КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1200
УДК 004(056.53::413.4)

Цуркан Василь Васильович
кандидат технічних наук, доцент, доцент; старший науковий співробітник
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України,
Київ, Україна
ORCID: 0000-0003-1352-042X
v.v.tsurkan@gmail.com

Ракович Владислав Сергійович
аспірант
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України,
Київ, Україна
ORCID: 0009-0008-4733-9120
covlad@ukr.net

МЕХАНІЗМ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Досліджено важливість об'єктів критичної інфраструктури для економіки, національної безпеки та оборони. Це пов'язано з наданнями ними життєво важливих функцій та/або послуг організаціям як державної, так і приватної форм власності. Унеможливлення їх порушування досягається упроваджуванням заходів і засобів обробляння, контролювання, переглядання ризиків безпеки. Крім того або ліквідуванням, або зменшуванням наслідків, або відновлюванням після реалізування загроз. Водночас адаптуванням до емерджентних ризиків безпеки. Це реалізується шляхом розробляння операторами критичної інфраструктури відповідних систем, зокрема, забезпечування кібербезпеки. Тому запобігання проявам негативних впливів і наслідків реалізується управлінням ризиками. Зокрема операторами критичної інфраструктури забезпечується реагування на інциденти з урахуванням національного плану. Цим обумовлено необхідність упроваджування механізму повідомляння про події кібербезпеки об'єктів критичної інфраструктури. За результатами аналізування останніх досліджень і публікацій встановлено їх направленість здебільшого на процеси виявляння і реагування на інциденти. З огляду на це, механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури визначено сукупністю процесів у межах структурованого представлення управління інцидентами. Для цього враховано зв'язки між їхніми складниками, зокрема, діяльністю, інформаційним активом, уразливістю, загрозою. Серед фаз основну увагу зосереджено на плануванні та готуванні, виявлянні й звітуванні, оцінюванні та вирішуванні. Кожною з них визначаються процеси від отримання відомостей про подію до прийняття рішення про належність її до одного з класів – інцидент/не інцидент. Ними в сукупності визначається механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури. Для цього використано настанови гармонізованих в Україні міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27035-1, 2, 3. Окрему увагу приділено засвоюванню уроків після звітування як про подію, так і про інцидент кібербезпеки. В такий спосіб можливо підтримувати актуальними процеси, шаблони повідомлень і звітів про них.

Ключові слова: об'єкт критичної інфраструктури, подія кібербезпеки; інцидент кібербезпеки; механізм повідомляння; повідомляння про подію кібербезпеки; звіт про подію кібербезпеки.

ВСТУП

Об'єкти критичної інфраструктури визначається з огляду на важливість для економіки, національної безпеки та оборони. Оскільки порушування їхнього функціонування може призвести до завдання шкоди життєво важливим національним інтересам. Запобігання цьому досягається забезпечуванням функційності,

безперервності роботи, відновлюваності та стійкості об’єктів критичної інфраструктури [1]. Завдяки такій діяльності унеможливлюються відмовляння, переривання, порушування надання життєво важливих функцій та/або послуг організаціями як державної, так і приватної форм власності [1], [2]. Для цього, по-перше, передбачається створювання умов та впроваджування заходів обробляння, контролювання, переглядання ризиків безпеки. По-друге, або ліквідування, або зменшування наслідків, або відновлювання після реалізування загроз. І, як наслідок, по-третє, адаптування до емерджентних ризиків [1], [3], [4]. Тому безпека зазначених об’єктів визначається станом, при якому надаються життєво важливі функції та/або послуги з прийнятним рівнем ризиків – від урядування та надання найважливіших публічних (адміністративних) послуг до дослідницької діяльності [1]. Ефективність виконання даного завдання забезпечується виокремлюванням секторів і загалом покладається на національну систему захисту критичної інфраструктури. Насамперед на об’єктовому рівні її управління операторами створюються, налагоджуються і підтримуються системи фізичної безпеки, безпеки операційних систем і, зокрема, кібербезпеки [1]. Серед невідкладних дій у межах функціонування таких систем виділяється реагування і невідкладне інформування відповідальних суб’єктів національної системи захисту критичної інфраструктури про інциденти кібербезпеки [1], [5].

Постановка проблеми. Інцидент кібербезпеки визначається подією як навмисного, так і ненавмисного характерів. Призводить до порушування безпеки системи електронних комунікацій, системи управління технологічними процесами та об’єкта критичної інфраструктури загалом [1], [5]. Це проявляється у впливанні на штатний режим функціонування кожного з них. Для запобігання проявам негативним впливів і наслідкам оператори критичної інфраструктури управляють ризиками кібербезпеки. Водночас вони забезпечують реагування на інциденти з урахуванням відповідного національного плану [5-7]. Виконання цих завдань покладається на призначену відповідальну особу або створений підрозділ. Ними управляється, координується і контролюється реалізування вимог до кібербезпеки об’єкта критичної інфраструктури. З огляду на це, посадові особи операторів критичної інфраструктури зобов’язані повідомляти в установленому порядку про інциденти кібербезпеки. Так обґрунтовується необхідність упроваджування механізму своєчасного повідомляння працівниками або відповідальної особи, або підрозділу кіберзахисту про події кібербезпеки встановленими каналами. Наприклад, телефоном, електронною поштою, месенджером. На основі отриманих відомостей приймається рішення про інформування секторального органу [8-10]. Зокрема у випадку виникання кризової ситуації на об’єкті критичної інфраструктури це організовується упродовж 30 хв від отримання повідомлення. Такими відомостями обумовлюється діяльність виявляння і реагування на інциденти кібербезпеки. Тому працівники повинні бути обізнані що, протягом якого проміжку часу та кому доводити до відома. Особливо це важливо на тлі постійного зростання кількості інцидентів [11]. Отже, визначання механізму повідомляння про події кібербезпеки об’єктів критичної інфраструктури є актуальним завданням.

Аналіз останніх досліджень і публікацій. Питання управління інцидентами кібербезпеки порушувалися в [12-21]. Проблему підвищування ефективності поводження з інцидентами інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах розглянуто в [12]. Як визначальний фактор їхнього розвитку виокремлено наявність захищеної системи обміну інформацією. Для інтелектуального управління інцидентами інформаційної безпеки запропоновано

імунний підхід. Показано практичну значимість отриманих результатів на прикладі прототипу структури та функцій імунної системи. Цим досягнуто адаптивність управління новими інцидентами інформаційної безпеки. Обмеженість типового підходу до повідомляння про інциденти через телефон досліджено в [13]. Зокрема основу увагу зосереджено на вірогідних часових затримках при доведенні до відома пов'язаної з ними інформації. Тож для раннього виявляння інцидентів розглянуто можливості та обмеження краудсорсингових платформ. Серед обмежень виокремлено наявність шуму та невизначеність отриманих даних. Їх подолання досягнуто завдяки кількісному визначанні зв'язку між показниками ефективності класифікування інцидентів і встановленими вимогами фахівцями з моделювання. Основні завдання команд реагування на інциденти комп'ютерної безпеки проаналізовано в [14]. Акцентовано на їх виконанні як у межах країни, так і завдяки міжнародній співпраці поза її межами. Серед основних завдань команди реагування на інциденти комп'ютерної безпеки виокремлено розпізнавання, запобігання, фіксування і обробляння відповідних подій. До того ж активне реагування у випадках існування прямих загроз. І, окрім співпраці з іншими командами розглянуто участь у національних та міжнародних проєктах за напрямом кібербезпеки. Існування таких можливостей досліджено на прикладі Польщі. Систему кібербезпеки об'єктів критичної інформаційної інфраструктури проаналізовано в [15]. Її визначено як складний комплекс програмних, криптографічних, організаційних заходів і засобів. При цьому порушено питання стосовно формування єдиного погляду на функції таких систем. Тож для встановлювання ступеня виконання покладних на неї завдань запропоновано використання показників ефективності. Загалом це дозволило визначити універсальні функції системи кібербезпеки, наприклад, виявляння інцидентів. Обробляння подій та інцидентів інформаційної безпеки проаналізовано в [16]. У межах даного процесу на команду реагування покладається їх класифікування, описання. Окрім того окрему увагу приділено представлянню потенційних інцидентів за результатами оцінювання ризиків інформаційної безпеки. Для цього визначено відповідні ознаки та наведено схему реєстрування. До того ж досліджено основні фактори та джерела порушень інформаційної безпеки. Завдання кіберзахисту об'єктів критичної інформаційної інфраструктури проаналізовано в [17]. За результатами аналізу відомих заходів запропоновано використання інтелектуальних можливостей SIEM-системи. Це представлено як перспективний напрям забезпечування кіберзахисту баз даних. Отриманим результатом враховано різні рівні контуру захищання інформаційно-комунікаційної системи. Відповідно до такого підходу досягається ефективне виявлення і реагування на інциденти кібербезпеки баз даних інформаційної системи. Актуальність питань асоційованих з інцидентами безпеки підкреслено в [18]. Насамперед це пов'язано з великим попитом використання цифрових технологій в усіх сферах повсякденної діяльності людини. Виокремлено серйозність наслідків настання інцидентів безпеки. З огляду на це, запропоновано фреймворк їхнього описання. Підґрунтям такого рішення стало аналізування повідомлень, кібератак. Як наслідок, запропоновано правила виявляння і структурованого описання інцидентів. Методи оцінювання ризиків кібербезпеки стосовно застосовності до захисту національної критичної інфраструктури проаналізовано в [19]. Встановлено їхню придатність для реагування на актуальні інциденти кібербезпеки. Окрім теоретичного, виокремлено й практичний аспект дослідження отриманих результатів за допомогою реальних систем критичної інфраструктури. Для покращування інтегрування і впроваджування заходів кібербезпеки запропоновано нові підходи та моделі. Цим враховано комплексний

характер загроз кібербезпеці. Теоретичне оцінювання звітності про інциденти кібербезпеки запропоновано в [20]. При цьому враховано її дуальність з огляду як на виявляння і реагування, так і засвоювання отриманих уроків. Серед типових проблем виокремлено небажання працівників повідомляти про інциденти кібербезпеки. До того ж існування недостатнього взаємозв'язку між звітністю і підвищенням обізнаності. Це спонукало до оптимізування зазначеної діяльності в межах організацій. Насамперед поєднання і поверхневого, і детального звітування про інциденти кібербезпеки, а також поширення інформації про отримані уроки за результатами реагування на них. Невизначеність розвивання інцидентів кібербезпеки, множинність можливих варіантів реагування та обмеженість ресурсів показано в [21]. Їх урахування досягнуто запропонованим методом прийняття рішень. За його основу взято системний підхід і формалізування процесу реагування. Отриманий результат орієнтований на обирання оптимального рішення за критерієм максимізування очікуваного ефекту. Крім цього, можливе оцінювання ефективності реалізованих заходів забезпечування кібербезпеки. Запропонований метод рекомендовано застосовувати в центрах оперативного реагування.

Отже, на основі аналізу останніх досліджень і публікацій встановлено їх направленість здебільшого на процеси виявляння і реагування на інциденти кібербезпеки. Тоді як повідомлянню працівниками про відповідні події в організаціях, зокрема, об'єктах критичної інфраструктури, попри його актуальність і важливість приділено недостатньо уваги.

Метою статті є встановлювання особливостей повідомляння працівниками об'єктів критичної інфраструктури відповідальній особі або підрозділу кіберзахисту про події кібербезпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Характерною особливістю упровадження заходів забезпечування кібербезпеки в організаціях як приватного, так і державного секторів є запобігання порушенням властивостей інформації з прийнятним ризиком [3], [22], [23]. Попри таку діяльність, і в активах, і в заходах можуть залишатися уразливості, які в майбутньому вірогідно призводитимуть до інцидентів кібербезпеки. До того ж цьому сприяють змінення обставин діяльності організацій, а також виникання емерджентних загроз [4]. Тому однією з передумов ефективності впроваджених заходів є готовність організацій, зокрема, й об'єктів критичної інфраструктури до реагування на інциденти кібербезпеки. За даних обставин їм рекомендується розробити та впровадити механізм повідомляння працівниками про події кібербезпеки встановленими каналами [22-24].

Під подією кібербезпеки розуміється подія, що вказує на можливі або порушення властивостей інформації, або збій відповідних заходів і засобів. Серед причин її виникання виокремлюються [3], [24]:

- наявність уразливостей (технічних, технологічних, організаційних, фізичних);
- наявність людських помилок (внутрішніх, зовнішніх зацікавлених сторін);
- недостатність оцінювання ризиків кібербезпеки;
- недостатність обробляння ризиків кібербезпеки;
- зміненість обставин діяльності організацій.

З огляду на виокремлені причини події кібербезпеки можуть вказувати на порушення, наприклад [24], шкідливим програмним забезпеченням (навмисні), унаслідок ненавмисної помилки працівника (випадкові), унаслідок пожежі, повені (екологічні),

комп'ютерними вірусами (технічні), унаслідок крадіжки паперового носія (нетехнічні). Виникання кожної з них не є ознакою успішності реалізування загроз і, як наслідок впливання на збереженість властивостей інформації. Тож відповідно до [24] подія є одним із визначальних об'єктів інциденту кібербезпеки. З огляду на рис. 1, діяльність об'єкта критичної інфраструктури обумовлюється інформаційним активами. Їм притаманні вразливості, кожна з яких наражає на порушення безпеки. Загроза використовує уразливість інформаційного активу та може призводити до погіршення (втрати) насамперед конфіденційності, цілісності та доступності. Обидві спричиняють виникання події кібербезпеки, яка у випадку класифікування її як інциденту впливає на інформаційний актив і, як наслідок, порушує діяльність об'єкта критичної інфраструктури.

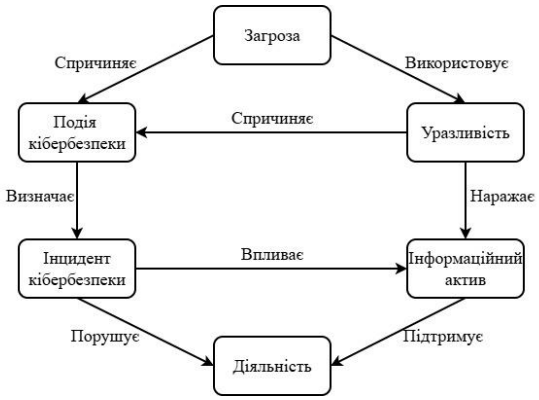

Рис. 1. Дескриптивне представлення зв'язків між об'єктами інциденту кібербезпеки [24]

Події отримуються від або зацікавлених сторін, або засобів забезпечування кібербезпеки, або зовнішніх джерел інформації (табл. 1). Вони виявляються різними способами та класифікуються на такі три категорії:

1. Технічні [25], [26]:
– засоби виявляння і запобігання вторгненням, наприклад: Snort, Suricata;
– засоби захищання кінцевих точок, наприклад: Crowdstrike Falcon, FortiClient;
– засоби аналізування журналів безпеки, наприклад: Splunk, Wazuh;
2. Людські [22], [25], [26]:
– внутрішні зацікавлені сторони;
– зовнішні зацікавлені сторони.
3. Організаційні [25], [26]:
– відділ інформаційних технологій, центр операцій безпеки, центр мережевих операцій, служба технічної підтримки;
– постачальники послуг, наприклад: Інтернет провайдери, постачальники телекомунікаційних послуг;
– медіа, наприклад: газети, телебачення, вебсайти, соціальні мережі.

Таблиця 1

Приклад фундаментальних критеріїв події кібербезпеки [26]

Категорія	Критерії
Важливість інформації	Низька, середня, важлива, дуже важлива
Впливовість події	Низька, середня, значна, дуже значна
Шкала пошкодження	Низькі, середні, значні, дуже значні

Відомості про подію кібербезпеки визначається з огляду на те коли, що, як і чому сталося подія, контактну інформацію інформатора [25]. Вони подаються за формою такої рекомендованої структури:

Основні відомості [25]:

- дата події;
- номер події;
- номери пов'язаних подій (за потреби).

Відомості про інформатора (працівник/джерело, рис. 2) [25]:

- ім'я, прізвище;
- контакти (адреса, організація, відділ, телефон, електронна адреса).

Опис події [25]:

- що сталося;
- як це сталося;
- чому це сталося;
- вірогідні враження інформаційних активів;
- негативний вплив на діяльність об'єкта критичної інфраструктури;
- виявлені вразливості інформаційних активів/заходів, засобів.

Відомості про подію [25]:

- дата та час події;
- дата та час виявлення події;
- дата та час повідомлення про подію.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Відповідно до [22-24] зменшування прямих та/або непрямих наслідків настання інцидентів кібербезпеки реалізується униканням або стримуванням впливу кожного з них на діяльності об'єктів критичної інфраструктури. Це пов'язується з порушеннями властивостей насамперед конфіденційності, цілісності та доступності інформаційних активів.

Запобігання цьому досягається встановлюванням цілей управління інцидентами кібербезпеки та визначанням для їх досягання окремих фаз зазначеного процесу. Кожну з них можна отримати для об'єкта критичної інфраструктури використанням як основи настанов ISO/IEC 27035-1. Тож отримаємо такий перелік [24]:

- події кібербезпеки виявляються і ефективно обробляються, зокрема, вирішується чи класифікувати їх як інцидент;
- виявлені події кібербезпеки оцінюються найбільш доцільним і ефективним способом у межах визначеної термінології;
- засвоєні уроки враховуються при виявлянні, оцінюванні, вирішуванні та звітуванні про події кібербезпеки. Зворотний зв'язок сприятиме збільшенню шансів запобігати настанню інцидентів, покращенню упроваджування заходів і, як наслідок, загального плану управління інцидентами кібербезпеки.

Для досягання встановлених цілей потребується наявність затвердженого керівництвом об'єкта критичної інфраструктури процесу управління інцидентами кібербезпеки. Зокрема його складника механізму повідомляння про події як сукупності процесів у межах структурованого представлення чотирьох окремих фаз (рис. 2) [24-26]:

1. Планувати та готувати. Ефективне повідомляння про події кібербезпеки визначається належністю планування і підготовляння. На цій фазі виконуються підготовчі заходи, за результатами яких розробляються політики, плани, процедури

поводження з інцидентами, призначається координатор. Водночас створюються команди спостережування, реагування, управління кризовими ситуаціями. Політикою управління інцидентами офіційно документуються принципи, процеси насамперед стосовно класифікування відповідальною особою (наприклад, координатором) подій. Окрема увага приділяється описанню звітування про події кібербезпеки за встановленим шаблоном. Це дозволить уникати пропусків та/або недооцінювання отриманих відомостей. Політика управління інцидентами кібербезпеки періодично переглядається і спрямовується на усіх внутрішніх і зовнішніх зацікавлених сторін. Характерною її особливістю є високорівневість і синтезованість відповідним планом. За змістом ним охоплюються узгоджене визначання подій кібербезпеки, опис їх категорування і класифікування, механізм повідомляння про них,

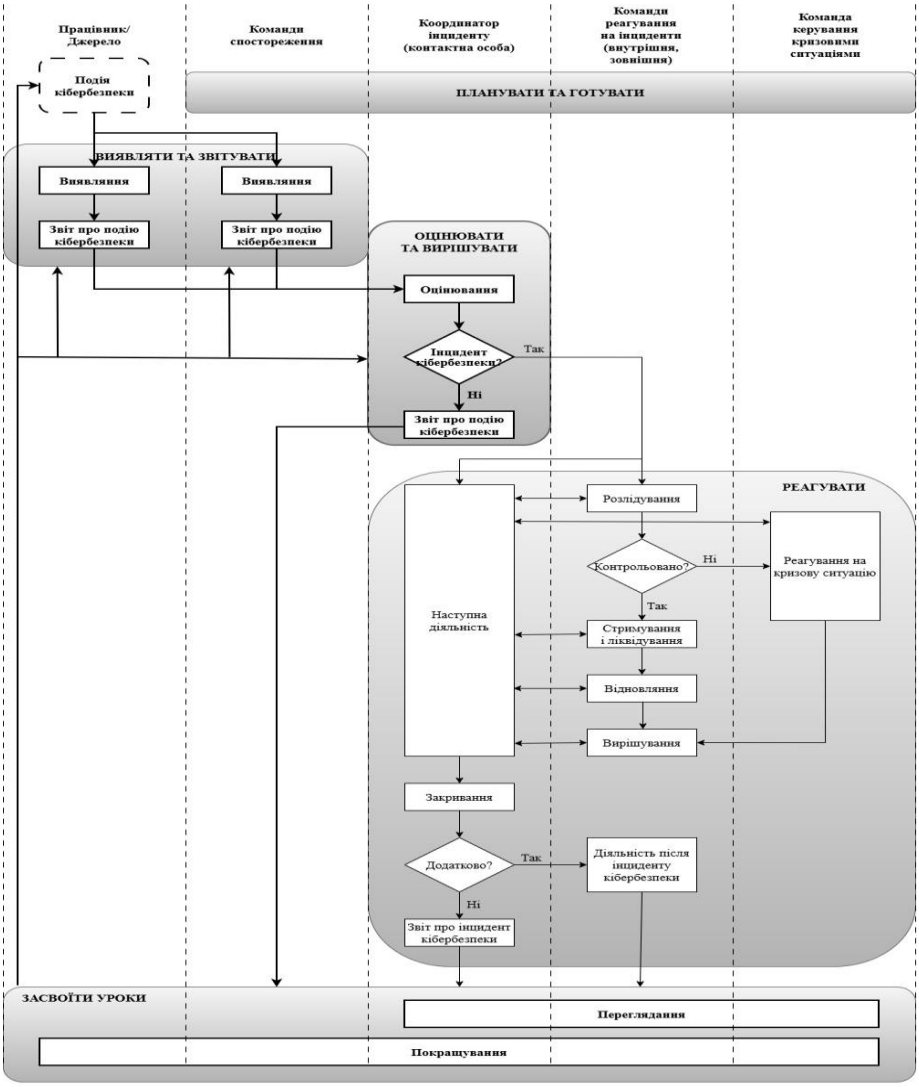

Рис. 2. Дескриптивне представлення потоку подій кібербезпеки [24]

організаційні ролі (наприклад, працівника, команди спостережування, координатора інцидентів) стосовно процесів виявляння, оцінювання, вирішення, звітування. Це дозволить персоналу бути обізнаним стосовно розпізнавання події кібербезпеки та дій в такому випадку.

2. Виявляти та звітувати. Включає одержання повідомлення про подію кібербезпеки від працівника, команди спостережування об'єкта критичної інфраструктури або іншого джерела. Після його отримання збираються відомості про неї, а також виявлені або пов'язані уразливості інформаційних активів, упроваджених заходів і засобів. Для отримання відомостей існує декілька вірогідних каналів, наприклад: телефоном, факсом, електронною поштою, месенджером, через панель управління. Важливо документувати накопичені відомості про подію кібербезпеки від виявляння до вирішування. Як наслідок, отримані результати синтезуються у формі звіту за встановленим шаблоном при плануванні та підготовлянні. Завдяки цьому можливий перехід до наступних завдань як у межах поточної, так і наступної фаз. Воно реалізується або ручними, або автоматизованими засобами. Тож підготовленим звітом про подію кібербезпеки узагальнюються усі доступні відомості для її розуміння і прийняття рішення про її класифікування як інциденту [24]. До таких відомостей належать: дата, час виявляння, ім'я інформатора, обставини та факти. Усі зібрані відомості про подію кібербезпеки, пов'язаних з нею уразливостей і загроз рекомендується зберігати в реєстрі інцидентів. Це сприяє проведенню оцінювання і прийняття рішень стосовно її класифікування. До того ж такі відомості корисні при виявлянні події кібербезпеки, вразливості інформаційного активу, заходів і, як наслідок, активуванні плану управління інцидентами.

3. Оцінювати та вирішувати. Відповідальним за управління діями реагування на інциденти кібербезпеки є координатор [24]. За результатами оцінювання події ним приймається рішення про її класифікування як інциденту з огляду на звіт і рекомендації в плані управління інцидентами. Наприклад [25], незначний інцидент кібербезпеки може призвести до кризової ситуації, якщо його належно не обробити, або незначний інцидент інформаційної безпеки без обробляння може призвести до інциденту кібербезпеки. безпеки. Залежно від прийнятого рішення координатор заявляє про інцидент; залучає, координує діяльність відповідних команд реагування на комп'ютерні надзвичайні ситуації (англ. Computer Emergency Response Team, CERT) та інциденти комп'ютерної безпеки (англ. Computer Security Incident Response Team, CSIRT). Наприклад, CERT-UA, MIL.CERT-UA, CSIRT-NBU, CSIRT ДержНДІ. В іншому випадку він узагальнює відомості та звітує про подію (події) кібербезпеки, а також, за потреби, пропонує покращування виявляння, оцінювання, звітування. Наприклад [5], в межах об'єкта критичної інфраструктури такими повноваженнями наділяються або призначена відповідальна особа зі завданнями керівника з кіберзахисту (організаційна функція), або керівник підрозділу кіберзахисту (організаційна роль). З урахування дій у межах даної фази рекомендується швидко прийняти рішення про клас події кібербезпеки – інциденти/не інцидент. Від цього залежить необхідність і водночас тривалість призначення команди реагування на інциденти, а також терміни їх обробляння.

4. Засвоювати уроки. Відбувається або після закривання інциденту кібербезпеки, або після завершування звітування про подію у випадку віднесення її до класу – не інцидент. Включає засвоювання досвіду на основі отриманого звіту і обробки інциденту асоційованих з ним загроз і вразливостей. Насамперед це стосується пропозицій, наприклад [24], з боку координатора, стосовно покращування механізму повідомляння про події кібербезпеки, їх виявляння, оцінювання і звітування. При цьому переглядається ефективність даних процесів, шаблонів повідомлення і звітів. До того ж встановлюється залученість за організаційною структурою до повідомляння про інциденти кібербезпеки об'єкта критичної інфраструктури. Засвоєні уроки

документуються, поширюються серед внутрішніх і зовнішніх зацікавлених сторін. Це дозволяє накопичувати досвід повідомляння про події і реагування на інциденти кібербезпеки загалом. Отримані знання, практичні вміння і навики тлумачаться як джерела для розробляння програм підвищення кібербезпекової обізнаності. Вони включають уроки на основі отримання реального досвіду. У такий спосіб може зменшуватися кількість помилок протягом застосувань механізму повідомляння про події і реагування на інциденти кібербезпеки.

Працівники об'єкта критичної інфраструктури повинні заохочуватися до повідомляння про події кібербезпеки «без страху бути покараними». Оскільки завдяки його своєчасності можливо запобігти настанню масштабних негативних наслідків. До того ж рекомендується зосереджуватися на вдосконалюванні та навчанні з метою бути більш безпечним і стійким до реалізувань загроз кібербезпеці [4], [24]. Ефективність реагування на інциденти визначається також внутрішнім комунікуванням [24], зокрема, важливо хто, що, як і кому повідомляє. Це впливає на своєчасність і належність реагування і, як наслідок, задоволення кібербезпекових потреб і об'єкта критичної інфраструктури, і суспільства. Тоді як завдяки зовнішньому комунікуванні убезпечуються імідж, бренд, репутація об'єкта критичної інфраструктури [24].

Тож використання представленого в [24-26] структурованого підходу до визначання механізму повідомляння про події і, загалом до управління інцидентами кібербезпеки об'єктів критичної інфраструктури характеризується таким перевагами:

- покращення реагування на інциденти кібербезпеки структуруванням процесів планування, підготовляння, виявляння, оцінювання і звітування про події кібербезпеки;
- зменшення негативних наслідків для об'єкта критичної інфраструктури своєчасним повідомлянням про події і, як наслідок, реагуванням на інциденти кібербезпеки;
- покращення пріоритезування подій кібербезпеки створюванням підґрунтя для визначання пріоритетів, використанням ефективних шкал категорування і класифікування;
- контролювання розподілюванням наявних ресурсів, відстежуванням часу від повідомляння про подію кібербезпеки до класифікування/не класифікування її як інциденту;
- визначання успішності розробляння і впроваджування системи управління інформаційною безпекою об'єкта критичної інфраструктури.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, визначено механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури. Для цього використано настанови гармонізованих в Україні міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27035-1, 2, 3. За результатами аналізування встановлено орієнтованість відомих теоретичних і практичних здобутків на процеси виявляння та реагування. При цьому припускається, що вхідними для них є відомості про інцидент кібербезпеки. Так демонструється актуальність і важливість обраного напряму досліджень. Оскільки як внутрішні, так і зовнішні зацікавлені сторони в кібербезпеці об'єктів критичної інфраструктури повинні бути обізнані про що, як і кому повідомляти. Тому при визначанні процесів даного механізму за основу взято дескриптивне представлення потоку подій кібербезпеки.

Насамперед у межах фаз планування і готування, виявляння і звітування, оцінювання і вирішення.

У перспективах подальших досліджень планується дослідити парадигму повідомляння про події кібербезпеки об'єктів критичної інфраструктури відповідно до положень міжнародних, національних і вітчизняних нормативних документів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verkhovna Rada of Ukraine. (2021). *Law of Ukraine "On critical infrastructure" (No. 1882-20, November 16)*. https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. National Bank of Ukraine. (2025). *On critical infrastructure of the financial sector (Resolution No. 69, June 27)*. https://zakon.rada.gov.ua/laws/show/v0069500-25#Text
3. International Organization for Standardization. (2022). *ISO/IEC 27005:2022—Information security risk management*.
4. Mokhor, V. V., Bakalynskyi, O. O., Dorohyi, Y. Y., & Tsurkan, V. V. (2024). Paradigm of new cybersecurity risks. In *Cybersecurity of energy* (pp. 116–117). Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine. https://doi.org/10.5281/zenodo.14601760
5. Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On the basic principles of cybersecurity of Ukraine" (No. 2163-19, October 5)*. https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Cabinet of Ministers of Ukraine. (2019). *On approval of general requirements for cyber protection of critical infrastructure objects (Resolution No. 518, June 19)*. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8
7. National Bank of Ukraine. (2025). *On critical infrastructure of the financial sector (Resolution No. 143, December 9)*. https://zakon.rada.gov.ua/laws/show/v0143500-25#Text
8. Cabinet of Ministers of Ukraine. (2022). *On approval of the regulation on information exchange between critical infrastructure protection entities (Resolution No. 1174, October 14)*. https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text
9. Cabinet of Ministers of Ukraine. (2025). *On approval of the procedure for interaction of entities in responding to cyber incidents, cyberattacks, and cyber threats (Resolution No. 1471, November 13)*. https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#n8
10. Cabinet of Ministers of Ukraine. (2025). *Some issues of response to cyber incidents, cyberattacks, and cyber threats (Resolution No. 1533, November 26)*. https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#n12
11. State Service of Special Communications and Information Protection of Ukraine. (n.d.). *Analytical materials*. https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku
12. Khoroshko, V. O., & Brailovskyi, M. M. (2021). Management of conflicts and information security incidents on the Internet. *Informatics and Mathematical Methods in Modeling, 11*(1–2), 15–25. https://doi.org/10.15276/imms.v11.no1-2.15
13. Senarath, Y., Mukhopadhyay, A., Vazirizade, S. M., Purohit, H., Nannapaneni, S., & Dubey, A. (2021). Practitioner-centric approach for early incident detection using crowdsourced data. In *IEEE International Conference on Data Mining* (pp. 1318–1323). https://doi.org/10.1109/ICDM51629.2021.00164
14. Nowikowska, M. (2022). The main tasks of CSIRT networks under the national cybersecurity system in Poland. In K. Chałubińska-Jentkiewicz et al. (Eds.), *Cybersecurity in Poland* (pp. 223–242). Springer. https://doi.org/10.1007/978-3-030-78551-2_15
15. Khlaponin, Y. I., Kozubtsov, I. M., Kozubtsova, L. M., & Shtonda, R. M. (2022). Functions of cybersecurity systems for critical infrastructure. *Cybersecurity: Education, Science, Technique, 3*(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341
16. Fayzullajon, B., Azam, G., & Sherzod, S. (2023). Handling information security events and incidents. In *Inventive Communication and Computational Technologies* (Vol. 383, pp. 509–514). Springer. https://doi.org/10.1007/978-981-19-4960-9_40
17. Subach, I. Y., & Vlasenko, O. V. (2023). Architecture of an intelligent SIEM system for detecting cyber incidents in military information systems. *Systems and Technologies of Communication, Informatization and Cybersecurity, 4*, 82–92. https://doi.org/10.58254/viti.4.2023.07.82
18. Basan, E., Bystraya, Z., Mogilny, A., Lesnikov, A., & Lapin, V. (2024). Development of a framework for describing security incidents. In *Advanced Information Security Management and Applications* (Vol. 863, pp. 19–30). Springer. https://doi.org/10.1007/978-3-031-72171-7_3

19. Shulha, V. P., Ivanchenko, Y. V., Vyshnevska, N. S., & Berber, A. S. (2024). Methods and models for assessing cybersecurity of critical infrastructure. *Modern Information Protection, 3*, 6–19. https://doi.org/10.31673/2409-7292.2024.030001
20. Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity: From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 1–17. https://doi.org/10.1016/j.giq.2024.102000
21. Sydorenko, V. M., & Maksymets, A. V. (2025). Decision-making method for cybersecurity incident management in critical infrastructure. *Information Security, 31*(2), 93–97. https://doi.org/10.18372/2225-5036.31.20701
22. International Organization for Standardization. (2022). *ISO/IEC 27001:2022—Information security management systems—Requirements*.
23. International Organization for Standardization. (2022). *ISO/IEC 27002:2022—Information security controls*.
24. International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023—Information security incident management—Part 1: Principles and process*.
25. International Organization for Standardization. (2023). *ISO/IEC 27035-2:2023—Guidelines for incident response preparation*.
26. International Organization for Standardization. (2020). *ISO/IEC 27035-3:2020—Guidelines for ICT incident response operations*.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Vasyl V. Tsurkan
Candidate of Technical Sciences, Associate Professor, Associate Professor; Senior Researcher
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»;
G.E. Pukhov Institute for Modelling in Energy
Engineering of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0003-1352-042X
v.v.tsurkan@gmail.com

Vladyslav S. Rakovych
Postgraduate Student
G. E. Pukhov Institute for Modelling in Energy
Engineering of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0009-0008-4733-9120
covlad@ukr.net

CYBERSECURITY INCIDENTS NOTIFICATION MECHANISM AT CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The importance of critical infrastructure facilities for the economy, national security, and defense has been demonstrated. This is due to the vital functions and/or services they provide to organizations in both the public and private sectors. Preventing their disruption is achieved by implementing measures and methods to manage, monitor, and assess security risks. Additionally, this involves either eliminating, mitigating the consequences, or recovering from threats once they materialize. At the same time, it involves adapting to emerging security risks. This is achieved by critical infrastructure operators developing appropriate systems, particularly those ensuring cybersecurity. Therefore, preventing negative impacts and consequences is achieved through risk management. In particular, critical infrastructure operators ensure incident response in accordance with the national plan. This necessitates the implementation of a cybersecurity event notification mechanism at critical infrastructure facilities. Analysis of recent studies and publications indicates that they focus primarily on the processes of detecting and responding to cybersecurity incident. In view of this, the cybersecurity event notification mechanism at critical infrastructure facilities is defined as a set of processes within a structured framework for incident management. To this end, the relationships between their components – specifically, activities, information assets, vulnerabilities, and threats –have been taken into account. Among the phases, the primary focus is on planning and preparation, detection and reporting, and assessment and resolution. Each of these phases defines the processes from receiving information about an event to deciding whether it falls into one of the categories – incident or non-incident. Together, they define the cybersecurity event notification mechanism at critical infrastructure facilities. To this end, the guidelines of the international standards ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035-1, 2, 3, harmonized in Ukraine, have been utilized. Particular attention is paid to learning lessons following the reporting of both events and cybersecurity incidents. This approach helps keep processes, cybersecurity event report templates, and related reports up to date.

Keywords: critical infrastructure facility, cybersecurity event; cybersecurity incident; notification mechanism; cybersecurity event notification; cybersecurity event report.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Verkhovna Rada of Ukraine. (2021). Law of Ukraine “On critical infrastructure” (No. 1882-20, November 16). https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. National Bank of Ukraine. (2025). On critical infrastructure of the financial sector (Resolution No. 69, June 27). https://zakon.rada.gov.ua/laws/show/v0069500-25#Text
3. International Organization for Standardization. (2022). ISO/IEC 27005:2022—Information security risk management.
4. Mokhor, V. V., Bakalynskyi, O. O., Dorohyi, Y. Y., & Tsurkan, V. V. (2024). Paradigm of new cybersecurity risks. In Cybersecurity of energy (pp. 116–117). Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine. https://doi.org/10.5281/zenodo.14601760
5. Verkhovna Rada of Ukraine. (2017). Law of Ukraine “On the basic principles of cybersecurity of Ukraine” (No. 2163-19, October 5). https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Cabinet of Ministers of Ukraine. (2019). On approval of general requirements for cyber protection of critical infrastructure objects (Resolution No. 518, June 19). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8
7. National Bank of Ukraine. (2025). On critical infrastructure of the financial sector (Resolution No. 143, December 9). https://zakon.rada.gov.ua/laws/show/v0143500-25#Text
8. Cabinet of Ministers of Ukraine. (2022). On approval of the regulation on information exchange between critical infrastructure protection entities (Resolution No. 1174, October 14). https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text
9. Cabinet of Ministers of Ukraine. (2025). On approval of the procedure for interaction of entities in responding to cyber incidents, cyberattacks, and cyber threats (Resolution No. 1471, November 13). https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#n8
10. Cabinet of Ministers of Ukraine. (2025). Some issues of response to cyber incidents, cyberattacks, and cyber threats (Resolution No. 1533, November 26). https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#n12
11. State Service of Special Communications and Information Protection of Ukraine. (n.d.). Analytical materials. https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku
12. Khoroshko, V. O., & Brailovskyi, M. M. (2021). Management of conflicts and information security incidents on the Internet. Informatics and Mathematical Methods in Modeling, 11(1–2), 15–25. https://doi.org/10.15276/imms.v11.no1-2.15
13. Senarath, Y., Mukhopadhyay, A., Vazirizade, S. M., Purohit, H., Nannapaneni, S., & Dubey, A. (2021). Practitioner-centric approach for early incident detection using crowdsourced data. In IEEE International Conference on Data Mining (pp. 1318–1323). https://doi.org/10.1109/ICDM51629.2021.00164
14. Nowikowska, M. (2022). The main tasks of CSIRT networks under the national cybersecurity system in Poland. In K. Chałubińska-Jentkiewicz et al. (Eds.), Cybersecurity in Poland (pp. 223–242). Springer. https://doi.org/10.1007/978-3-030-78551-2_15
15. Khlaponin, Y. I., Kozubtsov, I. M., Kozubtsova, L. M., & Shtonda, R. M. (2022). Functions of cybersecurity systems for critical infrastructure. Cybersecurity: Education, Science, Technique, 3(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341
16. Fayzullajon, B., Azam, G., & Sherzod, S. (2023). Handling information security events and incidents. In Inventive Communication and Computational Technologies (Vol. 383, pp. 509–514). Springer. https://doi.org/10.1007/978-981-19-4960-9_40
17. Subach, I. Y., & Vlasenko, O. V. (2023). Architecture of an intelligent SIEM system for detecting cyber incidents in military information systems. Systems and Technologies of Communication, Informatization and Cybersecurity, 4, 82–92. https://doi.org/10.58254/viti.4.2023.07.82
18. Basan, E., Bystraya, Z., Mogilny, A., Lesnikov, A., & Lapin, V. (2024). Development of a framework for describing security incidents. In Advanced Information Security Management and Applications (Vol. 863, pp. 19–30). Springer. https://doi.org/10.1007/978-3-031-72171-7_3
19. Shulha, V. P., Ivanchenko, Y. V., Vyshnevska, N. S., & Berber, A. S. (2024). Methods and models for assessing cybersecurity of critical infrastructure. Modern Information Protection, 3, 6–19. https://doi.org/10.31673/2409-7292.2024.030001
20. Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity: From threat detection to policy learning. Government Information Quarterly, 42(1), 1–17. https://doi.org/10.1016/j.giq.2024.102000
21. Sydorenko, V. M., & Maksymets, A. V. (2025). Decision-making method for cybersecurity incident management in critical infrastructure. Information Security, 31(2), 93–97. https://doi.org/10.18372/2225-5036.31.20701
22. International Organization for Standardization. (2022). ISO/IEC 27001:2022—Information security management systems—Requirements.
23. International Organization for Standardization. (2022). ISO/IEC 27002:2022—Information security controls.
24. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023—Information security incident management—Part 1: Principles and process.
25. International Organization for Standardization. (2023). ISO/IEC 27035-2:2023—Guidelines for incident response preparation.
26. International Organization for Standardization. (2020). ISO/IEC 27035-3:2020—Guidelines for ICT incident response operations.

Отримано редакцією журналу / Received: 28.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26