КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.1241341
УДК 004.03/.05

Хлапонін Юрій Іванович
доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії
Київський національний університет будівництва і архітектури, Київ, Україна
ORCID ID 0000-0002-9287-0817
y.khlaponin@gmail.com

Козубцова Леся Михайлівна
кандидат технічних наук, доцент кафедри математики та фізики
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0002-7866-8575
l.kozubtsova@i.ua

Козубцов Ігор Миколайович
доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Штонда Роман Михайлович
начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0001-5986-0847
shtonda1982@ukr.net

ФУНКЦІЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. Предметом дослідження у науковій статті є система захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. Система захисту інформації і кібербезпеки – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки. Оскільки система захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури є відносно новою, тому відсутній єдиний погляд на те, які функції має виконувати ця система. В результаті продовжується процес її формування та становлення як системи. Постала необхідність у визначенні функцій для подальшого оцінювання ефективності функціонування її як системи. Оцінювання передбачається здійснювати як в процесі створення, приймання, так і повсякденній експлуатації. Для реалізації процедури оцінювання ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури необхідні часткові показники ефективності. За допомогою цих показників, можна охарактеризувати ступінь досягнення системою поставлених перед нею завдань. Запропоновано згідно функцій наступні показники ефективності: ID Ідентифікація ризиків кібербезпеки; PR Кіберзахист; DE Виявлення кіберінцидентів; RS Реагування на кіберінциденти; RC Відновлення стану кібербезпеки. Наукова новизна одержаного результату полягає в тому, що запропоновано універсальні функції, які має реалізовувати система захисту інформації і кібербезпеки на об'єктах критичної інформаційної інфраструктурі. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування показників та критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.

Ключові слова: функція; система; захист інформації; кібербезпека; об'єкт критичної інформаційної інфраструктури

ВСТУП

Система захисту інформації і кібербезпеки (СЗІКБ) – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки. Оцінка ефективності може здійснюватися в процесі створення, приймання та експлуатації СЗІКБ. Слід визнавати, що СЗІКБ є відносно новою, саме тому об’єктивно відсутній єдиний погляд на те, які функції має виконувати ця система.

Постановка проблеми. Згідно Закону України “Про основні засади забезпечення кібербезпеки України” [1]; Стратегії кібербезпеки України [2]; Рішення Ради національної безпеки і оборони України від 10.07.17 “Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року” “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” [3] кібербезпеку ОКІІ визначено як пріоритетний напрямком наукових досліджень. Як не парадоксально, але на разі відсутнє нормативно-правове врегулювання питання щодо типового опису структури системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури (ОКІІ) та функцій, які вона має виконувати. Відсутність зазначених елементів призводить до унеможливлення проведення процедури з оцінювання ефективності функціонування зазначеної системи.

Таким чином, існує наукове завдання з обґрунтування ключових функцій системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури.

Аналіз останніх досліджень і публікацій. Проаналізуємо роботи, у яких започатковано розв'язання даної проблеми.

В авторській колективній роботі [4] запропоновано концептуальний підхід до побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України. Він ґрунтується на принципах масштабування та доповнення. Слід зазначити, що в фокус об’єкту дослідження не потрапив перелік функцій, які має виконувати зазначена система.

Подальший аналіз за ключовою зв’язкою зі слів «функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури» не дав позитивного результату пошуку. Однак пошук можливих підходів до оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України [5] підтвердив припущення про доцільність використання ризико-орієнтованого та імовірнісного підходів. На їх підставах запропонована методика обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки [6], яка ґрунтується на множині індикаторів стану кіберзахищеності. За ключовий індикатор обрано розрахунок кіберзахищеності за результатом внутрішнього (пасивного) аудиту у відповідності до поданої методики [7].

Поштовхом до вибору найбільш релевантних функцій послужили затверджені Державною службою спеціального зв’язку та захисту інформації України Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (ОКІІ) [8]. Як зазначається у тесті документа рекомендації об’єднують найкращі світові практики та чинну нормативну базу для відповідних об’єктів: атомних станцій, комунальних господарств, підприємств енергетичного сектору, банків та багатьох інших.

Виходячи з цих обставин пошук підходів до оцінювання ефективності функціонування системи захисту інформації і кібербезпеки є наразі актуальним, однак першочерговою задачею є обрання типових функцій, які має виконувати система захисту інформації і кібербезпеки критичної інформаційної інфраструктури.

Зазначені дослідження внесуть істотний вклад в розвиток і зміцнення воєнної безпеки кіберпростору України [9].

Мета статті. Метою статті є пропозиції щодо вибору функції, які має виконувати система захисту інформації і кібербезпеки критичної інформаційної інфраструктури, за результатами аналізу яких вдасться оцінити ефективність функціонування цієї системи.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Діяльність СЗІКБ із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки (рис. 1):

- ідентифікація ризиків;
- кіберзахист;
- виявлення кіберінцидентів;
- реагування;
- відновлення поточного стану кібербезпеки.

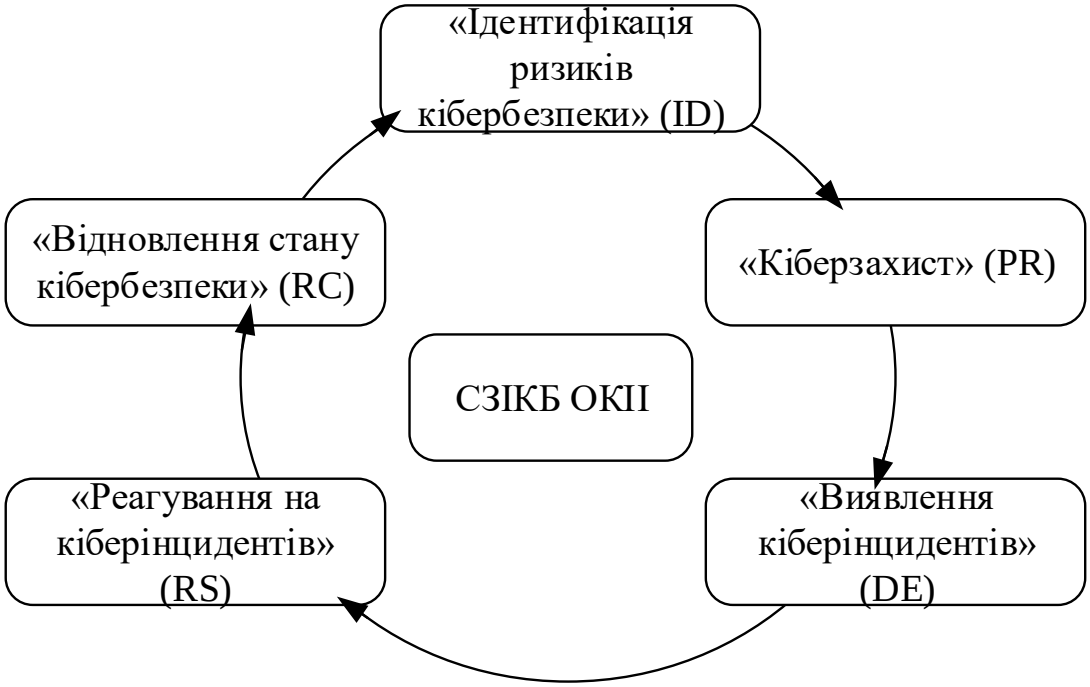

Рис. 1. Функціональний цикл управління кібербезпекою ОКІІ

Слід зазначити, що при розробці зазначеної структури враховувалися передовий досвід та рекомендацій [10 – 20].

Функції кібербезпеки забезпечують:

- прийняття рішення з управління ризиками кібербезпеки на ОКІІ;
- вибір та впровадження заходів кіберзахисту;
- реагування на загрози кібербезпеки;
- удосконалення кіберзахисту, враховуючи набутий досвід.

Функції кібербезпеки узгоджені з чинними підходами щодо управління ризиками кібербезпеки та допомагають продемонструвати ефективність інвестицій в кібербезпеку. Наприклад, планування забезпечення кібербезпеки і тренування персоналу покращують

своєчасне реагування на кіберінциденти та відновлення функціонування ОКІІ, в результаті чого знижується негативний вплив кіберінцидентів на своєчасність, безперервність надання життєво важливих послуг та функцій.

Функція «Ідентифікація ризиків кібербезпеки» (ID) системи СЗІКБ ОКІІ має реалізовувати передбачені заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ОКІІ щодо наявних ризиків, способів управління ризиками кібербезпеки для інформаційних систем, активів, даних, що використовуються для надання життєво важливих послуг та функцій. Реалізація заходів кіберзахисту класу «Ідентифікація ризиків» є чинником для ефективного використання Рекомендацій, розуміння умов, ресурсів, що підтримують надання життєво важливих послуг та функцій, а також пов'язаних ризиків кібербезпеки, обґрунтованого вибору конкретних заходів для впровадження. Це дозволяє визначити пріоритетність ризиків кібербезпеки потребами надання життєво важливих послуг та функцій, а також розподіляти ресурси і зусилля відповідно до встановлених пріоритетів.

Функція «Кіберзахист» (PR) системи СЗІКБ ОКІІ має реалізовувати визначену діяльність із розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєво важливих послуг та функцій ОКІ. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів.

Функція «Виявлення кіберінцидентів» (DE) системи СЗІКБ ОКІІ має реалізовувати передбачені заходи своєчасного виявлення кіберінцидентів.

Функція «Реагування на кіберінцидентів» (RS) системи СЗІКБ ОКІІ має реалізовувати передбачені заходи реагування на кіберінциденти та кібератаки. Реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту (кібератаки) на надання життєво важливих послуг та функцій.

Функція «Відновлення стану кібербезпеки» (RC) системи СЗІКБ ОКІІ має реалізовувати визначену діяльність щодо забезпечення спроможностей ОКІІ щодо стійкого, надійного та безперервного надання життєво важливих послуг та функцій, які були порушені внаслідок кіберінциденту (кібератаки). Ці заходи забезпечують своєчасне відновлення штатної роботи ОКІІ та зменшення негативного впливу кіберінциденту (кібератаки).

Обговорення результатів. Перелічені універсальні функції, які має виконувати СЗІКБ ОКІІ обрані відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» [1] та Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року №518 [21].

Обрані цільові функції пропонується застосовувати як показники при оцінюванні ефективності функціонування СЗІКБ ОКІІ. Ефективність системи захисту інформації і кібербезпеки ($E_{СЗІКБ}$) – ступінь відповідності досягнутих результатів поставленим цілям щодо захисту інформації. Показник ефективності – це величина, що характеризує ступінь досягнення системою будь-якої з поставлених перед нею завдань.

Відповідно до означень визначимо наступні показники ефективності ($E_{П(СЗІКБ)}$), як числові величини, що характеризуватимуть ступінь досягнення системою захисту інформації і кібербезпеки ОКІІ поставлених перед нею завдань. Для оцінки показників $E_{П(СЗІКБ)}$ рекомендуємо застосовувати наступні критерії табл. 1.

Таблиця 1.

Критерії оцінювання показників $E_{П(СЗІКБ)}$

Критерій $E_{П(СЗІКБ)}$	Рівень
$0 \le E_{П(СЗІКБ)} \le 0{,}25$	незадовільний (НЗ)
$0{,}25 < E_{П(СЗІКБ)} \le 0{,}5$	низький (Н)
$0{,}5 < E_{П(СЗІКБ)} \le 0{,}75$	середній (С)
$0{,}75 < E_{П(СЗІКБ)} \le 0{,}9$	високий (В)
$0{,}9 < E_{П(СЗІКБ)} \le 1$	найвищий (НВ)

Тоді узагальнений показник ефективності функціонування системи захисту інформації і кібербезпеки в ОКІІ пропонується обчислювати за формулою (1):

$$E_{СЗІКБ} = (k_1 \times E_{П(СЗІКБ)1}) + (k_2 \times E_{П(СЗІКБ)2}) + (k_3 \times E_{П(СЗІКБ)3}) + \\ + (k_4 \times E_{П(СЗІКБ)4}) + (k_5 \times E_{П(СЗІКБ)5}) \quad (1)$$

де $E_{(СЗІКБ)}$ – узагальнений показник ефективності функціонування системи захисту інформації і кібербезпеки в ОКІІ;

$E_{П(СЗІКБ)}$ – значення ефективності функціонування системи захисту інформації і кібербезпеки в ОКІІ за окремим показником;

$k_1 \dots k_5$ – вагові коефіцієнти, що враховують важливість показників ефективності функціонування системи захисту інформації і кібербезпеки в ОКІІ. Сума вагових коефіцієнтів дорівнює одиниці ($k_1 + k_2 + k_3 + k_4 + k_5 = 1$).

Критерії оцінювання ефективності функціонування СЗІКБ ОКІІ за узагальненим показником подані в (табл. 2).

Таблиця 2.

Критерії оцінки ефективності функціонування СЗІКБ ОКІІ за узагальненим показником

Критерій $E_{П(СЗІКБ)}$	Рівень
$0 \le E_{СЗІКБ} \le 0{,}25$	Частковий
$0{,}25 < E_{СЗІКБ} \le 0{,}5$	Ризикорієнтований
$0{,}5 < E_{СЗІКБ} \le 0{,}75$	Повторюваний
$0{,}75 < E_{СЗІКБ} \le 1$	Адаптивний

Лінгвістичний опис часткового рівня.

Практика кіберзахисту. Практична діяльність із реалізації заходів кіберзахисту та управління ризиками кібербезпеки не є формалізованою. Діяльність з впровадження заходів кіберзахисту та управління ризиками носить довільний та ситуативний характер. Пріоритетність виконання заходів кіберзахисту безпосередньо не враховує цілі ОКІІ щодо управління ризиками, характеристики загроз, завдання щодо надання життєво важливих послуг та функцій.

Політика управління ризиками. Обмежене розуміння ризику кібербезпеки на організаційному рівні. Інформованість керівництва та персоналу організації про ризики кібербезпеки є недостатньою. Загальний підхід до управління ризиками кібербезпеки в масштабі всього ОКІІ не встановлено. Заходи кіберзахисту впроваджуються нерегулярно, ситуативно, використовуючи різноманітний практичний досвід або інформацію, отриману із зовнішніх джерел. Процесів, що забезпечують внутрішній обмін інформацією про стан кібербезпеки, не зафіксовано.

Взаємодія з іншими ОКІ. Організація не розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів. Організація не опрацьовує або отримує інформацію (дослідження загроз, кращі практики, технології) від інших організацій (споживачі, постачальники, залежні від неї або від яких вона залежить організацій, організацій аналізу та поширення інформації, дослідники, державні органи) та не поширює таку інформацію. Організація взагалі не усвідомлює ризиків кібербезпеки, пов'язаних з послугами, які вона надає та якими користується.

Лінгвістичний опис ризикорієнтованого рівня.

Практика кіберзахисту. Практика реалізації заходів кіберзахисту та управління ризиками затверджується керівництвом організації, але може не встановлюватися, як загальна політика для організації. Пріоритетність діяльності з кібербезпеки та потреби захисту безпосередньо залежать від цілей організаційного ризику, середовища загроз або вимог щодо надання життєво важливих послуг та функцій.

Політика управління ризиками. Існує усвідомлення ризику кібербезпеки на організаційному рівні, але загальний підхід організації до управління ризиком кібербезпеки не встановлено. Інформація про кібербезпеку поширюється в межах організації на неофіційній основі. Розгляд кібербезпеки в цілях та програмах організації може відбуватися на деяких, але не на всіх рівнях організації. Оцінка ризиків кібербезпеки для організаційних та зовнішніх активів відбувається, але зазвичай не повторюється або однаково не проводиться.

Взаємодія з іншими ОКІ. Загалом організація розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів, але не їх обох. Організація опрацьовує та отримує деяку інформацію від інших організацій, створює на підставі неї власну інформацію, але може не поширювати таку інформацію між іншими організаціями. Крім того, організація усвідомлює ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується, але не діє послідовно або за затвердженими правилами.

Лінгвістичний опис повторювального рівня.

Практика кіберзахисту. Практика реалізації заходів кіберзахисту та управління ризиками в організації є офіційно затвердженою і визначена як політика. Результати кіберзахисту регулярно відстежуються та заходи кіберзахисту регулярно оновлюються на основі застосування процесів управління ризиками до змін у вимогах щодо надання життєвоважливої функції, мінливих загроз та технологічного ландшафту.

Політика управління ризиками. В організації існує загальний підхід до управління ризиками кібербезпеки. Політики інформування про ризики, процеси та процедури визначені, реалізуються за призначенням та переглядаються. Існують послідовні методи ефективного реагування на зміни ризику. Персонал володіє знаннями та вміннями виконувати призначені їм обов'язки. Організація послідовно і точно контролює ризик кібербезпеки для активів організації. Пов'язані та не пов'язані з кібербезпекою головні виконавці регулярно спілкуються щодо ризику кібербезпеки.

Взаємодія з іншими ОКІ. Організація розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів та може сприяти ширшому розумінню спільнотою ризиків. Організація регулярно опрацьовує та отримує інформацію від інших організацій, що доповнює власну створену інформацію та поширює її між іншими організаціями. Організація усвідомлює ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується.

Лінгвістичний опис адаптивного рівня.

Практика кіберзахисту. Організація адаптує свою практику в галузі кібербезпеки

на основі попередніх та поточних заходів з кібербезпеки, включаючи отримані результати та прогнозні показники. Завдяки процесу безперервного вдосконалення, що передбачає передові технології та практики кібербезпеки, організація активно адаптується до мінливих кіберзагроз та своєчасно й ефективно реагує на кіберзагрози, що розвиваються та ускладняються.

Політика управління ризиками. В організації існує загальний підхід до управління ризиком кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних кіберінцидентів. Взаємозв'язок між ризиком кібербезпеки та цілями організації чітко усвідомлюється та враховується під час прийняття рішень. Головні виконавці контролюють ризик кібербезпеки в тому самому контексті, що і фінансовий ризик та інші ризики для організації. Управління ризиками кібербезпеки є частиною організаційної культури і розвивається на основі усвідомлення попередньої діяльності та постійного усвідомлення діяльності у своїх системах та телекомунікаційних мережах. Організація може швидко та ефективно враховувати зміни у тому, як підходити до опрацювання та повідомляти про ризик.

Взаємодія з іншими ОКІ. Організація розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів, сприяє ширшому розумінню спільнотою ризиків. Організація отримує, генерує та переглядає пріоритетну інформацію для продовження аналізу цих ризиків по мірі розвитку ландшафту загроз та технологій. Організація поширює цю інформацією як в середині організації, так і назовні для подальшого опрацювання. Організація використовує інформацію в режимі реального часу або майже в режимі реального часу і послідовно реагує на ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи результати дослідження викладеного в основній частині, що для реалізації процедури оцінювання ефективності функціонування СЗІКБ ОКІІ необхідні часткові показники ефективності, тобто величини за допомогою, яких можна охарактеризувати ступінь досягнення системою будь-якого з поставлених перед нею завдань. Оскільки вимоги до показника ефективності: мати певний фізичний зміст; бути придатним для кількісного аналізу; мати просту і зручну форму; відображати одну із значущих сторін функціонування системи; забезпечувати необхідну чутливість. Поодинокі (часткові) показники ефективності, відображають якусь із значущих сторін функціонування системи (ймовірність виявлення порушника або ймовірність його нейтралізації силами охорони і т.п.). Виходячи з цього пропонуються наступні показники ефективності ($E_{П(СЗІКБ)}$): ID Ідентифікація ризиків кібербезпеки; PR Кіберзахист; DE Виявлення кіберінцидентів; RS Реагування на кіберінциденти; RC Відновлення стану кібербезпеки.

Наукова новизна одержаного результату полягає в тому, що запропоновано універсальні функції, які має реалізовувати система захисту інформації і кібербезпеки на об'єктах критичної інформаційної інфраструктурі.

Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування показників та критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

2 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Указ Президента України № 96/2016 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/96/2016#Text.

3 Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32, Рішення Ради національної безпеки і оборони України (2017) (Україна). https://zakon.rada.gov.ua/laws/show/n0006525-17#Text.

4 Козубцов, І.М., Куцаєв, В.В., Ткач, В.О., Козубцова, Л.М. (2015). Концептуальний підхід до побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України на принципах масштабування та доповнення. *Сучасні інформаційні технології у сфері безпеки та оборони*, *3*(24), 47-55.

5 Козубцов, І. М., Нещерет, І. Г., Терещенко, Т. П. (2021). Пошук підходів до оцінювання ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України. У *І Міжнародна науково-технічна конференція "Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку"* (с. 159). ВІТІ.

6 Козубцова, Л.М., Рудоміно-Дусятська, І.А., Сновида, В.Є. (2021). Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво,* (45), 19-25.

7 Zabara, S., Kozubtsova, L. Kozubtsov, I. (2020). Improved method of diagnostics of cyber security of the information system taking into account disruptive cyber impacts. «Danish Scientific Journal» (DSJ). *Kobenhavn. Denmark, 35*(1), 68-74.

8 Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року №601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури». https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.

9 Живило, Є.О., Черноног, О.О., Машталір, В.В. (2016). Стратегія воєнної безпеки кіберпростору України. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації*, (1), 41-52.

10 Department of Energy. (2021). Cybersecurity Capability Maturity Model. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

11 Center for Internet Security. (2021). CIS Controls V8. https://www.cisecurity.org/controls.

12 Information Systems Audit and Control Association (ISACA) (2021). Control Objectives for Information and Related Technologies. https://www.isaca.org/resources/cobit.

13 International Energy Agency. (2021). Enhancing Cyber Resilience in Electricity Systems. https://webstore.iea.org/download/direct/4359.

14 International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu.

15 International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). https://www.iso.org/standard/54534.html.

16 National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. https://doi.org/10.18434/mds2-2348.

17 North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

18 National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018.

19 National Institute of Standards and Technology (2021) National Online Informative References Program. https://csrc.nist.gov/projects/olir.

20 Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST

Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4.

21 Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 518 (2019) (Україна). https://zakon.rada.gov.ua/laws/show/518-2019-п#Text.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Yuri I. Khlaponin
Doctor of Technical Sciences, Professor , head of the Department of cybersecurity and computer engineering
Kiev National University of Civil Engineering and Architecture, Kiev, Ukraine
ORCID ID 0000-0002-9287-0817
y.khlaponin@gmail.com

Lesya M. Kozubtsova
Candidate of Technical Sciences, Associate professor of the Department of mathematics and physics
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID 0000-0002-7866-8575
l.kozubtsova@i.ua

Igor M. Kozubtsov
Doctor of Pedagogical Sciences, candidate of technical sciences, senior researcher, leading researcher of the research department
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Roman M. Shtonda
Head of the research department
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0001-5986-0847
shtonda1982@ukr.net

FUNCTIONS OF THE INFORMATION SECURITY AND CYBERSECURITY SYSTEM OF CRITICAL INFORMATION INFRASTRUCTURE

Abstract. The subject of research in the scientific article is the system of Information Protection and cybersecurity of critical information infrastructure objects. An information security and cybersecurity system is a complex set of software, cryptographic, organizational, and other tools, methods, and measures designed to protect information and cybersecurity. Since the system of Information Protection and cybersecurity of critical information infrastructure facilities is relatively new, there is no single view on what functions this system should perform. As a result, the process of its formation and formation as a system continues. There was a need to define functions for further evaluation of the effectiveness of its functioning as a system. Evaluation is supposed to be carried out both in the process of creation, acceptance, and daily operation. Partial performance indicators are required to implement the procedure for evaluating the effectiveness of the information security system and cybersecurity of critical information infrastructure facilities. Using these indicators, it is possible to characterize the degree of achievement of the system's tasks assigned to it. The following performance indicators are proposed according to the functions: ID identification of cybersecurity risks; PR Cyber Defense; DE detection of cyber incidents; RS response to cyber incidents; RC restoration of the state of cybersecurity. The scientific novelty of the obtained result lies in the fact that Universal functions are proposed that the information security and cybersecurity system should implement at critical information infrastructure facilities. The presented study does not exhaust all aspects of this problem. The theoretical results obtained in the course of scientific research form the basis for further justification of indicators and criteria for evaluating the effectiveness of the information security and cybersecurity system.

Keywords: function; system; information protection; cybersecurity; critical information infrastructure object

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy № 2163-VIII (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu

kiberbezpeky Ukrainy", Ukaz Prezydenta Ukrainy № 96/2016 (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/96/2016#Text.
3. Pro stan vykonannia rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii», vvedenoho v diiu Ukazom Prezydenta Ukrainy vid 13 liutoho 2017 roku № 32, Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2017) (Ukraina). https://zakon.rada.gov.ua/laws/show/n0006525-17#Text.
4. Kozubtsov, I.M., Kutsaiev, V.V., Tkach, V.O., Kozubtsova, L.M. (2015). Kontseptualnyi pidkhid do pobudovy systemy kibernetychnoi bezpeky statsionarnykh informatsiino-telekomunikatsiinykh vuzliv Ukrainy na pryntsypakh masshtabuvannia ta dopovnennia. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 3(24), 47-55.
5. Kozubtsov, I. M., Neshcheret, I. H., Tereshchenko, T. P. (2021). Poshuk pidkhodiv do otsiniuvannia efektyvnosti funktsionuvannia systemy zakhystu informatsii i kiberbezpeky v informatsiino-telekomunikatsiinykh systemakh Zbroinykh Syl Ukrainy. U I Mizhnarodna naukovo-tekhnichna konferentsiia “Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky: aktualni pytannia i tendentsii rozvytku” (s. 159). VITI.
6. Kozubtsova, L.M., Rudomino-Dusiatska, I.A., Snovyda, V.Ie. (2021). Obchyslennia pokaznykiv efektyvnosti funktsionuvannia systemy zakhystu informatsii i kiberbezpeky. Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo, (45), 19-25.Zabara, S., Kozubtsova, L. Kozubtsov, I. (2020). Improved method of diagnostics of cyber security of the information system taking into account disruptive cyber impacts. «Danish Scientific Journal» (DSJ). *Kobenhavn. Denmark*, *35*(1), 68-74.
7. Nakaz Administratsii Derzhspetszviazku vid 06 zhovtnia 2021 roku №601 «Pro zatverdzhennia Metodychnykh rekomendatsii shchodo pidvyshchennia rivnia kiberzakhystu krytychnoi informatsiinoi infrastruktury». https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.
8. Zhyvylo, Ye.O., Chernonoh, O.O., Mashtalir, V.V. (2016). Stratehiia voiennoi bezpeky kiberprostoru Ukrainy. Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii, (1), 41-52.
9. Department of Energy. (2021). Cybersecurity Capability Maturity Model. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
10. Center for Internet Security. (2021). CIS Controls V8. https://www.cisecurity.org/controls.
11. Information Systems Audit and Control Association (ISACA) (2021). Control Objectives for Information and Related Technologies. https://www.isaca.org/resources/cobit.
12. International Energy Agency. (2021). Enhancing Cyber Resilience in Electricity Systems. https://webstore.iea.org/download/direct/4359.
13. International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu.
14. International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). https://www.iso.org/standard/54534.html.
15. National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. https://doi.org/10.18434/mds2-2348.
16. North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
17. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018.
18. National Institute of Standards and Technology (2021) National Online Informative References Program. https://csrc.nist.gov/projects/olir.
19. Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4.
20. Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury, Postanova Kabinetu Ministriv Ukrainy № 518 (2019) (Ukraina). https://zakon.rada.gov.ua/laws/show/518-2019-p#Text.