DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

УДК 343.973

Сахарова Олена Борисівна,
кандидат юридичних наук,
старший науковий співробітник, начальник відділу
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0002-9759-5324

СУТНІСТЬ ТА ЗМІСТ ПРОЦЕДУРИ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ВІДПОВІДНО ДО МІЖНАРОДНИХ СТАНДАРТІВ ISO ТА NIST

У статті розкриваються сутність та зміст процедури розслідування кіберінцидентів відповідно до міжнародних стандартів ISO та NIST. Зокрема, згідно з ISO/IEC 27042:2015, надається визначення поняття "розслідування кіберінцидентів" та наводяться етапи процедури розслідування кіберінциденту. Акцентується увага на тому, що система заходів кіберзахисту має базуватися на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом із технологіями забезпечення кібербезпеки.

Ключові слова: *кіберінциденти, міжнародні стандарти ISO та NIST, розслідування кіберінцидентів, кібератаки, кіберзлочини, процедура розслідування кіберінциденту.*

Кібератаки стали звичним явищем у всьому світі, становлячи реальну і серйозну загрозу на державному та корпоративному рівнях. Зросла не тільки кількість атак, а і їхня складність, масштабність. Кіберзлочини стають все більш складними та витонченими, що значно ускладнює процес їх виявлення та попередження. Так, кіберзлочини, як й інформаційні технології, постійно вдосконалюються, у зв'язку з чим з'являються нові види злочинних посягань. Спостерігається зростання технологічного рівня кібератак/кіберзлочинів. При цьому велика кількість кіберзагроз є непоміченою.

Традиційні механізми захисту не можуть протистояти сучасним кіберзагрозам. Багато юридичних осіб не мають достатнього рівня обізнаності та необхідної кількості ресурсів, щоб захистити себе від внутрішніх і зовнішніх кіберзагроз. Саме тому впровадження практики розслідування кіберінцидентів є необхідним кроком для забезпечення стабільності діяльності як державних органів, так і бізнесу компаній, збереження клієнтів та постійного розвитку.

Згідно з ISO/IEC 27042:2015 "Інформаційні технології. Методи захисту. Керівництва з аналізу та інтерпретації цифрового доказу" ("Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence") розслідування (investigation) кіберінцидентів – це застосування експертизи, аналізу та інтерпретації для сприяння у розумінні кіберінциденту.

Процедура розслідування кіберінциденту складається з таких послідовних етапів:

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

1) *Підготовка* – на цьому етапі слід провести попередню підготовку до розслідування кіберінциденту. Етап підготовки до розслідування кіберінцидентів полягає у зборі та аналізі інформації про кіберінциденти, навчанні персоналу та підготовці необхідного інструментарію для реагування та розслідування кіберінциденту. Команда реагування та розслідування кіберінцидентів повинна класифікувати та описати кожен кіберінцидент, що стався у компанії / державному органі, а також класифікувати та описати можливі кіберінциденти, припущення про які були зроблені на основі аналізу ризиків настання тієї чи іншої події інформаційної безпеки.

2) *Виявлення* – на цьому етапі встановлюється факт несанкціонованої події, тобто кіберінциденту. Залежно від серйозності кіберінциденту, крім збору даних, слід прийняти рішення про порядок реагування на цю подію.

Звіт про виявлення та реєстрацію кіберінциденту має містити докладний опис кіберінциденту, перелік залучених співробітників, прізвище співробітника, що зафіксував кіберінцидент, дату його виникнення та реєстрації [1, с. 121].

Оперативні дані сенсорів безпеки повинні аналізуватися та оцінюватися на предмет наявності сигнатур відомих кіберінцидентів за допомогою бази знань інтелектуальної системи підтримки прийняття рішень щодо управління кіберінцидентами. Після чого кожний адміністратор, користувач чи співробітник має одержати інструкцію, що визначатиме, якими повинні бути його дії [1, с. 121].

3) *Збір даних* – дані слід отримувати від інструментів, що використовуються для збору даних про трафік. Цей етап дуже важливий. Обмін даними про трафік здійснюється з високою швидкістю, тому пізніше отримати ті ж дані про мережний трафік буде неможливо.

4) *Збереження даних* – отримані вихідні дані про мережний трафік слід зберігати на пристрої резервного копіювання, зберігається також хеш-код всіх даних.

5) *Розслідування* – на цьому етапі слід звести разом усі зібрані сліди (докази). Здійснюється пошук доказів виявлення артефактів кібератаки. Ознаки класифікуються і зіставляються, та на їх основі виконуються важливі спостереження з використанням існуючих кібератак. На цьому етапі може бути встановлений тракт кібератаки і шляхом багаторазового виконання аналізу атрибутів можна дійти висновку щодо ідентифікаційних даних зловмисника.

6) *Звіт* – спостереження та пояснення до розслідування слід викладати мовою, зрозумілою юристам.

Інтелектуальна система підтримки прийняття рішень щодо управління кіберінцидентами на підставі звіту має надавати інструкцію щодо усунення причин і наслідків кіберінциденту, включаючи опис загальних заходів, які необхідно розпочати, та конкретні дії для кожного кіберінциденту, а також терміни, протягом яких варто усунути наслідки та причини кіберінциденту [1, с. 122]. Варто розробити класифікацію кіберінцидентів – визначити рівні критичності кіберінцидентів, описати кіберінциденти кожного рівня й терміни їх усунення.

Після усунення наслідків кіберінциденту й відновлення нормального функціонування діяльності державного органу або бізнес-процесів, доцільно виконати дії щодо запобігання повторному виникненню кіберінциденту [1, с. 122]. Для визначення необхідності реалізації таких дій інтелектуальна система підтримки

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

прийняття рішень щодо управління кіберінцидентами повинна провести аналіз кіберризиків, у межах якого визначити доцільність коригувальних і превентивних дій.

Щоб проаналізувати причини кіберінцидентів, необхідно зберегти зібрані вихідні дані та не допустити їх пошкодження. Зокрема, у разі судових розглядів необхідно зберегти зібрані дані, щоб цілісність та законність доказів залишалися без змін. Для цього інструменти збереження даних повинні підтримувати такі можливості [2]:

- генерування контрольних сум та цифрових підписів;
- перевірку повного збереження зібраних даних;
- генерування міток часу для фіксації часу збирання та збереження даних;
- запис зібраних даних на пристрій одноразового запису та багаторазового читання;
- політика зберігання даних має дотримуватися належним чином;
- забезпечення збереження зібраних даних протягом усього терміну дії зазначеної політики зберігання даних;
- зберігання зібраних даних та метаданих у формалізованому вигляді.

Дані, зібрані та збережені за допомогою відповідних інструментів, можуть використовуватись для розслідування причин кіберінцидентів та як докази при виявленні відповідальних осіб за кіберінцидент. Тому інструмент збирання та збереження даних для аналізу кіберінцидентів має забезпечувати такі можливості щодо гарантування надійності, що стосуються управління користувачами та даними [2]:

- інструмент повинен надавати засоби для обмеження та контролю доступу користувачів до самого інструменту та до даних, що зберігаються;
- інструмент не має допускати спроб перезапису, зміни або видалення збережених даних без належної авторизації;
- інструмент повинен забезпечувати функції управління безпекою, щоб авторизовані адміністратори могли конфігурувати функції безпеки, політику безпеки і важливі дані та керувати ними;
- під час передачі зібраних даних між фізично ізольованими пристроями дані повинні шифруватися для забезпечення їх конфіденційності та цілісності;
- у всіх засобах передачі даних, пов'язаних з інструментом, слід використовувати захищений шифрований протокол зв'язку;
- інструмент повинен забезпечувати функцію резервного копіювання збережених даних;
- інструмент має забезпечувати можливість ведення журналів подій, звітів про помилки та аудиту;
- інструмент повинен забезпечувати можливості обробки метаданих і формалізованого контенту та їх спільного використання відповідно до чинної політики безпеки.

Обробка кіберінцидентів передбачає визначення їх пріоритетів, що дозволяє оцінювати ймовірність реалізації кіберризиків і тяжкості наслідків від них, і відповідно, своєчасно реагувати і розслідувати кіберінциденти з найвищими ризиками [3, с. 119]. Пріоритет визначається впливом (комерційним збитком

або потенційним пошкодженням, зокрема бази користувачів, кібербезпеки, репутації, бренду), терміновістю (швидкодією щодо усунення ознак кіберінциденту, зокрема витік даних або активне поширення шкідливого програмного забезпечення) [3, с. 119]. Зазвичай кіберінциденти обробляються відповідно до присвоєного їм пріоритету.

У наш цифровий час дуже швидкими темпами розвиваються різноманітні інформаційні технології, але, на жаль, разом з ними розвивається і кіберзлочинність, якій намагаються протистояти як окремі країни, так й на міжнародному рівні шляхом розробки міжнародних та національних норм і стандартів з питань кіберзахисту та кібербезпеки з метою стримування та протидії кіберінцидентам та кіберзлочинам.

Система заходів кіберзахисту має базуватися на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом із технологіями забезпечення кібербезпеки [4].

Організаційно-технічна складова заходів протидії кіберзлочинності полягає у впровадженні організаційно-технічної моделі кіберзахисту, включаючи забезпечення державно-приватної взаємодії, при реалізації заходів запобігання, виявлення, розслідування, реагування на кіберінциденти і кібератаки, усунення їх наслідків [5, с. 96].

Організаційно-технічна модель кіберзахисту, виявлення та розслідування кіберінцидентів та кіберзлочинів має базуватися на міжнародних ризик-орієнтованих стандартах управління кібербезпекою: стандартах ISO/IEC 27032:2012 "Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки" ("Information technology. Security techniques. Guidelines for cybersecurity"), ISO/IEC 27037:2012 "Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів" ("Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence"), ISO/IEC 27041:2015 "Настанова щодо забезпечення прийнятності та адекватності методів розслідування" ("Guidance on assuring suitability and adequacy of incident investigative method"), ISO/IEC 27043:2015 "Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів" ("Information technology. Security techniques. Incident investigation principles and processes") *[*5, с. 96], Рекомендації Міжнародного союзу електрозв'язку МСЕ-Т X.1216 (09/2020) "Вимоги до збирання та збереження доказів інцидентів кібербезпеки" [2]. Так, у Рекомендації МСЕ-Т X.1216 (09/2020) описано загальну процедуру реагування на кіберінциденти та їх розслідування. Крім того, у цій Рекомендації проведено аналіз джерел доказів кіберінцидентів та визначено вимоги до можливостей інструментів, що використовуються для збирання та збереження таких доказів у процесі розслідування.

Зокрема, різні керівні вказівки ІСО/МЕК, що стосуються цифрового розслідування та реагування на кіберінциденти, стандартизовані в документах ISO/IEC 27035-3:2020 "Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 3. Керівні вказівки для операцій з реагування на інциденти в сфері інформаційно-комунікаційних технологій" ("Information technology Information security incident management Part 3: Guidelines for ICT incident

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

response operations"), ISO/IEC 27037:2012 "Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів" ("Guidelines for identification, collection, acquisition and preservation of digital evidence"), ISO/IEC 27041:2015 "Настанова щодо забезпечення прийнятності та адекватності методів розслідування" ("Guidance on assuring suitability and adequacy of incident investigative method"), ISO/IEC 27042:2015 "Інформаційні технології. Методи захисту. Керівництва з аналізу та інтерпретації цифрового доказу" ("Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence") та ISO/IEC 27043:2015 "Принципи та процеси розслідування інцидентів" ("Incident investigation principles and processes"). Ці керівні вказівки призначені в основному для надання інформації про передовий досвід та обробку цифрових доказів на всіх етапах процедури розслідування кіберінцидентів [2].

У IETF RFC 3227 (2002) "Guidelines for Evidence Collection and Archiving" також містяться керівні вказівки щодо збору та архівування доказів, включаючи підготовку та розгляд етапів збору даних; вибір архівних носіїв та документації для забезпечення збереження речових доказів при їх передачі; набір інструментів, необхідних для збору та архівування доказів [2]. Однак ці керівні вказівки щодо вибору або розробки інструментів розслідування кіберінцидентів сформульовані недостатньо чітко.

Документ CMU/SEI-2004-TR-015 "Defining incident management processes for CISRT" описує методологію планування, впровадження, оцінки та поліпшення процесів управління кіберінцидентами [6]. У цьому документі увага зосереджується на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділу, що забезпечує сервіс і підтримку запобігання, обробки і реагування на кіберінциденти; вводиться низка критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, наводяться докладні процесні карти [6].

У міжнародному стандарті NIST SP 800-61 "Computer security incident handling guide" представлений збірник "найкращих практик" з побудови процесів обробки, управління кіберінцидентами та реагування на них [6]. У цьому стандарті детально розбираються питання реагування на різні типи кіберзагроз, такі як поширення шкідливого програмного забезпечення, несанкціонований доступ тощо.

Водночас ключовим моментом захисту від кіберзлочинності є підготовка і виявлення вразливих місць, а також стійкість з погляду взаємодії із загальними системами управління. Керувати інформаційною безпекою, а також визначити злочинців і притягнути їх до відповідальності допоможуть міжнародні стандарти серії ISO/IEC 27000, розроблені спільним технічним комітетом Міжнародної організації з стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) – ISO/IEC JTC 1 [7].

Перший стандарт серії – ISO/IEC 27001 щодо систем управління інформаційною безпекою (ISMS) опубліковано вже більше 20 років тому. З того часу у серії видано понад 40 міжнародних стандартів, що охоплюють все: від створення спільного словника (ISO/IEC 27000), управління ризиками (ISO/IEC 27005), безпеки у хмарних технологіях (ISO/IEC 27017 і ISO/IEC 27018) до методів експертизи, що використовують для аналізу цифрових доказів та розслідування кіберінцидентів (вже згадані вище ISO/ IEC 27042 та ISO/IEC 27043 відповідно) [7].

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

Наприклад, ISO/IEC 27043 пропонує настанови, що описують процеси та принципи, які застосовують до різних видів досліджень, включаючи несанкціонований доступ, пошкодження даних, збої в системі або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові дані розслідування кіберінцидентів [7].

ISO/IEC 27043 забезпечує керівництво на основі ідеалізованих моделей для вивчення загальних процесів для розслідування кіберінцидентів у різних сценаріях їх розслідування, що включають цифрові докази. Зазначене Керівництво описує процеси та принципи, що застосовуються до різних видів розслідувань кіберінцидентів, у тому числі не обмежуючись до несанкціонованого доступу, спотворення даних, системних збоїв або корпоративних порушень інформаційної безпеки, а також будь-яких інших цифрових розслідувань.

Розробники стандартів серії ISO/IEC 27000 зазначають, що основоположний стандарт серії ISO/IEC 27001 постійно вдосконалюється. Завдяки впровадженню стандарту ISO/IEC 27001 можна оцінювати кіберризики, впроваджувати засоби контролю щодо їх пом'якшення, а потім контролювати та переглядати кіберризики та контроль за ними, покращуючи за необхідності кіберзахист. Таким чином, будь-який державний орган та компанія завжди готові до кібератак.

Системи управління інформаційною безпекою ISMS застосовують до всіх типів організацій та всіх видів підприємницької діяльності, зокрема для малих та середніх підприємств (SMEs), які є частиною ланцюгів постачання, і тому дуже важливо, щоб вони контролювали та управляли своєю інформаційною безпекою та кіберризиками, щоб захистити себе від зловмисників у кіберпросторі.

У 2019 р. було опубліковано міжнародний стандарт ISO/IEC 27701:2019 "Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки", раніше відомий як ISO/IEC 27552, який було переглянуто, він додатково розширює ISO/IEC 27001 для вирішення конкретних потреб у сфері конфіденційності. Тепер новий стандарт визначає вимоги та надає керівництво зі створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою у формі розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційністю у контексті організації. Іншими словами, створено систему управління інформацією для захисту персональних даних (PIMS).

Таким чином, стандарти серії ISO/IEC 27000 дійсно допомагають зробити безпечнішими усі сфери інформаційного життя, захищаючи приватність, фінанси, індивідуальну або корпоративну репутацію, при цьому постійно розвиваючись і вдосконалюючись [7].

Відзначимо, що найбільшу кількість стандартів, рекомендацій і технічних звітів у сфері реагування, обробки, керування кіберінцидентами розроблено в США [1, с. 116].

Міжнародні стандарти ISO/IEC та інші як методологічні засади мають використовуватися для створення системи управління кіберінцидентами, яка б цілком вписувалася та була б логічним продовженням наявних і сертифікованих систем керування управлінськими процесами, зокрема, таких як система технічної експлуатації та система менеджменту якості ISO 9001 [1, с. 121].

Організаційно-технічна модель кіберзахисту, виявлення та розслідування кіберінцидентів та кіберзлочинів включає моделі оцінки ризику та прийняття рішень у кіберпросторі, а їх стандартизація та впровадження безпосередньо впливає на ефективність заходів з протидії кіберінцидентам та кібератакам.

Отже, в Україні доцільно продовжувати роботу у напрямку подальшого удосконалення нормативно-правової бази шляхом впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері кібербезпеки та кіберзахисту, особливо в умовах воєнного часу, коли спостерігається збільшення кількості кібератак на об'єкти критичної інфраструктури України з боку країни-агресора.

Зокрема, актуальними у всіх країнах є питання захисту автоматизованих систем управління важливими інфраструктурними об'єктами держави. Підтвердженням тому є велика кількість стандартів і кращих практик з інформаційної безпеки автоматизованих систем управління критичними об'єктами держави, випущених міжнародними інститутами зі стандартизації, галузевими або державними організаціями. Причинами такої активності є високий ступінь ризику кібертерористичних загроз у сучасному світі і вразливість автоматизованих систем управління ключовими об'єктами держави перед сучасними кібератаками.

На жаль, доводиться констатувати, що поточна ситуація в Україні із забезпеченням кібербезпеки в технологічних мережах автоматизованих систем управління ключовими об'єктами держави не викликає оптимізму. Вразливостей у технологічних мережах ключових підприємств і організацій вітчизняної економіки більш ніж достатньо. На деяких об'єктах технологічні мережі є частиною єдиної офісної мережі з підключенням до мереж загального користування. При цьому обладнання автоматизованих систем управління ключовими об'єктами не має практично ніяких засобів захисту, і оновлення операційних систем проводяться вкрай рідко (або взагалі не проводяться). Очевидно, що такі технологічні мережі автоматизованих систем управління ключових підприємств і організацій вітчизняної економіки є досить легкою мішенню для кібератак.

Питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій у вітчизняній професійній спільноті. Наразі в Україні як єдиний (крім банківського сектору) державний стандарт технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5–004–99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [8, с. 56]. НД ТЗІ 2.5–004–99 використовується у проєктуванні та створенні комплексної системи захисту інформації (КСЗІ) державних інформаційних ресурсів, а також спеціалізованих інформаційних систем, у яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої визначено законом.

На відміну від найпоширенішої у світі серії стандартів ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5–004–99 є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткому регламенту – комплексній системі захисту інформації (КСЗІ)[1] [8, с. 57]. З погляду фахівців, сама ідея, внутрішня

[1] Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

структура і модель впровадження КСЗІ здебільшого не відповідають вимогам сучасного кіберзахисту, особливо в недержавному секторі [8, с. 57], через недостатню гнучкість, громіздкість, застарілу концепцію захисту тощо. Загалом на сьогодні низка нормативних документів про технічний захист інформації (НД ТЗІ), а також КСЗІ морально застаріли та впродовж багатьох років довели свою неефективність. Комплексна система захисту інформації (КСЗІ), базована на українському стандарті КСЗІ НД ТЗІ 2.5–004–99, здебільшого піддається гострій критиці у вітчизняних експертних та бізнесових колах [8, с. 56]. Найнагальнішим кроком є заміна НД ТЗІ більш ефективним і сучасним базовим стандартом та запровадження галузевих стандартів систем захисту інформації.

Упровадження системи управління інформаційною безпекою (далі – СУІБ) відповідно до серії стандартів ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів [8, с. 57].

Так, пов'язаний із стандартом ISO/IEC 27000:2018 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник" ("Information technology – Security techniques – Information security management systems – Overview and vocabulary") стандарт ISO/IEC 27032:2012 визнає найбільш поширеними такі кіберзагрози:

• атаки соціального інжинірингу;

• хакінг (злам комп'ютерної системи);

• поширення шкідливого програмного забезпечення ("шкідливих програм" / комп'ютерних вірусів ("malware"));

• впровадження шпигунських програм;

• дію інших потенційно небажаних програмних кодів.

Відповідно до стандарту ISO/IEC 27032:2012 технічні рекомендації з протидії ризикам реалізації названих кіберзагроз містять заходи:

• готовності до відбиття кібератак з боку:

а) автономних шкідливих кодів;

б) окремих зловмисників;

в) злочинних і агресивних організацій в Інтернеті;

• виявлення і моніторингу кібератак;

• нейтралізації кібератак.

Стандарт ISO/IEC 27032:2012 виділяє для розгляду три ключових напрями забезпечення кібербезпеки:

• протидія кібератакам, що проводиться з використанням шкідливого та/або потенційно небажаного програмного коду;

• протидія кібератакам, що проводиться із застосуванням технологій соціального інжинірингу;

• співробітництво, координація спільних дій і поширення інформації.

ISO/IEC 27032:2012 стосується питань забезпечення інформаційної безпеки, мережевої безпеки, безпеки в Інтернеті, безпеки ключової інформаційної інфраструктури (CIP), включаючи інформаційні системи [9]. Водночас, як наголошується у стандарті, кібербезпека не є синонімом безпеки в Інтернеті, мережевої безпеки, безпеки програм і додатків, інформаційної безпеки та захисту ключової інформаційної інфраструктури і систем.

Стандарт ISO/IEC 27032:2012 пропонує рекомендації щодо політик; методів; процесів; заходів технічної безпеки.

Загалом згідно з цим стандартом кібербезпека спирається на інформаційну безпеку, безпеку додатків, мережеву безпеку і безпеку Інтернету як на блоки свого фундаменту.

Так, стандарт ISO/IEC 27039:2015 "Information technology. Security techniques. Selection, deployment and operations of intrusion detection systems" ("Запобігання вторгненням") надає керівництво у підготовці до розгортання систем виявлення та запобігання спробам вторгнення.

Також доцільно узагальнити міжнародні стандарти з питань реагування та розслідування кіберінцидентів. Практичний підхід до побудови еталонного процесу реагування та розслідування кіберінцидентів докладно описаний у таких міжнародних стандартах [10]:

• ISO/IEC 27001:2015 "Information security management system. Requirements" – стандарт, який містить як рекомендації щодо побудови, впровадження, використання та підтримки системи управління інформаційною безпекою загалом, так і підходи до управління кіберінцидентами.

• NIST SP 800-61 "Computer security incident handling guide" – повноцінне керівництво з обробки кіберінцидентів, яке описує різні підходи до реагування на кіберінциденти та їх обробку.

• CMU/SEI-2004-TR-015 "Defining incident management processes for CISRT" – документ для оцінки ефективності роботи підрозділу CISRT (Critical Incident Stress Response Team), що забезпечує запобігання, обробку та реагування на кіберінциденти.

• ISO/IEC 27035 "Information security incident management" – документ встановлює рекомендації щодо управління кіберінцидентами стосовно планування, експлуатації, аналізу та покращення процесу.

• NIST SP 800-83 "Guide to Malware Incident Prevention and Handling" – керівництво із запобігання та обробки кіберінцидентів, пов'язаних із зараженням робочих станцій та ноутбуків шкідливим програмним забезпеченням.

• NIST SP 800-86 "Guide to Integrating Forensic Techniques into Incident Response" – керівництво з техніки проведення розслідувань у межах реакції на виявлені кіберінциденти.

Отже, застосування норм, зазначених міжнародних стандартів ISO, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту, сприятиме підвищенню захисту державних органів, компаній від кіберінцидентів та кіберзлочинів завдяки упровадженню на цих об'єктах СУІБ.

При цьому упровадження стандартів із питань управління інформаційною безпекою ISO є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування і вдосконалення СУІБ та кіберзахисту юридичних осіб.

Застосування СУІБ має поширюватися на всі аспекти та процеси діяльності юридичних осіб різних галузей, інформаційні ресурси та інформаційні системи зі створенням єдиної системи кібербезпеки.

DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Гладиш С.В.* Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. *Реєстрація, зберігання і обробка даних*. 2008. Т. 10. № 1. С. 116–124.

2. Рекомендация МСЭ-Т X.1216 (09/2020) "Требования к сбору и сохранению доказательств инцидентов кибербезопасности". URL: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1641-201609-I!!PDF-R&type=items (дата звернення: 12.09.2022).

3. *Козаченко П.П., Панаско О.М.* Управління інцидентами в контексті інформаційної безпеки підприємства. *Specialized and multidisciplinary scientific researches*. Vol. 2. P. 119–120 (дата звернення: 12.09.2022).

4. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 р. № 601. URL: 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 (дата звернення: 13.09.2022).

5. *Довгань О.Д., Тарасюк А.В.* Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

6. Управління інцидентами інформаційної безпеки. URL: https://studfile.net/preview/16435760/ (дата звернення: 12.09.2022).

7. Нові стандарти для інформаційної безпеки: ДП "Волинський науково-виробничий центр стандартизації, метрології та сертифікації". URL: http://volynstandart.com.ua/info_security/4193/news/ (дата звернення: 13.09.2022).

8. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с.

9. Кібербезпека і інформаційна безпека. Стандарт ISO/IEC 27032. URL: https://ua.ikmj.com/cybersecurity-and-information-security-iso-iec-27032/ (дата звернення: 12.09.2022).

10. *Дрюков В.* Управление инцидентами и событиями информационной безопасности. URL: https://safe-surf.ru/specialists/article/5236/611719/ (дата звернення: 11.09.2022).

REFERENCES

1. *Hladysh S.V.* (2008). Reiestratsiia, zberihannia i obrobka danykh. "Support for decision-making regarding the management of information security incidents in organizational and technical systems". No 1. P. 116–124 [In Ukrainian].

2. Rekomendatsiia MSE-T X.1216 (09/2020) "Trebovaniia k sboru y sokhraneniiu dokazatielstv intsydientov kybierbiezopasnosti". "Requirements for Collecting and Preserving Evidence of Cybersecurity Incidents". (09/2020). Recommendation ITU-T X.1216. URL: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1641-201609-I!!PDF-R&type=items. (Date of Application: 12.09.2022) [In Russian].

3. *Kozachenko P.P., Panasko O.M.* Upravlinnia intsydentamy v konteksti informatsiynoi bezpeky pidpryiemstva. "Incident management in the context of enterprise information security". Specialized and multidisciplinary scientific researches, No 2. P. 119–120. [In Ukrainian].

4. Pro zatverdzhennia Metodychnykh rekomendatsii shchodo pidvyshchennia rivnia kiberzakhystu krytychnoi informatsiinoi infrastruktury. "Order of the State Special Communications Administration On the approval of Methodological recommendations for increasing the level of cyber protection of critical information infrastructure from October 6 2021, No 601". URL: 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. (Date of Application: 12.09.2022) [In Ukrainian].

5. *Dovhan O.D., Tarasjuk A.V.* (2018). Hlobalna kultura kiberbezpeky v systemi zapobihannia kiberzlochynnosti v Ukraini. "Global culture of cyber security in the system of cybercrime prevention in Ukraine". Informatsiia i pravo. No 3. P. 94–103. [In Ukrainian].

6. Upravlinnia intsydentamy informatsiinoi bezpeky. "Management of information security incidents". URL: https://studfile.net/preview/16435760/. (Date of Application: 12.09.2022) [In Ukrainian].

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

7. Novi standarty dlia informatsinoi bezpeky. “New standards for information security”: SE “Volyn Scientific and Industrial Center for Standardization, Metrology and Certification”. URL:http://volynstandart.com.ua/info_security/4193/news/. (Date of Application: 13.09.2022) [In Ukrainian].

8. *Dubov D.* (Eds.). (2018). Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy. “Public-private partnership in the field of cyber security”: international experience and opportunities for Ukraine. Kyiv: NISD. 84 p. [In Ukrainian].

9. Kiberbezpeka i informatsiyna bezpeka. “Cyber security and information security”. ISO/IEC 27032 standard. URL: https://ua.ikmj.com/cybersecurity-and-information-security-iso-iec-27032/. (Date of Application: 12.09.2022) [In Ukrainian].

10. *Driukov V.* Upravlieniie intsydientami i sobytyyamy informatsionnoi biezopasnosti. “Information security incident and event management”. URL: https://safe-surf.ru/specialists/article/5236/611719/. (Date of Application: 11.09.2022) [In Russian].

UDC 343.973

Sakharova Olena,
Candidate of Juridical Sciences, Senior Research Officer, Head of the Department,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0002-9759-5324

ESSENCE AND CONTENT OF THE CYBER INCIDENT INVESTIGATION PROCEDURE IN ACCORDANCE WITH ISO AND NIST INTERNATIONAL STANDARDS

The article reveals the essence and content of the procedure for investigating cyber incidents in accordance with the international standards ISO and NIST. In particular, according to ISO/IEC 27042:2015, the author provides a definition of the concept of “investigation of cyber incidents” and provides the stages of the procedure for investigating a cyber incident. The article systematically analyzes the content of an intelligent decision support system for managing cyber incidents. At the same time, the author focuses on the fact that the system of cyber protection measures should be based on regulatory documents, national and international standards, established practices for protecting information and ensuring cyber security, which develop along with cyber security technologies.

The analysis of the organizational and technical model of cyber defense, the identification and investigation of cyber incidents and cyber crimes, based on international risk-oriented cyber security management standards: ISO/IEC 27032: 2012 “Information technology. Security techniques. Guidelines for cybersecurity”, ISO/IEC 27037:2012 “Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence”, ISO/IEC 27041:2015 “Guidance on assuring suitability and adequacy of incident investigative method”, ISO/IEC 27043:2015 “Information technology. Security techniques. Incident investigation principles and processes”, Recommendations of the International Telecommunication Union MCE-T X.1216 (09/2020) “Requirements for the collection and preservation of evidence of cybersecurity incidents”.

In the process of conducting the study, the author also emphasizes that the international standard NIST SP 800-61 “Computer security incident handling guide”

presents a collection of “best practices” for building processes for processing, managing and responding to cyber incidents.

At the end of the article, the author comes to the conclusion that today in Ukraine a number of regulatory documents on the technical protection of information (ND TZI), as well as on a comprehensive system of information protection, are obsolete and have proven to be ineffective for many years, so it is advisable to introduce an information management system security in accordance with the ISO/ IEC 27000 series of standards, which allows you to optimize the process of protecting information resources and managing risks for these resources.

Keywords: cyber incidents, ISO and NIST international standards, cyber incident investigation, cyber attacks, cyber crimes, cyber incident investigation procedure.

Отримано 10.10.2022