КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.699
УДК 004.77

Козачок Валерій Анатолійович
к.т.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Драпатий Михайло Васильович
аспірант кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0002-1247-6180
m.drapatyi.asp@kubg.edu.ua

АНАЛІЗ ТЕХНОЛОГІЇ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Ця стаття спрямована на аналіз та огляд сучасних технологій, що використовуються при розслідуванні інцидентів безпеки на об'єктах критичної інфраструктури. Дослідження та впровадження новітніх стратегій та підходів у цій області може сприяти підвищенню рівня захисту важливих систем, а також виявленню та реагуванню на нові кіберзагрози, зберігаючи надійність функціонування суспільства в цілому. На сьогодні актуальним питанням безпекової галузі є спрямування на стан інформаційної безпеки об'єктів критичної інфраструктури з ефективним застосуванням відповідних заходів щодо підтримання її в належному стані. Інформаційний простір, ресурси, інфраструктура та технології, значною мірою впливають на рівень потенціалу держави та її збройних сил. Сьогодні, як ніколи, інформаційна компонента в стратегії забезпечення національної та воєнної безпеки держави вийшла на перший план [1], [2]. Вивчення та впровадження технологічних тенденцій кіберзахисту у секторі критичної інфраструктури дозволяє реагувати на складність сучасних кіберзагроз та забезпечує підвищення захищеності систем у реальному часі.

Ключові слова: об'єкт критичної інфраструктури; кібербезпека; кіберзахист; інциденти безпеки; розслідування інцидентів безпеки; управління інцидентами інформаційної безпеки; групи реагування на інциденти інформаційної безпеки, інструменти розслідування інцидентів безпеки.

ВСТУП

Темпи розвитку глобальної інформаційної інфраструктури на основі сучасних інформаційних технологій є підґрунтям того, що на сьогодні, як елементи національної критичної інфраструктури так і інші бізнес утворення з різними формами власності стають об'єктами деструктивних впливів злочинних та різноманітних терористичних угруповань.

Приклади багатьох країн світу (США, країни ЄС, Південна Корея тощо) з розвиненою інформаційною інфраструктурою свідчать про значне збільшення залежності соціально-економічної стабільності, національної безпеки, інформаційної та кібербезпеки загалом від рівня захищеності інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Одним із важливіших завдань є розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян у сфері інформаційної безпеки.

Об’єкти інформаційної діяльності та їх інформаційні системи все частіше стикаються з різними загрозами безпеки такими як шпигунство, комп’ютерне шахрайство та ін. Такі джерела збитку, як комп’ютерні віруси, комп’ютерний злом і атаки типу відмови в обслуговуванні, стають поширенішими, агресивнішими та все більш витонченішими.

Залежність від інформаційних систем і послуг означає, що елементи національної критичної інфраструктури та інші бізнес утворення, стають все більш уразливими по відношенню до загроз безпеки.

Зважаючи на значущість кібербезпеки в сучасному світі, об’єкти критичної інфраструктури стають особливою мішенню для кіберзлочинців та кіберзагроз. Ці об’єкти включають енергетичні системи, транспорт, комунікаційні мережі, медичні установи та інші важливі сектори, які забезпечують необхідність функціонування суспільства.

Критично важливими об’єктами (далі — об’єктами критичної інфраструктури) згідно з [3] є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

Напади на критичну інфраструктуру можуть мати серйозні наслідки, зокрема призвести до перерв у постачанні послуг, втрати конфіденційності даних або навіть загрожувати життю людей. У зв’язку з постійним розвитком технологій та зростанням кількості кіберзагроз, захист критичної інфраструктури стає надзвичайно важливим завданням.

Дослідження методів підвищення кіберзахисту на об’єктах критичної інфраструктури стає запорукою розвитку стратегій та технологій, які спрямовані на запобігання та захист від кібератак.

Постановка проблеми. В наш час активно зростають загрози кібербезпеці об’єктам критичної інфраструктури (ОКІ) та виникає потреба в інноваційних підходах до захису.

ОКІ є ключовими компонентами суспільства, такими як енергетика, транспорт, медичні установи, телекомунікації тощо. Ці сектори є особливо вразливими перед кіберзагрозами через залежність суспільства від їхньої неперервної роботи.

Небезпека зловживання кібератаками на ОКІ постійно зростає через швидкі темпи цифровізації та підключення до мереж Інтернету. Технічні прогреси у кіберзлочинності стають все більш складними та виразними, і це вимагає надзвичайно інноваційних підходів до кіберзахисту.

Одним із основних аспектів, який слід розглядати при розробці інноваційних підходів до захисту ОКІ від кіберзагроз є своєчасне та якісне проведення розслідувань інцидентів безпеки з метою унеможливлення їх повторення.

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

В авторській колективній роботі [4] розглянута діяльність спрямована на зниження ризиків кібербезпеки і включає циклічний процес управління, що складається з п’яти функцій: ідентифікації ризиків, кіберзахисту, виявлення кіберінцидентів, реагування та відновлення стану кібербезпеки. Описано, як кожна функція сприяє ефективному

управлінню ризиками та забезпечує надійність та безпеку ОКІ. Також в роботі запропоновані методи часткових показників ефективності.

В роботі [5] розглянуто моделі захисту критичної інформаційної інфраструктури, етапи і методи збору даних при виборі моделі захисту, розглянуті рівні забезпечення інформаційної інфраструктури та їх взаємодія, визначена структура моделювання процесу формування загроз та їх життєвий цикл. Автори статті зазначають, що безпека, базована на використанні формалізованих моделей, дозволяє уникнути помилок у розробці. Однак, вони також наголошують на необхідності періодичного перегляду моделей для максимальної адаптації до змін у завданнях та умовах, що виникають з часом.

В роботі [6] розроблена програмна реалізація та експериментальне дослідження системи корелювання подій та управління інцидентами кібербезпеки на ОКІ.

В роботі [7] проаналізовані сучасні підходи, що використовуються для забезпечення кібербезпеки в контексті критичної інфраструктури. Дослідження і впровадження новітніх стратегій та підходів у цій області може сприяти реагуванню на нові кіберзагрози, зберігаючи надійність та функціонування суспільства в цілому підвищенню рівня захисту важливих інформаційних систем.

Відсутність в українських наукових фахових виданнях обговорення результатів зарубіжних наукових досліджень, а також нормативно-правової бази з питань організації та проведення розслідування інцидентів безпеки на ОКІ є підставою для проведення власних досліджень.

Загалом, робота підкреслює проблеми захисту інформації та важливість поєднання традиційних та інноваційних підходів для ефективного управління інформаційною безпекою.

Мета статті полягає у аналізі та огляді інновацій та сучасних підходів, що використовуються для забезпечення кібербезпеки в контексті розслідування інцидентів безпеки на ОКІ.

Дослідження і впровадження новітніх стратегій та підходів у цій області може сприяти реагуванню на нові кіберзагрози, зберігаючи надійність та функціонування суспільства в цілому підвищенню рівня захисту важливих інформаційних систем.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасне суспільство, отримавши в результаті розвитку інформаційних і комунікаційних технологій небачені досі можливості в галузі обміну інформацією, стало надзвичайно вразливим щодо стороннього шкідливого кібернетичного впливу та різних видів загроз.

Мережа Інтернет надала міжнародним терористам зручне для злочинної діяльності середовище, в якому частота і складність кібератак постійно зростають, а кібертероризм починає використовуватися у міждержавних стосунках та світовій політиці.

Міжнародний кібертероризм неможливий без підтримки і координації дій з боку агресивних держав. Кібератаки здійснюються здебільшого під керівництвом спецорганів недружніх держав і спроможні без використання традиційних видів озброєння нанести атакованій державі безповоротних втрат.

Жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки (ІБ), будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно

несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасних підприємств зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз ІБ. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

В стандарті ISO/IEC TR 18044 [8] для досягнення мети управління інцидентами ІБ використовується циклічна модель PDCA. Дана модель передбачає чотири окремих етапи управління: планування, експлуатація, аналіз і покращення процесу.

Одним із ключових процесів на етапі експлуатації є розслідування інцидентів. Перш ніж перейти до розкриття процесу розслідування інцидентів безпеки, проаналізуємо сутність поняття інциденту інформаційної безпеки.

Інцидентом кібербезпеки [3] називають подію або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Графічна інтерпретація поняття інциденту ІБ наведено на рис. 1.

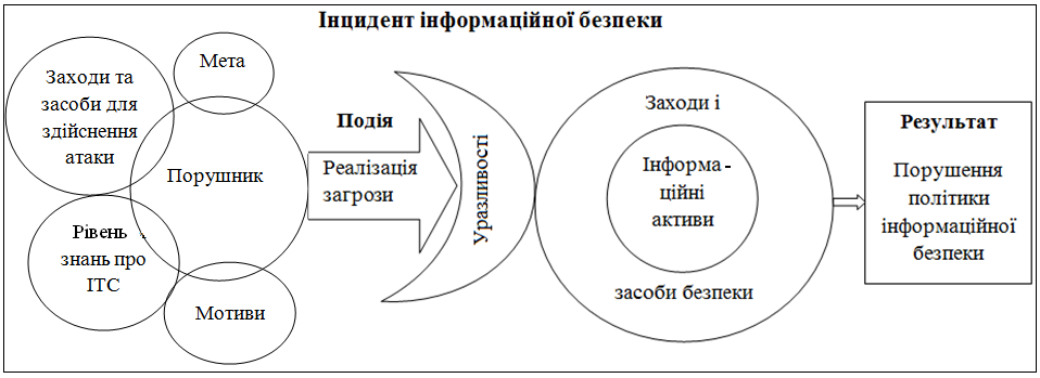

Рис. 1. Модель інциденту ІБ

Для зменшення ризику нанесення збитків, пов'язаних з інцидентами ІБ бажано використовувати як організаційні заходи так і програмно-апаратні засоби розслідування інцидентів ІБ.

Розслідування інцидентів ІБ включає:

- підтвердження факту настання інциденту (чи не є даний інцидент результатом невизначених чинників — природних умов або катастроф);
- збір доказів по інциденту та визначення причин інциденту;
- об'єкту (інформація відкрита або з обмеженим доступом) та/або суб'єкту (співробітник фірми, клієнт і т. ін.), проти якого спрямовано інцидент;
- місця та часу інциденту; засобів та заходів для здійснення атаки;
- розміру збитків;
- порушника або групи порушників, а також, осіб, які знали про наміри порушників й намагалися приховати сліди інциденту;
- мети порушення;

– причин, що могли послугувати для успішної реалізації атаки;
– відповідних дисциплінарних стягнень.

Процес розслідування інцидентів ІБ прийнято [9] ділити на чотири етапи: збір, дослідження, аналіз і відображення.

До організаційних заходів розслідування інцидентів ІБ входить створення та налагодження роботи спеціальних груп реагування на інциденти.

Для успішного розслідування інцидентів ІБ важлива швидкість і організованість дій груп реагування на інциденти.

В перше була створена група реагування - команда CERT/CC (CERT Coordination Center) [10], що виникла в 1988 році як Computer Security Incident Response Team (група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує у складі Інституту розробки програмного забезпечення при Університеті Карнегі — Меллона (Software Engineering Institute, Carnegie Mellon University) і фінансується урядом США. Починався цей проект з ініціативи студентів та викладачів університету (у відповідь на перше глобальне поширення шкідливого програмного забезпечення під назвою «Хробак Моріса») і дуже швидко перетворився спочатку в проект національного, а незабаром і міжнародного масштабу.

Окрім проведення незалежних досліджень та виконання різноманітних завдань щодо забезпечення безпеки глобальної інформаційної інфраструктури, ця організація здійснює централізований збір відомостей про всі уразливості в різних інформаційних системах і підтримку бази знань про такі уразливості в актуальному стані. Відомості про щойно виявлені уразливості, шкідливі програми і способи порушення ІБ розсилаються електронною поштою у вигляді бюлетеню.

CERT/CC здійснює постійну дослідницьку роботу щодо:

– визначення характеру можливих наслідків використання виявлених уразливостей і вірусів;
– аналізу наявних засобів використання уразливостей;
– аналізу того, наскільки активно використовуються уразливості і наскільки широко поширені віруси;
– взаємодії з постачальниками інформаційних систем з метою більш глибокого аналізу виявлення уразливостей.

На основі проведеного аналізу CERT/CC розробляє заходи щодо усунення уразливостей і рекомендації щодо зменшення негативних наслідків. За результатами цієї роботи всім передплатникам розсилається інформація про загрози ІБ і можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова й технічна документація, проводиться подальша дослідницька і методична робота. Зокрема, CERT/CC підтримує програму безпечної розробки програмного забезпечення («Secure Coding»), що ґрунтується на тому, що більша частина уразливостей виникає внаслідок відносно невеликого числа помилок у програмному коді інформаційних систем. Таким чином, CERT/CC на основі накопичених результатів аналізу уразливостей проводить цілеспрямовану роботу з виявлення типових програмних помилок, вироблення стандартів безпечного програмування та поширення цієї інформації серед розробників програмного забезпечення.

Крім основної інформаційної роботи з уразливостями, CERT/CC також займається супутніми видами діяльності:

– організацією навчальних курсів з різних напрямків (мережевої безпеки, управління інформаційними ризиками, організації роботи груп реагування);
– сертифікацією фахівців з реагування на інциденти у сфері ІБ;

– підтримкою фундаментальних наукових досліджень у різних галузях ІБ, таких як методи розробки безпечних додатків, виявлення уразливостей, аналіз шпигунського програмного забезпечення, вирішення питань безпеки як складова частина процесу розробки тощо;
– сприяння розвитку локальних (національних і корпоративних) груп реагування на інциденти.

З огляду на те, що CERT — торгова марка, яка захищена законодавством США, у світовій практиці прийнято вживати для позначення груп реагування на інциденти назву **CERT/CSIRT** (Computer Emergency Response Team / Computer Security Incident Response Team).

CSIRT — група реагування на інциденти комп'ютерної безпеки ДержНДІ технологій кібербезпеки, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. Основним функціональним напрямом діяльності CSIRT є забезпечення протидії кіберзагрозам в автоматизованих системах та інформаційно-комунікаційних системах ДержНДІ технологій кібербезпеки та підприємств енергетичної галузі [11].

CSIRT — є позаштатною структурною одиницею ДержНДІ технологій кібербезпеки, яка взаємодіє із з командами CERT-UA, Системою виявлення вразливостей і реагування на кіберінцеденти та кібератаки, зовнішніми організаціями та іншими суб'єктами національної системи кібербезпеки.

Завдання CSIRT:

- накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;
- надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;
- організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;
- взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;
- взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;
- взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;
- опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;
- сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Таким чином, функціонування груп CERT/CSIRT можуть надати такі переваги своїм клієнтам:

- централізовану координацію питань, пов'язаних з ІБ всередині організації;
- спеціалізовану та централізовану систему обробки повідомлень про інцидентів ІБ і своєчасне реагування на них;
- надання експертизи і підтримки в процесі відновлення після впливу інцидентів ІБ;
- забезпечення юридичної допомоги та взаємодії з відповідними правоохоронними органами і службами з метою ефективного розслідування інцидентів ІБ (зокрема, підтримку у судових процесах);
- відслідковування як методів і способів порушення ІБ, так і сучасних методів та засобів захисту інформаційних систем;
- стимулювання партнерів і клієнтів до спільної взаємодії та розвитку у сфері забезпечення ІБ;
- збирання статистики, яка буде корисною для розробки, впровадження та удосконалення систем захисту інформації тощо.

На сьогодні у світі функціонує розвинута мережа структур швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів, які мають назви CERT або CSIRT. На даний момент існують різні типи груп реагування на інциденти ІБ. Одні забезпечують безпеку Інтернет — координаційний центр CERT (Computer Emergency Response Team, http://www.cert.org), інші — вузько направлені (наприклад, корпоративні групи реагування). Перелік найбільш відомих груп можна знайти на всесвітньому форумі FIRST (Forum of Incident Response and Security Teams, http://www.first.org/).

Координацію діяльності таких структур на міжнародному рівні здійснює міжнародна організація Форум груп реагування на інциденти і забезпечення безпеки (Forum of Incident Response and Security Teams, FIRST), яка об'єднує зусилля різних груп реагування на інциденти ІБ. На сайті FIRST (http://www.first.org) можна знайти повний список її учасників.

Зауважимо, що в разі вчинення дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також на ОКІ слід звертатися до спеціалізованого підрозділу Держспецзв'язку Computer Emergency Response Team of Ukraine (CERT-UA, www.cert.gov.ua), який у 2009 році отримав статус повноцінного члена FIRST (Full Member).

CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України [12]. З 2009 року є акредитованим членом Форуму команд реагування на інциденти безпеки FIRST.

Завдання CERT-UA:

- накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;
- надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;
- організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

- взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;
- взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;
- взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;
- опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;
- сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

У процесі аналізу інциденту команда реагування повинна мати доступ до всіх необхідних для аналізу ресурсів інформаційної системи, таких як: засоби перегляду стану портів операційного середовища; свідчення роботи операційних систем, застосунків, протоколів, систем виявлення вторгнень, сигнатур антивірусів; засоби перегляду статистичних журналів роботи мережі найбільш критичних пристроїв (веб-серверів, серверів електронної пошти, протоколів роботи FTP-серверів); засоби перегляду журналів активності застосунків; журнали криптографічних засобів; операційні системи (для аналізу журнальних файлів, зокрема з правами адміністратора); дані про завантаження оновлень в операційних середовищах; інформація про регламент резервного копіювання та тестування резервних носіїв.

До таких засобів необхідно також додати ПЗ і апаратні засоби збору даних:

- комп'ютерну систему для зберігання свідчень розслідування інцидентів;
- мобільні комп'ютери для зручності роботи команди розслідування інцидентів;
- випробувальну лабораторію для аналізу можливого розвитку інциденту;
- комплекти чистих CD і DVD носіїв;
- принтери;
- ПЗ для аналізу стану дискової підсистеми;
- сніфери й аналізатори протоколів для аналізу мережевого трафіку;
- завантажувальні диски всіх використовуваних в організації операційних середовищ;
- супутні пристрої, такі як диктофони, цифрові фото та відеокамери для збору доказової бази в процесі розслідування.

Що стосується програмної складової процесу розслідування інцидентів ІБ, то на даний час існує велика кількість програмних комплексів які використовуються при проведенні розслідування інцидентів безпеки в інформаційно-комунікаційних системах.

Для проведення розслідування інцидентів, як правило, користуються:

- спеціалізованими операційними системами для проведення розслідування — DEFT Linux, FCCU GNU/Linux Forensic Boot CD, Helix3;
- публічними пошуковими системами;
- засобами клонування жорстких дисків та інших носіїв;

- спеціалізованими програмними засобами для проведення розслідування та управління інцидентами інформаційної безпеки;
- наборами хешів для фільтрації вмісту досліджуваної файлової системи;
- програмними засобами для дослідження локальних обчислювальних мереж — сніфери, DLP-системи, IRM-системи;
- утилітами створення контрольних сум та цифрових підписів файлів та інші.

Наведемо приклади декількох програмних комплексів [13] – [22].

Autopsy — це платформа цифрової криміналістики і графічний інтерфейс для Sleuth Kit і інших цифрових криміналістичних інструментів. Вона використовується правоохоронними органами, військовими і корпоративними експертами для розслідування того, що сталося на комп'ютерах.

Autopsy була створена самодостатньою платформою з модулями, які поставляються і доступні зі сторонніх джерел. Деякі з цих модулів забезпечують:

- **Timeline Analysis** (аналіз активності за часом) — високого рівня інтерфейс графічного представлення активності в досліджуваній системі.
- **Hash Filtering** (фільтрація по Хешам) — позначає файли, про які відомо, що вони погані, і ігнорує хороші файли.
- **Keyword Search** (пошук за ключовими словами) — індексований пошук за ключовими словами для пошуку файлів, які згадують релевантні терміни.
- **Web Artifacts** (веб артефакти) — витягує історію, закладки та кукіз з Firefox, Chrome і IE.
- **Data Carving** (вишкрібання даних) — відновлення видалених файлів з НЕ розподіленого простору з використанням PhotoRec
- **Multimedia** (мультимедіа) — Витягує EXIF з картинок і перегляд відео.
- **Indicators of Compromise** (індикатори компрометації) — Сканує комп'ютер з використанням STIX.

Autopsy запускає фонові завдання паралельно, використовуючи безліч ядер і виводить результати відразу після їх виявлення.

Autopsy безкоштовна. Якщо бюджет урізають, без економічно ефективних цифрових криміналістичних інструментів не обійтися. Autopsy пропонує ті ж основні функції, що й інші інструменти для цифрової криміналістики, а також пропонує інші основні функції, такі як аналіз веб артефактів і аналіз регістра, які відсутні в інших комерційних інструментах.

Список можливостей Autopsy:

- Розраховані на багато користувачів кейси.
- Аналіз активності за часом: показ системних подій в графічному інтерфейсі для допомоги в ідентифікації активності.
- Пошук за ключовими словами: витяг тексту і модулі індексного пошуку дають можливість знайти файли, які згадують специфічні терміни.
- Веб артефакти: витяг веб активності з популярних браузерів для допомоги в ідентифікації користувача активності.
- Аналіз реєстру: використовується RegRipper для ідентифікації доступу до останніх документів і USB пристроїв.
- Аналіз файлів LNK: визначає ярлики і відкриті документи.
- Аналіз електронної пошти: розбір повідомлень в форматі MBOX, таким як Thunderbird.
- EXIF: витягує інформацію про геолокації і камери з файлів JPEG.

- Сортування за типами файлів: угруповання файлів по їх типу для пошуку всіх зображень або документів.
- Відтворення медіа: переглядайте відео та зображень в додатку, зовнішній переглядач не потрібно.
- Перегляд мініатюр: показ мініатюрних зображень для допомоги в швидкому огляді картинок.
- Надійний аналіз файлової системи: підтримка популярних файлових систем, включаючи NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2 і UFS з The Sleuth Kit.
- Фільтрація файлів по Хешам: відфільтровування добре відомих файлів з використанням NSRL і позначка поганих файлів, використовуючи призначені для користувача наборі хешів в форматах HashKeeper, md5sum і EnCase.
- Теги: позначає файли тегами, з довільними іменами тегів, такими як «закладки», «підозрілі» та додавайте коментарі.
- Визначення типу файлу на основі сигнатур і виявлення невідповідності розширення файлу його вмісту.
- Модуль цікавих файлів позначає файли і папки, грунтуючись на імені і шляхи.
- Підтримка Android: витяг даних з SMS, журналу дзвінків, контактів, Tango, Words with Friends та інших.

Autopsy аналізує образи дисків, локальні диски або папки з локальними файлами. Образи дисків можуть бути як в сирому/dd, так і в E01 форматі. Підтримка E01 забезпечується libewf.

Autopsy дозволяє створювати дослідникам додаткові типи звітів. Під замовчуванням доступні звіти в файлах HTML, XLS і Body.

Слідчі можуть згенерувати більш ніж один звіт за раз, а також редагувати існуючі або створювати нові модулі для настройки поведінки під їх специфічні потреби.

Encrypted Disk Detector — це безкоштовна програма для операційної системи Microsoft Windows, яку можна запускати в системі для пошуку зашифрованих томів. Додаток може виявити зашифровані томи TrueCrypt, PGP, Safeboot та Bitlocker.

Encrypted Disk Detector корисний під час реагування на інцидент для швидкої та ненав’язливої перевірки зашифрованих томів у комп’ютерній системі.

Програмне забезпечення спочатку перевіряє фізичні диски, перш ніж перейти на логічні томи в системі. Потенційно зашифровані томи підсвічуються ним безпосередньо.

Encrypted Disk Detector був протестований на Windows XP та Windows Vista. Він працює нормально на сервері Windows 2000/2003.

Wireshark (раніше — Ethereal) — програма-аналізатор трафіку для комп’ютерних мереж Ethernet і деяких інших. Має графічний користувальницький інтерфейс. У червні 2006 року проект був перейменований в Wireshark через проблеми з торговою маркою.

Програма дозволяє користувачеві переглядати весь трафік в режимі реального часу.

Існують версії для більшості типів системи UNIX, в тому числі Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Windows.

Wireshark — це додаток, який «знає» структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Wireshark уміє працювати з безліччю форматів вхідних даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

Wireshark — це передовий і широко використовуваний аналізатор мережевих протоколів. Це дозволяє бачити, що відбувається у мережі, на мікроскопічному рівні і є

фактичним (і часто де-юре) стандартом для багатьох комерційних та некомерційних підприємств, державних установ та освітніх установ.

Wireshark має багатий набір функцій, який включає в себе наступне:

- глибока перевірка сотень протоколів, причому постійно додається більше;
- захоплення в режимі реального часу та офлайн-аналіз;
- стандартний трипанельний браузер пакетів;
- мультиплатформа працює на Windows, Linux, macOS, Solaris, FreeBSD, NetBSD та багатьох інших;
- захоплені мережеві дані можна переглядати за допомогою графічного інтерфейсу користувача або за допомогою утиліти TShark в режимі TTY;
- найпотужніші фільтри дисплея;
- розширений VoIP-аналіз;
- читання/запис багатьох різних форматів файлів захоплення: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (стислий і нестиснутий), Sniffer® Pro та NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek та багато інших;
- файли захоплення, стиснуті за допомогою gzip, можна декомпресувати на льоту;
- дані в реальному часі можна читати з Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI та інших;
- підтримка розшифровки багатьох протоколів, включаючи IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP та WPA/WPA2;
- правила забарвлення можна застосувати до списку пакетів для швидкого, інтуїтивного аналізу;
- вихідні дані можна експортувати у XML, PostScript®, CSV або звичайний текст.

MAGNET RAM Capture — це безкоштовний інструмент візуалізації, призначений для захоплення фізичної пам’яті комп’ютера підозрюваного, що дозволяє слідчим відновити та проаналізувати цінні артефакти, які часто знаходяться лише в пам’яті.

Інструмент має невеликий розмір пам’яті, що означає, що слідчі можуть запустити інструмент, мінімізуючи дані, перезаписані в пам’ять. Є можливість експортувати захоплені дані пам’яті у форматі RAW (.DMP/.RAW/.BIN) та легко завантажувати їх у провідні інструменти аналізу, включаючи Magnet AXIOM та Magnet IEF.

Докази, які можна знайти в оперативній пам’яті, включають процеси та програми, що працюють у системі, мережеві підключення, докази вторгнення шкідливого програмного забезпечення, вулики реєстру, імена користувачів та паролі, розшифровані файли та ключі та докази діяльності, які зазвичай не зберігаються на локальному жорсткому диску.

Magnet RAM Capture підтримує системи Windows, включаючи XP, Vista, 7, 8, 10, 2003, 2008 та 2012 рр. Magnet RAM Capture має приємний та простий графічний інтерфейс, тому запустити його дуже просто. Він створює дамп необробленої пам’яті з .DMP розширенням.

Оскільки пам’ять, зібрана утилітою, зберігається у форматі необроблених даних, її можна проаналізувати за допомогою більшості інструментів аналізу пам’яті та криміналістичних інструментів, включаючи IEF, Volatility та Mandiant Redline.

Фізична пам’ять зберігає велику кількість інформації, і захоплення пам’яті з живої системи має бути частиною робочого процесу будь-якого слідчого. Незалежно від того, чи працюєте ви над зараженням шкідливим програмним забезпеченням, інцидентом із вторгненням чи викраденням IP, у пам’яті обов’язково знайдуться докази, які можуть бути життєво важливими для вашого розслідування.

NetworkMiner — це інструмент судово-аналітичного аналізу мережі (NFAT) з відкритим кодом для Windows (але також працює в Linux/Mac OS X/FreeBSD). NetworkMiner може бути використаний як пасивний інструмент зчитування/захоплення пакетів мережі для виявлення операційних систем, сеансів, імен хостів, відкритих портів тощо, не передаючи жодного трафіку в мережу. NetworkMiner також може аналізувати файли PCAP для офлайн-аналізу та регенерувати/збирати передані файли та сертифікати з файлів PCAP.

NetworkMiner дозволяє легко виконувати вдосконалений аналіз мережевого трафіку (NTA), забезпечуючи вилучені артефакти в інтуїтивно зрозумілому користувацькому інтерфейсі. Спосіб подання даних не тільки спрощує аналіз, але й економить дорогоцінний час для аналітика або судового слідчого.

З моменту першого випуску в 2007 році NetworkMiner став популярним інструментом серед команд реагування на інциденти, а також правоохоронних органів.

NetworkMiner може витягувати файли, електронні листи та сертифікати, передані через мережу, шляхом аналізу файлу PCAP або шляхом аналізу трафіку безпосередньо з мережі.

Ще однією дуже корисною функцією є те, що користувач може шукати проаналізовані або збережені дані за ключовими словами. NetworkMiner дозволяє користувачеві вставити довільний рядок чи шаблони байтів, які слід шукати за допомогою функції пошуку за ключовими словами.

Утиліта пасивно аналізує дамп з трафіком, безпомилково визначає учасників обміну мережевими даними і розпізнає операційні системи, встановлені на кожному хості, за розміром вікна, часу життя пакета і унікальному набору прапорів.

NetworkMiner також може видавати структуровану інформацію про відкриті сесії, активні порти і іншої інфраструктури мережі, знімає банери різних демонів.

Найважливіша особливість даного аналізатора трафіку це можливість витягувати файли і сертифікати, що передаються по мережі. Ця функція може бути використана для перехоплення і збереження всіляких аудіо- і відео-файлів.

Nmap («Картограф мережі») — це безкоштовний і відкритий код (ліцензія) утиліта для виявлення мережі та аудиту безпеки.

Nmap — це скорочення від Network Mapper. Це інструмент командного рядка з відкритим кодом Linux, який використовується для сканування IP-адрес та портів у мережі та виявлення встановлених програм.

Nmap дозволяє адміністраторам мережі знаходити, які пристрої працюють у їх мережі, виявляти відкриті порти та служби та виявляти вразливості.

Багато системних та мережевих адміністраторів також вважають це корисним для таких завдань, як інвентаризація мережі, управління графіками оновлення служби та моніторинг часу роботи хосту чи служби. Nmap використовує необроблені IP-пакети новими способами, щоб визначити, які хости доступні в мережі, які послуги (ім’я та версія програми) пропонують ці хости, які операційні системи (та версії ОС) працюють, який тип фільтрів пакетів/брандмауерів використовуються, і десятки інших характеристик.

Він був розроблений для швидкого сканування великих мереж, але чудово працює проти окремих хостів. Nmap працює на всіх основних комп'ютерних операційних системах, а офіційні двійкові пакети доступні для Linux, Windows та Mac OS X.

Nmap був визнаний «Продуктом безпеки року» за версією Linux Journal, Info World, Linux Questions.Org та Codetalker Digest. Він навіть був представлений у дванадцяти фільмах, серед яких «Перезавантажена матриця», «Померти важко 4», «Дівчина з татуюванням дракона» та «Ультиматум Борна».

Nmap це гнучкий комплекс який підтримує десятки вдосконалених методів відображення мереж, заповнених IP-фільтрами, брандмауерами, маршрутизаторами та іншими перешкодами. Це включає в себе безліч сканування портів механізмів (як TCP і UDP), ОС виявлення, визначення версії, пінг зачисток, і багато іншого.

Nmap підтримується більшістю операційних систем, включаючи Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga тощо.

Nmap, безсумнівно, є «швейцарським армійським ножем» мереж завдяки своєму інвентарю різноманітних команд.

Це дозволяє швидко сканувати та знаходити важливу інформацію про мережу, хости, порти, брандмауери та операційні системи.

Nmap має численні налаштування, які допомагають системним адміністраторам детально аналізувати мережу.

Belkasoft Live RAM Capturer — це крихітний безкоштовний криміналістичний інструмент, який дозволяє надійно витягати весь вміст енергонезалежної пам'яті комп'ютера, навіть якщо він захищений активною системою боротьби з налагодженням чи антидемпінгом. Доступні окремі 32-розрядні та 64-розрядні збірки, щоб максимально мінімізувати розмір інструменту. Дампи пам'яті, зафіксовані за допомогою Belkasoft Live RAM Capturer, можна проаналізувати за допомогою Live RAM Analysis в Belkasoft Evidence Center. Belkasoft Live RAM Capturer сумісний з усіма версіями та версіями Windows, включаючи XP, Vista, Windows 7, 8 та 10, 2003 та 2008 Server.

Звалища пам'яті є цінним джерелом ефемерних доказів та нестабільної інформації. Дампи пам'яті можуть містити паролі до зашифрованих томів (TrueCrypt, BitLocker, PGP Disk), облікові дані для входу в обліковий запис для багатьох веб-пошти та служб соціальних мереж, таких як Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; служби обміну файлами, такі як Dropbox, Flickr, SkyDrive тощо.

Для того, щоб витягти ефемерні докази з уже захоплених звалищ пам'яті, судові експерти повинні використовувати належне програмне забезпечення для аналізу, таке як Belkasoft Evidence Center. Крім того, деякі інші інструменти можна використовувати для вилучення паролів до зашифрованих томів.

Отримати енергонезалежну пам'ять із комп'ютера, на якому встановлено систему захисту від налагодження чи антидемпінгову систему, досить складно. Більшість засобів збору пам'яті працюють у режимі користувача системи і не можуть обійти захист такої системи захисту (які працюють у найбільш привілейованому режимі ядра системи).

Belkasoft Live RAM Capturer розроблений для коректної роботи, навіть якщо працює агресивна система боротьби з налагодженням чи звантаження пам'яті. Працюючи в режимі ядра, Belkasoft Live RAM Capturer грає на одному рівні з цими системами захисту, маючи можливість правильно отримувати адресний простір програм, захищених найсучаснішими системами, такими як nProtect GameGuard.

Belkasoft Live RAM Capturer має найменший можливий розмір, не вимагає встановлення і може бути запущений за лічені секунди з флеш-накопичувача USB. На

відміну від багатьох конкуруючих інструментів, що працюють в режимі користувача системи, Belkasoft Live RAM Capturer постачається з 32-розрядними та 64-розрядними драйверами ядра, що дозволяє інструменту працювати в найбільш привілейованому режимі ядра. Дампи пам'яті, придбані за допомогою Belkasoft Live RAM Capturer, можуть бути проаналізовані за допомогою аналізу оперативної пам'яті Belkasoft Evidence Center.

Belkasoft Live RAM Capturer перевершує багато популярних програм для збору пам'яті через різницю в цілях дизайну. Поточні версії конкуруючих інструментів (AccessData FTK Imager 3.0.0.1443, PMDump 1.2) працюють у користувацькому режимі системи, що робить їх сприйнятливими до антидемпінгових дій, що виконуються активними системами захисту від налагодження, такими як nProtect GameGuard.

HashMyFiles — це невелика утиліта, яка дозволяє розрахувати хеші MD5 і SHA1 одного або декількох файлів у системі. Існує можливість легко скопіювати хеш-список MD5/SHA1 у буфер обміну або зберегти їх у текстовому/html/xml-файлі.

HashMyFiles також можна запустити з контекстного меню Провідника Windows і відобразити хеші MD5/SHA1 вибраного файлу або папки.

Ця утиліта працює на Windows 2000/XP/2003/Vista/Windows 7/Windows 8/Windows 10.

HashMyFiles не вимагає жодного процесу встановлення або додаткових файлів DLL. Для того, щоб почати його використовувати, необхідно просто запустити виконуваний файл (HashMyFiles.exe) Після його запуску можна додавати файли та папки, які необхідно переглянути їх хеші MD5/SHA1.

HashMyFiles також можна використовувати безпосередньо з Провідника Windows. Якщо запустити опцію HashMyFiles для папки, вона відобразить хеші для всіх файлів у вибраній папці. Якщо запустити параметр HashMyFiles для одного файлу, він відображатиме лише хеші для цього файлу.

Crowd Response — це автоматизований інструмент, який дозволяє збирати системну інформацію для реагування на інциденти та заходи безпеки. Цей інструмент може охоплювати операційну систему на базі Windows або MAC OSX.

Інформація, яку можна зібрати за допомогою цієї утиліти:

- список каталогів, включаючи папки та підпапки;
- список користувачів;
- процес, який обробляє список;
- перелік усіх процесів;
- витягнути рядки з пам'яті запущених процесів;
- витягнути ключ реєстру та інформацію про значення;
- файли реєстру;
- сканування правил YARA.

Блокувальники запису USB

USB-накопичувач є загальним пристроєм, який команда з реагування на аварії використовуватиме для збору та розслідування будь-яких атак. USB включатиме ряд інструментів, необхідних для запуску та аналізу артефактів системи. Він також може містити журнали та звіти, які користувачеві потрібно редагувати, коли вони знову підключатимуться до своєї системи. Після того, як журнали та метадані зібрані, користувач повинен переконатися, що немає можливості змінити зібрану інформацію. Якщо є бажання заблокувати пристрій USB, є можливість скористатись утилітою блокування запису USB.

Orion USB Write Blocker — це програма, яка дозволяє користувачеві або ввімкнути захист від запису для всіх USB-пристроїв, підключених до комп'ютера, або повністю заблокувати USB-пристрої. Програма є портативною і не вимагає інсталяції. Ця утиліта випущена як безкоштовна.

Утиліта **DSi USB Write Blocker Utility** допоможе перетворити USB-накопичувач у режим лише для читання, тому жодні зміни та модифікації не дозволяються, що настає в кінці, коли збирається вся інформація.

Інструмент підтримується у більшості операційних систем Windows, і за допомогою опції сумісності є можливість зробити його запущеним на найновішій ОС.

Цей інструмент дозволить проводити збір інформації, не зачіпаючи та не пошкоджуючи дані.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розкриття сутності поняття інцидента інформаційної безпеки дозволяє відтворити образ потенційного порушника, зрозуміти причини та процес настання інциденту. Дана робота дозволить сформувати загальні представлення про процес розслідування інцидентів ІБ, хоча кожен із етапів процесу може стати в подальшому темою окремого дослідження.

Запровадження процесу розслідування інцидентів ІБ на ОКІ дозволить:

- підвищити рівень інформаційної безпеки;
- посилити увагу до попередження інцидентів шляхом віднаходження винних у його виникненні та його причин;
- знизити негативні наслідки на бізнес-процеси організації;
- дозволить скорегувати політику інформаційної безпеки ОКІ.

В Україні боротьбою з кібертероризмом на ОКІ займаються спеціалізовані підрозділи національної поліції, СБУ та Держспецзв'язку, які тісно співпрацюють з міжнародними підрозділами боротьби з кіберзлочинністю та провідними міжнародними компаніями в галузі ІТ і кібербезпеки. Активну позицію в боротьбі з кібертероризмом займає НАТО. Це проявляється в активізації його роботи з країнами-партнерами та створенні трастового фонду з кібербезпеки. Тісний контакт з правоохоронними органами європейських країн та партнерами в галузі кібернетичної безпеки підтримує Європол.

Однак, уникнути інцидентів у кібернетичному просторі неможливо. Оперативна реакція на прояви міжнародного кібертероризму та інтенсивність дослідження нових та очікуваних інцидентів з метою їх врахування у політиці безпеки залежать від наявності належних інвестицій та об'єднання зусиль світових організацій і компаній, які спеціалізуються у сфері кібернетичної безпеки.

Загрозу кібернетичній безпеці становлять як зовнішні, так і внутрішні інциденти. Безпека інформаційної системи значною мірою залежить від правильного підбору кадрів, вивчення ними основ соціального інжинірингу та неухильного дотримання вимог політики безпеки.

Ефективність боротьби з новими видами інцидентів у сфері міжнародної кібербезпеки залежить від залучення світовою спільнотою належних інвестицій та тісної співпраці національних і міжнародних правоохоронних органів з провідними компаніями у галузі інформаційних технологій та кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України", Указ Президента України № 287/2015 (2020) (Україна). https://zakon.rada.gov.ua/laws/show/287/2015#Text
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України № 447/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Хлапонін, Ю. І., Козубцова, Л. М., Козубцов, І. М., & Штонда, Р. М. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка, 3(15),* 124–134. https://doi.org/10.28925/2663-4023.2022.15.124134
5. Кожедуб, Ю., Василенко, С., Максимець, А., & Гирда, В. (2021). Концептуальна модель захисту інформації об'єктів критичної Інформаційної інфраструктури України. *Information Technology and Security, 9(2(17)),* 151–164.
6. Гнатюк, С. О., Бердибаєв, Р. Ш., Сидоренко, В. М., Жигаревич, О. К., & Смірнова Т. В. (2023). Система королювання подій та управління інцидентами інформаційної безпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка, 3(19),* 176–196. https://doi.org/10.28925/2663-4023.2023.19.176196
7. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич , І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22),* 156–167. https://doi.org/10.28925/2663-4023.2023.22.156167
8. Information security incident management (IDT). (2004). *Information technology - Security techniques* - (ISO/IEC TR 18044:2004).
9. Kent, K., Chevalier, S., Grance T., Dang H. (2006). *Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST).* https://doi.org/10.6028/NIST.SP.800-86
10. *CERT Coordination Center.* (б. д.). CERT Vulnerability Notes Database. https://www.kb.cert.org
11. *Про CSIRT.* (б. д.). CSIRT Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації. https://csirt.csi.cip.gov.ua/uk/pages/about-csirt
12. *CERT-UA.* (б. д.). https://cert.gov.ua/
13. *opsy | Digital Forensics.* (б. д.). Autopsy. https://www.autopsy.com/
14. *Wireshark · Go Deep.* (б. д.). Wireshark. https://www.wireshark.org/
15. *Magnet Forensics | Unlock the truth. Protect the innocent.* (б. д.). Magnet Forensics. https://www.magnetforensics.com/
16. *NETRESEC - Network Forensics and Network Security Monitoring*. (б. д.). Netresec. https://www.netresec.com/
17. *Nmap: the Network Mapper - Free Security Scanner.* (б. д.). https://nmap.org/
18. *Belkasoft: Intelligent Software for Digital Forensics and Cyber Incident Response*. (б. д.). https://belkasoft.com/
19. *HashMyFiles: Calculate MD5/SHA1/CRC32 hash of files*. (б. д.). NirSoft. https://www.nirsoft.net/utils/hash_my_files.html#google_vignette
20. **NEW* Community Tool: CrowdResponse*. (б. д.). CrowdStrike: We Stop Breaches with AI-native Cybersecurity. https://www.crowdstrike.com/en-us/blog/new-community-tool-crowdresponse/
21. *USB 3.1 WriteBlocker | WiebeTech*. (б. д.). WiebeTech | Digital Forensics. https://wiebetech.com/products/usb-3-1-writeblocker/
22. *DSi USB Write Blocker*. (2018). Hackercombat. https://www.hackercombat.com/digital-forensic-tools-availability-in-the-nutshell/dsi-usb-write-blocker/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Valerii Kozachok
PhD, Associate Professor, Associate Professor of the Department of
Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Mykhailo Drapatyi
PhD Student of the Department of Information and
Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0002-1247-6180
m.drapatyi.asp@kubg.edu.ua

ANALYSIS OF SECURITY INCIDENT INVESTIGATION TECHNOLOGI AT CRITICAL INFRASTRUCTURE FACILITIES

Abstract. This article aims to analyze and review modern technologies used in the investigation of security incidents at critical infrastructure facilities. Research and implementation of the latest strategies and approaches in this area can contribute to increasing the level of protection of important systems, as well as to the detection and response to new cyber threats, while maintaining the reliability of the functioning of society as a whole. Today, the urgent issue of the security industry is to address the state of information security of critical infrastructure objects with the effective application of appropriate measures to maintain it in proper condition. The information space, resources, infrastructure and technologies significantly affect the level of potential of the state and its armed forces. Today, more than ever, the information component in the strategy of ensuring the national and military security of the state has come to the fore [1], [2]. The study and implementation of technological trends of cyber protection in the sector of critical infrastructure allows to respond to the complexity of modern cyber threats and ensures an increase in the security of systems in real time.

Keywords: object of critical infrastructure; cyber security; cyber protection; security incidents; investigation of security incidents; information security incident management; information security incident response teams, security incident investigation tools.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On the Decision of the National Security and Defence Council of Ukraine of 6 May 2015 'On the National Security Strategy of Ukraine', Decree of the President of Ukraine No. 287/2015 (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/287/2015#Text.
2. On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine', Decree of the President of Ukraine No. 447/2021 (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R. (2022). Functions Of The Information Security And Cybersecurity System Of Critical Information Infrastructure. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(15),* 124–134. https://doi.org/10.28925/2663-4023.2022.15.124134
5. Kozhedub, Y., Vasylenko, S., Maksymets, A., & Girda, V. (2021). Conceptual model of information protection of critical information infrastructure of Ukraine. *Information Technology and Security, 9(2(17)),* 151–164. https://doi.org/10.20535/2411-1031.2021.9.2.249889

6. Gnatyuk, S., Berdibayev , R., Sydorenko, V., Zhyharevych, O., & Smirnova, T. (2023). System for cyber security events correlation and incident management in critical infrastructure objects. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19),* 176–196. https://doi.org/10.28925/2663-4023.2023.19.176196
7. Mashtaliar, Y., Kozachok, V., Brzhevska, Z., Bohdanov, O., Oksanych, I., & Lytvynov, V. (2023). Research of development and innovation of cyber protection at critical infrastructure facilities. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(22),* 156–167. https://doi.org/10.28925/2663-4023.2023.22.156167
8. Information security incident management (IDT). (2004). *Information technology - Security techniques* - (ISO/IEC TR 18044:2004).
9. Kent, K., Chevalier, S., Grance T., Dang H. (2006). *Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST).* https://doi.org/10.6028/NIST.SP.800-86
10. *CERT Coordination Center.* (б. д.). CERT Vulnerability Notes Database. https://www.kb.cert.org
11. *About CSIRT.* (n.d.). CSIRT of the State Research Institute of Cybersecurity and Information Protection Technologies. https://csirt.csi.cip.gov.ua/uk/pages/about-csirt
12. *CERT-UA.* (б. д.). https://cert.gov.ua/
13. *opsy | Digital Forensics.* (б. д.). Autopsy. https://www.autopsy.com/
14. *Wireshark · Go Deep.* (б. д.). Wireshark. https://www.wireshark.org/
15. *Magnet Forensics | Unlock the truth. Protect the innocent.* (б. д.). Magnet Forensics. https://www.magnetforensics.com/
16. *NETRESEC - Network Forensics and Network Security Monitoring*. (б. д.). Netresec. https://www.netresec.com/
17. *Nmap: the Network Mapper - Free Security Scanner.* (б. д.). https://nmap.org/
18. *Belkasoft: Intelligent Software for Digital Forensics and Cyber Incident Response*. (б. д.). https://belkasoft.com/
19. *HashMyFiles: Calculate MD5/SHA1/CRC32 hash of files*. (б. д.). NirSoft. https://www.nirsoft.net/utils/hash_my_files.html#google_vignette
20. **NEW* Community Tool: CrowdResponse*. (б. д.). CrowdStrike: We Stop Breaches with AI-native Cybersecurity. https://www.crowdstrike.com/en-us/blog/new-community-tool-crowdresponse/
21. *USB 3.1 WriteBlocker | WiebeTech*. (б. д.). WiebeTech | Digital Forensics. https://wiebetech.com/products/usb-3-1-writeblocker/
22. *DSi USB Write Blocker*. (2018). Hackercombat. https://www.hackercombat.com/digital-forensic-tools-availability-in-the-nutshell/dsi-usb-write-blocker/