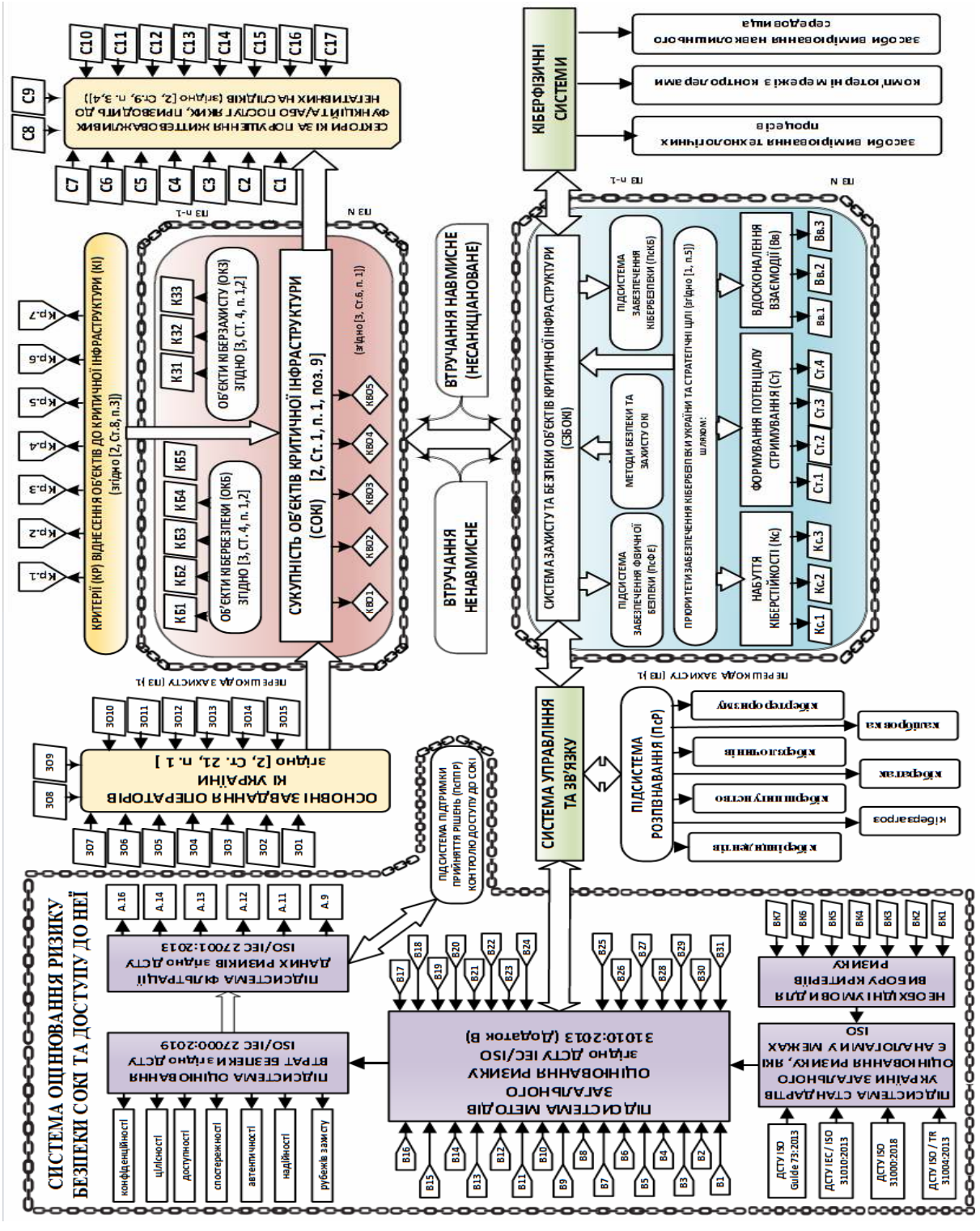

Рисунок 1 – Структурно-лінгвістична схема (СЛС) методології побудови Системи захисту та безпеки об’єктів критичної інфраструктури (ОКІ) з позицій зниження результативності ризиків

При цьому підсистема фільтрації даних ризиків виконує вирішальну роль щодо наступних об'єктів та процесів: управління доступом; зон фізичної без-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

пеки та захисту від навколишнього середовища; безпеки під час обробки інформації; безпеки зв'язку; придбання, розробка та підтримка систем та управління інцидентами інформаційної безпеки. Причому детальний опис змісту аспектів, згідно вимог менеджменту інформаційної безпеки, наведено у [8], а найбільш важливі для процесів оцінки та обробки ризиків безпеки СОКІ висвітлені в таблиці 3. Хоча очевидно, що жодна підсистема фільтрації (обробки) даних ризиків не здатна забезпечувати 100% ефективність.

Таблиця 3

Аспекти процесів оцінки та обробки ризиків безпеки СОКІ

Позначення	Напрями та зміст аспектів
А.9	Управління доступом
А.11	Фізична безпека та захист від навколишнього середовища А.11.1 Зони безпеки А.11.2 Безпека обладнання
А.12	Безпека при обробці інформації А.12.1 Операційні процедури та відповідальність А.12.2 Захист від шкідливого ПЗ А.12.3 Резервне копіювання А.12.4 Логи та моніторинг А.12.5 Контроль системного програмного забезпечення (ПЗ) А.12.6 Управління технічними уразливістю А.12.7 Проведення аудиту інформаційних систем
А.13	Безпека зв'язку А.13.1 Управління безпекою мережі А.13.2 Передача інформації
А.14	Придбання, розробка та підтримка систем А.14.1 Вимоги безпеки до інформаційних систем А.14.2 Безпека при розробці та допоміжних процесах А.14.3 Тестові дані
А.16	Управління інцидентами інформаційної безпеки А.16.1 Управління інцидентами інформаційної безпеки та покращення

Наведені дані в таблиці 3 дозволяють оптимізувати доступ до СОКІ завдяки підсистемі підтримки прийняття рішень (ПсППРД) доступу до СОКІ. Ця підсистема завжди функціонуватиме в умовах «невизначеності», у тому числі залежної від зміни кліматичних умов навколишнього середовища. Причому, в ДСТУ ISO 31000:2018 [5, п.3.1, Примітка 5], акцентують увагу на тому, що «неопределённость – это состояние полного или частичного отсутствия информации, необходимой для понимания события (3.5), его последствий (3.6) и их вероятностей», де мають місце наступні формулювання: «событие (event): - воз-

никновение или изменение специфического набора условий»; «последствие (consequence): - результат воздействия события (3.5) на объект».

Однак, слід зауважити, що відповідно до документів ISO/IEC будь-які вимірювання засобами вимірювання (ЗВ), у тому числі пов'язані з контролем навколишнього середовища або параметрів технологічних процесів, також піддаються принципу невизначеності. Тому доцільно виставляти підвищені зобов`язання до надійності і безпеки ЗВ з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації принципу невизначеності [10] при забезпеченні метрологічної достовірності вимірювань за допомогою будь-яких ЗВ [11].

Отже, ПсППР доступу до СОКІ зобов'язана забезпечувати розв'язання задач як щодо фізичного захисту від наслідків впливу навколишнього середовища, так і при реалізації безпеки безпосереднього процесу отримання та обробки супутньої інформації, що гіпотетично підпадає під можливі кіберінциденти.

Як відомо, добре організована з використанням сучасних технічних засобів системи контролю та управління доступом (СКУД) дозволяють вирішувати цілу низку завдань, до яких (як найважливішим) можна віднести такі [12]: «противодействие промышленному шпионажу; противодействие воровству; противодействие саботажу; противодействие умышленному повреждению материальных ценностей; учет рабочего времени; контроль своевременности прихода и ухода сотрудников; защита конфиденциальности информации; регулирование потока посетителей; контроль въезда и выезда транспорта. Кроме этого, СКУД является барьером для любопытных». Останнім часом, при реалізації конкретних СКУД, також використовують різні способи та реалізують пристрої для ідентифікації та аутентифікації особистості.

Отже, правильно побудована (адекватна реальності) модель СОКІ з його Системою захисту та безпеки, а також модель порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики, є важливою складовою успішного проведення аналізу ризику та визначення вимог до складу та характеристик інтегральної системи захисту. Проте, навіть в умовах багаторівневої системи перешкод жодна пізнавальна модель не може одночасно виконувати необхідно безліч завдань "захисного напрямку" [13, с.93]. Саме цьому доцільно оцінювати ефективність моделі в конкретному (обраному) аспекті її реалізації.

Причому в області СКУД не приділено достатньо серйозної уваги щодо контролю за подоланням повітряних рубежів захисту до підриву конкретної

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

захисної (охоронюваної) оболонки об'єкта. Тому для прикладу з виявленням несанкціонованих повітряних атак зловмисників, які використовують дрони, підходить демонстрація (задача) можливості забезпечення штатного рівня захисту ОКІ шляхом реалізації кореляційних радіолокаційних пристроїв ближньої взаємодії [14, с. 403] із супутніми пороговими блоками. При цьому завдання загальної та параметричної ідентифікації розпізнавання потенційних атак за допомогою дослідження гіпотетичної сигнальної аналогової дії слід також зводити, аналогічно [1], до кореляційного аналізу зондувальних та відбитих сигналів від дронів, які вторглись у повітряну область КВО, що охороняється.

Висновки. Таким чином, запропонована структурно-лінгвістична схема методології побудови системи захисту та безпеки об’єктів критичної інфраструктури з позицій зниження результативності ризиків. Виконано аналіз Системи оцінювання ризику безпеки сукупності ОКІ та доступу до неї. Показано, що СЛС має універсальну структуру та фактично може бути використана в будь-якій організованій сфері діяльності соціуму незалежно від виду галузі, розмірів організації, виділених матеріальних засобів та інтелектуального рівня штатного персоналу, відповідального за цю галузь безпеки та захисту. Обґрунтовано можливості реалізації, з позицій зниження результативності ризиків, функції щодо нівелювання потенційно небезпечних атак відносно СОКІ, які спрямовані як на розкрадання, спотворення цілісності та достовірності інформації, так і на можливі порушення так званих фізичних рубежів захисту інформації.

ЛІТЕРАТУРА

1. Тарасенко Ю.С. Методология побудови познавательной модели безопасности критической инфраструктуры. The methodology of building the cognitive model of critical infrastructure’s security/ Ю.С.Тарасенко, В.Ю. Клим // Materials of International scientific symposium: “Prospektive globale wissenschaftliche Trends '2022/Prospective global scientific trends'2022”,Karlsruhe,Germany,May,2022. –10 с.

2. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). [Чинний від 2014–07–01]. Вид. офіц. Київ: Мінекономрозвитку України, 2014. 17 с.

3. ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) Системи управління якістю. Основні положення та словник термінів. Київ ДП «УкрНДНЦ», 2016. 51 с.

4. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014–07–01]. Вид. офіц. Київ: Мінекономрозвитку України, 2015. 80 с.

5. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT).

[Чинний від 2019–01–01]. [Електронний ресурс]. – Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed– 2:v1:en
6. ДСТУ ISO/TR 31004:2013 Управління ризиками – Керівництво з впровадження ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT). [Чинний від 2019–01–01]. [Електронний ресурс]. – Режим доступа: https://www.iso.org/ standard/56610.html?browse=tc
7. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Київ ДП «УкрНДНЦ». Наказ від 16.10.2019 № 312.
8. ISO/IEC 27001:2013 Информационные технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности — Требования /Information technology — Security techniques — Information security management systems —Requirements/ Вторая редакція. 2013-10-01.
9. Закон Украины Про критичну інфраструктуру № 1882 - IX від 16.11.2021р. // Голос України. . – № 236 (14.12.2021).
10. ISO/IEC Guide 98– 1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. Неопределенность измерения. Часть 1. Введение в руководства по выражению неопределенности измерения. М. Стандартинформ. 2017.
11. Тарасенко Ю.С. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань / Ю.С.Тарасенко, В.Г. Соляніков // Збірник матеріалів міжнародної науково-практичної інтернет-конференції «Інноваційні технології, моделі управління кібербезпекою – «ІТМК– 2021», Дніпро, 14 – 16 квітня 2021 р. – С.29 – 30.
12. Ворона В. А. Системы контроля и управления доступом / В.°А.Ворона, В. А.Тихонов. – М.: Горячая линия – Телеком, 2010. – 272 с.
13. Вострецова Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова – Екатеринбург: изд- во Урал. ун- та, 2019. – 204 с.
14. Тарасенко Ю.С. Фізичні основи радіолокації: навч. посіб. / Ю.С.°Тарасенко – Д.: «Пороги», 2011. – 487с.

REFERENCES

1. Tarasenko Yu.S. Metodolohyia pobudovy poznavatelnoi modely bezopasnosty krytycheskoi ynfrastrukturы. The methodology of building the cognitive model of critical infrastructure’s security/Yu.S.Tarasenko, V.Iu. Klym//Materials of International scientific symposium: “Prospektive globale wissenschaftliche Trends '2022/Prospective global scientific trends' 2022”,Karlsruhe, Germany, May,2022.10 s.
2. DSTU ISO Guide 73:2013. Keruvannia ryzykom. Slovnyk terminiv (ISO Guide 73:2009, IDT). [Chynnyi vid 2014–07–01]. Vyd. ofits. Kyiv : Minekonomrozvytku Ukrainy, 2014. 17 s.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

3. DSTU ISO 9000:2015 (ISO 9000:2015,IDT) Systemy upravlinnia yakistiu. Osnovni polozhennia ta slovnyk terminiv. Kyiv DP «UkrNDNTs», 2016. 51 s.
4. DSTU IEC/ISO 31010:2013 Keruvannia ryzykom. Metody zahalnoho otsiniuvannia ryzyku (IEC/ISO 31010:2009, IDT). [Chynnyi vid 2014–07–01]. Vyd. ofits. Kyiv : Minekonomrozvytku Ukrainy, 2015. 80 s.
5. DSTU ISO 31000:2018 Menedzhment ryzykiv. Pryntsypy ta nastanovy (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). [Chynnyi vid 2019–01–01]. [Electronic resource] – Access mode: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed– 2:v1:en
6. DSTU ISO/TR 31004:2013 Upravlinnia ryzykamy – Kerivnytstvo z vprovadzhennia ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT). [Chynnyi vid 2019–01–01]. [Electronic resource] – Access mode: https://www.iso.org/standard/56610.html?browse=tc
7. DSTU ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Informatsiini tekhnolohii. Metody zakhystu. Systemy keruvannia informatsiinoiu bezpekoiu. Ohliad i slovnyk terminiv. Kyiv DP «UkrNDNTs». Nakaz vid 16.10.2019 № 312.
8. ISO/IEC 27001:2013 Informatsyonnye tekhnolohyy — Metody obespechenyia bezopasnosty — Systemы menedzhmenta ynformatsyonnoi bezopasnosty — Trebovanyia /Information technology — Security techniques — Information security management systems —Requirements/ Vtoraia redaktsiia. 2013.10.01.
9. Zakon Ukrainy Pro krytychnu infrastrukturu № 1882 - IX vid 16.11.2021r. // Holos Ukrainy. № 236 (14.12.2021).
10. ISO/IEC Guide 98– 1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. M. Standartynform. 2017.
11. Tarasenko Yu.S. Informatsiini systemy z pozytsii zabezpechennia nadiinosti ta nevyznachenosti vymiriuvan /Yu.S.Tarasenko, V.H. Soliannikov // Zbirnyk materialiv mizhnarodnoi naukovo-praktychnoi internet-konferentsii «Innovatsiini tekhnolohii, modeli upravlinnia kiberbezpekoiu – «ITMK– 2021», Dnipro, 2021. S.29 – 30.
12. Vorona V.A. Systemy kontrolia y upravlenyia dostupom / V.A.Vorona, V.°A.Tykhonov. M.: Horiachaia lynyia – Telekom, 2010. 272 s.
13. Vostretsova E. V. Osnovy informatsyonnoi bezopasnosty: uchebnoe posobye dlia studentov vuzov /E. V. Vostretsova. Ekaterynburh: yzd- vo Ural. un- ta, 2019. 204 s.
14. Tarasenko Yu.S. Fizychni osnovy radiolokatsii: navch. posib. / Yu.S.Tarasenko . D.: «Porohy», 2011. 487s.

Received 16.05.2022.
Accepted 18.05.2022.

Safety of critical infrastructure objects from the positions of risk effectiveness reduction

In the Ukrainian standards of general risk assessment, according to analogues within ISO, safety aspects are mainly informative. Therefore, both the quality of risk assessment and the reduction of its negative consequences (risk effectiveness) depend on the proper use of methods and techniques. that is why in order to prevent unauthorized physical and information access, ie any damage and interference with loss of confidentiality, integrity, accessibility, observation, authenticity and reliability of both official information of the organization and the integrity of the production system of the organization with their facilityes of obtaining, processing and storing information, it is necessary to make the correct choice of risk assessment method and further ensure the proper implementation of protection in accordance with the reduction of risk effectiveness.

The purpose of the work is to substantiate and analyze the proposed structural and linguistic scheme of the methodology of construction of the System of protection and safety of critical infrastructure objects (CIO) from the standpoint of risk effectiveness.

From the point of view of reduction of hypothetical negative consequences from risks for regular of CIO the conditions for potential risk criteria are given and the System of risk assessment of the security of the set of critical infrastructure objects (SCIO) is considered with access to it, which includes subsystems of: the Ukrainian standards of general risk assessment, declared methods of general risk assessment; assessment of security losses according to confidentiality, integrity, accessibility, observation, authenticity, reliability and stability of protection boundaries; filtering of these risks and supporting decision-making on access control to SCIO. The advisability of the increased obligations concerning reliability and safety of measuring instruments is proved in order to strict requirements for cybersecurity risk assessment in terms of realization the principle of uncertainty while ensuring the metrological reliability of measurements.

Тарасенко Юрій Станіславович —доцент кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів.
Клим Вікторія Юріївна — доцент кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів.

Tarasenko Yuri Stanislavovich — Assistant Professor of the Chair of Cybersecurity and Information Technologies, University of Customs and Finance.
Klym Viktoriia Yuriyivna — Assistant Professor of the Chair of Cybersecurity and Information Technologies, University of Customs and Finance.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)