DOI: 10.18372/2410-7840.23.16401
УДК 004.056.53

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЗА РАХУНОК ЗАСТОСУВАННЯ ПЛАТФОРМИ THREAT INTELLIGENCE

Артем Жилін, Богдан Ніколаєнко, Олександр Бакалинський

З розвитком інформаційних технологій збільшились потреби щодо вирішення задачі захисту інформації, оскільки вона стала найважливішим стратегічним ресурсом. Водночас, збільшується вразливість сучасного інформаційного суспільства до недостовірної інформації, несвоєчасного надходження інформації, промислового шпигунства, комп'ютерної злочинності, тощо. В такому разі швидкість виявлення загрози, в контексті добування системної інформації про зловмисників і можливих технік та інструментів реалізації кібератак з метою їх опису та оперативного реагування на них є однією з актуальних задач. Зокрема, постає задача у застосуванні нових систем збору інформації про кіберподії, реагування на них, зберігання та обмін цією інформацією, а також на її основі способів та засобів пошуку зловмисників за допомогою комплексних систем, або платформ. Для вирішення задач такого типу досліджується перспективний напрямок Threat Intelligence як новий механізм отримання знань про кібератаки. Визначено Threat Intelligence в задачах забезпечення кіберзахисту. Проведено аналіз індикаторів кібератак та інструменти їх отримання. Здійснено порівняння стандартів опису індикаторів компрометації та платформ їх обробки. Розроблено методику Threat Intelligence в задачах оперативного виявлення та блокування кіберзагроз державним інформаційним ресурсам. Ця методика дає можливість покращити продуктивність роботи аналітиків кібербезпеки та підвищити захищеність ресурсів та інформаційних систем.

Ключові слова: *Threat Intelligence, державні інформаційні ресурси, захищеність, загрози, зловмисники, індикатори кібератак, кіберзахист.*

ВСТУП

Декілька років тому основними векторами кіберзагроз з якими працювали фахівці з кіберзахисту були масові кібератаками. Сьогодні ці атаки розглядаються як вторинні загрози, які просто створюють "шум" у мережі. Здебільшого, організації та установи захищаються від них успішно, аналізуючи перші випадки виявлення кібератак, формуючи їх індикатори компрометації (IoC) та швидко поширюючи ці індикатори. Найбільш серйозні порушення кіберзахисту відбуваються за рахунок добре сплановних, складних атак, спрямованих на конкретні компанії або галузі. Добре профінансовані нападники ускладнюють виявлення своїх атак. Вони використовують методи соціальної інженерії, які не можуть бути ідентифіковані за допомогою простих індикаторів компрометації або заблоковані традиційними засобами захисту, та постійно адаптують свої інструменти, тактику та процедури, щоб уникнути новітніх заходів кібербезпеки. В додаток до зазначеного, кількість самих кіберзагроз стрімко зростає. Атаки і як наслідок компрометація комп'ютерних мереж можуть здійснюватися за хвилини, а процес виявлення, реагування та усунення наслідків атаки займає дні, тижні і навіть місяці. І найчастіше виявлення відбувається вже після того, як зловмисник скомпрометував державні інформаційні ресурси. При цьому, відповідно до щорічного звіту з інформаційної безпеки Cisco [1] фахівці з безпеки протягом свого робочого дня здатні обробити лише 56% вхідних повідомлень про загрози, а серед цих повідомлень обґрунтованим визнається тільки кожне друге (тобто 28%). Таким чином, 44% інцидентів залишаються без уваги. При цьому в організаціях критично не вистачає не тільки ресурсів, що дозволяють обробити всі інциденти, але і загальної системи, завдяки якій стало б можливим реагувати на них на ранніх стадіях кібератак – в

ідеалі до експлуатації, а також накопичувати розподілені знання про загрози, обмінюватися отриманими даними, розслідувати причини загроз і миттєво реагувати на них. Для більш швидкого накопичення інформації про можливі загрози слід прагнути до спільного використання корисних даних від широкого кола джерел. При цьому важливо, щоб ця інформація була стандартизована, тобто стандарти і протоколи передачі та надання даних були визначені заздалегідь. Відстеження загроз – одна з найважливіших функцій для ефективного захисту інформаційної системи організації. Threat Intelligence (TI) – система, що дозволяє дізнаватися про загрози, атаки до того, як вони зможуть нашкодити [2]. У випадках, якщо інцидент все ж стався, TI дозволить відреагувати, провести аналіз та відповідно розслідування, при цьому розширюючи свою базу знань контекстом, механізмами, індикаторами компрометації та аналітикою про існуючі або можливі загрози.

В той же час не потрібно перекладати дослівно поняття Threat Intelligence й розуміти як саме розвідка загроз у кіберпросторі в сенсі зазначеному в [3]. Слово "Intelligence" в англійській мові крім значення "розвідка" в сенсі військового підрозділу або процесу отримання прихованої інформації про країни, компанії, тощо, має ще значення здатність розуміти, вивчати, формувати судження та думки, засновані на фактах. Тому поряд з визначенням Threat Intelligence як розвідки загроз доцільно застосовувати аналоги – добування знань про загрози, або взагалі знання про загрози. Саме в цьому контексті автори й розуміють Threat Intelligence, який є, на їх думку, одним з процесів забезпечення кіберзахисту.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

В [4] надається інформація щодо обмежень які з'являються при обміну інформацією про кіберзагрози в рамках платформ TI, а також приводяться шляхи рішення цих обмежень та варіанти використання платформ TI. Найкращі практики використання TI, тенденції щодо цього й основні визначення в сфері TI наводяться в [5]. Питання спорідненості задач Threat Intelligence та Threat Hunting при розслідуванні кібератак, відтворення тактик зловмисників згідно моделі MITRE ATT&CK та інструментів які можливо при цьому використати наведено в [6]. Водночас питання підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи TI безпосередньо в задачах оперативного виявлення та блокування кіберзагроз у відомій літературі не розглядалося.

Тому, метою даної статті є розгляд можливості підвищення захищеності державних інформаційних ресурсів за рахунок застосування TI в задачах оперативного виявлення та блокування кіберзагроз.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розвідка загроз, добування знань про загрози (з англ. Threat Intelligence) визначається як сукупність знань, які будуються відповідно до спостережень, й містять в собі індикатори компрометації, механізми й контекст здійснення атак, а також практичні рекомендації щодо усунення виявлених та можливих загроз. Сервіси кіберрозвідки поєднують в собі інфраструктуру кібермоніторингу з висновками спеціалістів центрів розслідування та реагування на інциденти. Дані для даної інфраструктури поступають з розподіленої мережі моніторингу, Honeypot-пасток, результатів аналізу бот-мереж, різних конференцій, приватних груп у соціальних мережах, а також в результаті обміну інформацією між об'єднаннями по протидії кіберзагрозам [7].

Інформація про загрози – життєво важливий компонент ефективного захисту. Вона дозволяє передбачити атаки і готуватися до них заздалегідь, а не займатися дорогим і тривалим усуненням їх наслідків. Обробляючи і

аналізуючи дані із сотень джерел, можна отримати персоналізовану, перевірену і значиму інформацію, необхідну для підготовки до атак і відображенню актуальних загроз.

Рівні ТІ. Інформація, що отримується під час ТІ різнопланова – від мережевих артефактів й індикаторів компрометації до ідентифікації зловмисника. При чому, наприклад, технічним спеціалістам для налаштування засобів захисту більш важливою є інформація саме щодо індикаторів компрометації. Тому виникає необхідність виокремлення рівнів ТІ та інформації, яка на цих рівнях добувається та оброблюється.

Наразі не існує узагальненого розподілення рівнів ТІ, тому було проаналізовано існуючі представлення рівнів ТІ різними організаціями [8-10] та підсумовано в таблиці 1, яка виділяє дані організації та інформацію, що здобувається та оброблюється на цих рівнях.

Таблиця 1

Визначення рівнів та вихідної інформації в них іноземними організаціями

Організації	Рівні ТІ	Вихідна інформація
Національний центр кібербезпеки Великобританії (NCSC)	1. Тактичний	методології, інструменти та тактики, дії та інше про зловмисників
	2. Технічний	індикатори певного шкідливого програмного забезпечення
	3. Оперативний	деталі конкретної вхідної атаки, оцінка здатності організації визначати майбутні кіберзагрози
	4. Стратегічний	інформація високого рівня зі зменшення ризиків (стратегічні зрушення) – вище керівництво оцінює оцінки загрози
Threat Connect	1. Технічний	індикатори компрометації, виявлення сигнатур
	2. Тактичний	методології, інструменти та тактики
	3. Оперативний	індикатори компрометації
	4. Стратегічний	зменшення ризиків за рахунок моделей загроз, можливостей зловмисників
National Institute of Standards and Technology (NIST)	1. Тактичний	сповіщення системи безпеки, виявлення сигнатур, а в розширених випадках - деяка форма kill chain аналізу на основі відомостей про зловмисників або поведінки мережі
	2. Оперативний	визначення ботнетів, шкідливих програм, фішинг та ін.
	3. Стратегічний	визначення намірів та можливостей зловмисників
Fortinet	1. Оперативний	структуровані дані, індикатори компрометації
	2. Тактичний	низькорівневі звіти або структуровані дані, розуміння тактики, технік та процедур зловмисників
	3. Стратегічний	високорівневі звіти, моделі зловмисників, їх наміри, мотивація, плани

Як видно з табл. 1, зазначені джерела визначають 3 (тактичний, оперативний, стратегічний), або 4 (тактичний, технічний, оперативний, стратегічний) рівні ТІ. Визначення таких рівнів зумовлено різною природою даних, що добуваються та оброблюються під час ТІ. Ці ж дані й призначаються різним спеціалістам. Наприклад, звіт національної діяльності не можна порівняти з IP-адресою, і не може бути застосований таким же чином. Узагальнюючі отримані відомості під час аналізу рівнів ТІ й дані відносно цих рівнів, враховуючі існуючі рівні воєнного мистецтва, виділимо в Threat Intelligence три окремі рівні: стратегічний, оперативний та тактичний. Розглянемо їх більш детально.

Стратегічний рівень – це рівень де оброблюється інформація високого рівня, на основі якої приймається рішення керівництвом або старшою посадовою особою. На стратегічному рівні розвідки загроз працюють стратеги, як правило, рівня правління організації або тих, хто подає звіт до правління. Мета ТІ стратегічного рівня полягає в тому, щоб допо-

могти стратегам зрозуміти поточні та ймовірні ризики, отримати атрибути зловмисників, ідентифікувати їх, визначити їх стратегії та цілі. Матеріали розвідки часто представляють у вигляді звітів, де описуються геополітичне становище, активність APT-угруповань по напрямку діяльності організації, тенденції кібератак, високорівневі ризики, ймовірності їх реалізації та шляхи оброблення цих ризиків.

Зазначені відомості добуваються аналізом відкритих джерел (OSINT), отримуються з доповідей аналітичних організацій, від команд реагування на комп'ютерні інциденти (CERT) та компаній із сфери кіберзахисту у вигляді "фідів" [11]. Слід вказати, що з цих джерел можна отримати відповідну інформацію для оперативного та тактичного рівнів TI. Також для отримання інформації, що оцінюється на стратегічному рівні, застосовуються технології пошуку вразливостей в своїх комп'ютерних мережах та системах (Threat hunting) та криміналістичний аналіз мережевого трафіку (Network forensic). Ця інформація дає аналітикам стратегічного рівня розуміння ландшафту загроз в своїй інфраструктурі.

Оперативний рівень – рівень, на якому добувається інформація про ймовірні атаки на організацію, про їх можливі тактики, техніки та процедури, котрі вже мали місце. Ця інформація отримується шляхом аналізу подій, що виявляються мережевими засобами захисту (міжмережевими екранами Firewalls, мережевими приманками Honeypots та Honeynets), засобами захисту кінцевих пристроїв.

Вказані засоби захисту зазвичай виступають у ролі джерел даних для системи управління мережевими подіями та повідомленнями SIEM, за допомогою якої спеціалісти шляхом агрегації, кореляції та обробки виявлених подій можуть визначити тактики, техніки та процедури атак, що вже здійснилися.

В той же час для налаштування цих засобів захисту використовується інформація отримана з відкритих джерел, або з "фідів" щодо ймовірних складних advanced persistent threat (APT) атак.

Тактичний рівень. На тактичному рівні під час розвідки загроз на основі даних від систем виявлення та запобігання вторгнень (IDS/IPS), мережевих сенсорів, даних лог файлів серверів, кінцевих пристроїв, спеціалізованих засобів захисту (наприклад, Security E-mail Gateway) виявляються мережеві артефакти та ідентифікатори компрометації комп'ютерної мережі й може бути висунута гіпотеза щодо інструментів здійснення атаки.

За рахунок використання мережевого сканера та сканера вразливостей добувається інформація про наявні вразливості компонентів комп'ютерної мережі. Під час проведення OSINT також добувається інформація щодо вразливостей й ідентифікаторів компрометації, які властиві саме комп'ютерній мережі організації.

На основі отриманих даних мережеві адміністратори або спеціалісти з захисту інформації можуть відреагувати на кібератаку, налаштувати та скоректувати правила виявлення атак в системах захисту комп'ютерних мереж. Узагальнимо описані рівні TI та інформацію, яка отримується, у вигляді таблиці (табл. 2). Проаналізовані джерела та узагальнені рівні TI надають розуміння тільки того яка інформація добувається, опрацьовується та використовується на кожному з цих рівнів. Це відповідає підходам до побудови організаційно-технічної моделі кіберзахисту, наведеним у [13].

Звісно, що кінцева мета як TI так й розслідування кібератак полягає у ідентифікації зловмисника та його намірів.

Для досягнення цієї мети можливо використовувати **формалізовані моделі виявлення вторгнень зловмисників у кіберпросторі,** які безпосередньо оперують інформацію отриманою під час TI, а саме Q модель та Діамантову модель.

Таблиця 2

Рівні TI

	Рівні	Вихідна інформація
Threat Intelligence	Стратегічний	Ідентифікація противника, його можливих імен, псевдонімів, e-mail адрес, тощо. Визначення намірів та можливостей, зменшення ризиків за рахунок вивчення моделей загроз
	Оперативний	Розуміння тактик, технік та процедур противника, реагування на атаки, написання правил для захисних механізмів
	Тактичний (технічний)	Інструменти, мережеві артефакти, індикатори компрометації

Ці моделі ґрунтовно досліджено в [12], приведемо короткий їх огляд з точки зору їх застосування при TI. **Q модель**. Модель розроблена як карта процесу атрибуції: вона дозволяє людям, які не мають достатньої технічної бази реалізовувати детальну атрибуцію кібератаки (рис. 1) [14]. Це дозволяє вченим, а також політикам чи керівникам збільшувати значну технічну деталізацію і здійснювати змістовну комунікацію з технічними фахівцями.

Рис. 1 Q модель

І навпаки, модель дозволяє експертам-криміналістам оцінити стратегічний і політичний контекст. Сама модель має три рівні (стратегічний, оперативний, тактичний) та ділиться на три етапи (концептуальний, емпіричний, комунікаційний). Перший етап концептуальний: він представляє атрибуцію як процес обговорення моделі в загальних рисах, вводячи кілька критичних відмінностей та динаміки. Під час цього етапу спеціалісти повинні відповісти на питання як (тактичний рівень), хто (оперативний), чому (стратегічний рівень) здійснив атаку, яка була його мета, сили та засоби. Емпіричний рівень ставить уточнюючі, конкретні питання до концептуального рівня, надаючи відповідь на які можливо знайти індикатори компрометації для більш точної атрибуції зловмисника. Комунікаційний етап визначає повноту інформації та суб'єктів, яким вона передається під час обміну результатами дослідження, а також порядок цього обміну. Кінцевою метою атрибуції в Q моделі є визначення організації чи уряду, а не окремих осіб. Але за рахунок маркування, уніфікації та геотегів окремі індикатори можуть бути потужними доказовими зв'язками між артефактами та організаціями.

Діамантова модель [15]**.** Модель описує кібератаку як складову чотирьох основних функцій: противника, інфраструктури, можливостей та жертви. Ці особливості пов'язані з вершинами, що представляють їх основні відносини та розташовані у формі діаманту (рис. 2).

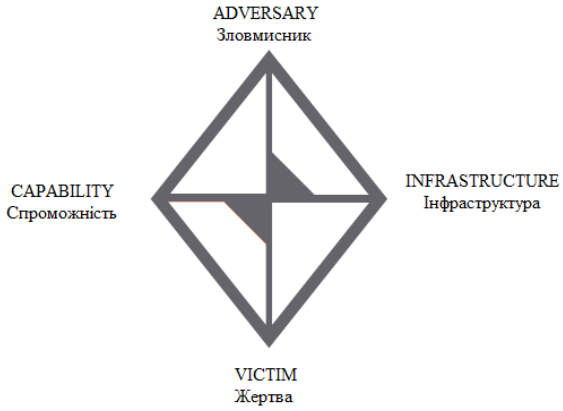

Рис. 2 Діамантова модель

Ця модель також визначає додаткові функції для підтримки конструкцій вищих рівнів, таких як поєднання подій разом в потоках активності та подальше об'єднання подій. Модель встановлює формальний метод, що застосовує наукові принципи до аналізу вторгнень, зокрема вимірювання, тестування та повторюваність. Цей науковий підхід і простота дають покращення аналітичної ефективності та точності. Зрештою, ця модель забезпечує можливості інтеграції розвідки загроз в режимі реального часу для захисту мережі, ав-

томатичної кореляції та класифікації подій. У найпростішій формі (рис. 2), модель описує, що противник має спроможність атакувати інфраструктуру жертви. Ці елементи називаються подіями.

Під час розвідки загроз або розслідування кібератак аналітик заповнює вершини моделі, коли виявляє події. Вершини пов'язані ребрами й виділяють зв'язки між функціями. Проходячи по ребрах та вершинах, аналітики виявляють більше інформації про операції зловмисника та виявляють нові спроможності (можливості), інфраструктуру та жертву. Подія визначає лише один крок у серії, яку противник повинен виконати для досягнення своєї мети.

Окрім Q моделі та Діамантової моделі, які безпосередньо описують процес проведення ТІ, слід зазначити існування таких моделей як **Kill Chain** та **MITRE ATT&CK**, що описують поведінку зловмисника при здійсненні кібератаки. Так Kill Chain [16] визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Для досягнення успіху зловмисник повинен пройти зазвичай усі вісім етапів – розвідка, озброєння, доставка, зараження, інсталяція, отримання управління, виконання дій, знищення слідів. Матриця MITRE ATT&CK являє собою структурований список відомих поводжень зловмисників, розділений на тактики, техніки та процедури, виражений у вигляді таблиць (матриць). Матриці для різних ситуацій і типів зловмисників публікуються на сайті MITRE [17]. Матриця ATT&CK може бути корисною для кіберрозвідки, оскільки вона дозволяє стандартизувати та описувати поведінку зловмисників. Зловмисники можуть відслідковуватися за допомогою асоціації – спостерігаючи мережеві події та події на кінцевих пристроях можна співвідносити їх з методами і тактиками в ATT&CK, які використовують ті чи інші угруповання.

Отримана під час ТІ інформація, виявлені індикатори компрометації та загрози, порядок та формат обміну повідомленнями та звітами потребують стандартизації. Розрізняють стандарти опису [18]:

- даних низького рівня (PCAP, CEF);
- показників компрометації (MAEC, Snort rule, MMDEF, CybOX);
- перелічення (CVE, CWE, CPE);
- кількісного опису загроз (CVSS, XCCDF);
- форматів звіту (CVRF, IODF, STIX).

Застосовуючи один із стандартних форматів організація може мінімізувати неоднозначність інформації, а також використовувати інструменти, які підтримують обмін за допомогою цих стандартів. Проте існують інші важливі технічні міркування для обміну інформацією, зокрема транспортні механізми, які використовуються для запиту та передачі даних. Крім того, під час використання нестандартних форматів даних, вибір методу сортування може мати суттєві наслідки для загальної продуктивності та простоти інтеграції з існуючими інструментами. В таблиці 3 представлені стандарти, їх рівні, можливості представлення інформації та приклад програм, які їх використовують.

Таблиця 3

Стандарти та інструменти для обміну та обробки інформації

Рівень стандарту	Назва стандарту	Можливість представлення інформації	Програми, які використовують стандарт
Дані низького рівня	PCAP	пакет, взятий з мережі	Tcpdump, Wireshark
	CEF	журналювання подій апаратними засобами	ArcSight SIEM
Показники компрометації	MAEC	характеристики ШПЗ та їх дії	Anubis, ThreatExpert, Cuckoo Sandbox
	MMDEF	назви файлів, хеш-файлів, поведінки ШПЗ	Cuckoo Sandbox
	Snort rules	IP-адреси, порти, протокол, напрям, HTTP-запит і параметри відповіді	Snort, Suricata
	CybOX	мережеві потоки, мережеві артефакти, файли, SMS-повідомлення, зображення, повідомлення електронної пошти	python-cybox
Перелічення	CVE	опис загроз	STIX, VERIS
	CWE	опис загроз, що часто застосовуються	IODEF-SC

	CPE	найменування операційних систем, пакетів програмного забезпечення, класів апаратних пристроїв	MAEC, CybOX
Кількісний опис загроз	CVSS	оцінка загрози від 0 до 10	IODEF-SC, Cuckoo Sandbox
	XCCDF	повний опис та середовище, в якому реалізується загроза	SCAP
Формати звітів	CVRF	описує весь життєвий цикл обробки вразливості	Використовується всередині комунікацій постачальників
	IODEF	формат XML, обмін інформацією про інциденти	ArcSight
	STIX	повний опис подій одним із вище зазначених стандартів	CRITs, Microsoft Interflow

Робота сучасних платформ на рівнях TI. В даний час критично не вистачає не тільки ресурсів, що дозволяють обробити всі інциденти кібербезпеки, але і загальних систем, завдяки яким стало б можливим реагувати на них на ранніх стадіях кібератак, а також добувати та накопичувати розподілені знання про загрози, обмінюватися отриманими даними, розслідувати причини атак, реагувати на них та знаходити зловмисників. Тому, було розглянуто основні платформи кіберрозвідки (Threat Intelligence Platform – TIP), які виконують ці завдання, а також сформована таблиця щодо можливостей роботи даних платформ згідно рівнів TI (табл. 4). Можливості, функції та призначення кожної платформи детально висвітленні в загальному доступі.

Таблиця 4

Порівняння основних платформ розвідки відповідно рівнів TI

Платформа	Тип	Рівні		
		Тактичний	Оперативний	Стратегічний
MISP	відкрита	+	+	-
CRITs	відкрита	+	+	-
TheHeroic	відкрита	+	+	+
YETI	відкрита	+	+	-
GOSINT Framework	відкрита	+	+	+
R-Vision	відкрита	+	+	+
ThreatStream	комерційна	+	+	+
IBM QRadar Security Intelligence Platform	комерційна	+	+	-

Отже, платформа розвідки загроз може бути розгорнута в якості програмного забезпечення як послуга для полегшення управління кіберрозвідкою, накопичення та обміну інформацією про такі об'єкти як зловмисники, компанії, інциденти, вразливості та TTP [19].

Це визначається її здатністю виконувати чотири ключові функції: агрегація розвідки з декількох джерел; коригування, нормалізація, збагачення та оцінка ризиків; інтеграція з існуючими системами безпеки; аналіз і обмін інформацією про загрози. В той же час не всі TIP можуть накопичувати, обробляти та обмінюватися інформацією всіх рівнів TI, також не відомі загальні методики процесу TI. Тому, пропонується наступна методика TI в задачах оперативного виявлення та блокування кіберзагроз державним інформаційним ресурсам (рис. 3).

Запропонована методика TI (рис. 3) поділяється на чотири етапи, які полягають у наступному:

Етап 1. На першому етапі пропонується розділити розвідку загроз на три рівні: тактичний (технічний), оперативний та стратегічний, відповідно до яких визначаються інструменти виявлення та збору даних (етап 2).

Етап 2. На даному етапі проводиться аналіз атак за допомогою інструментів виявлення та збору даних. Етап 2 має три підетапи згідно моделі послідовності дій атаки противника, а саме: збір даних атаки, обробка, реагування та визначення стратегій і цілей зловмисника. *Збір даних атаки* передбачає використання систем IPS/IDS, SIEM, антивірусних програм, log-файлів, проксі-серверів, інструментів тестування вразливостей мережі, інструментів сканування портів, Security E-mail Gateway та інших. Після збору всіх можливих даних про кібератаку відбувається їх *обробка та реагування* на інциденти. Це можливо завдяки додання правил для Firewall, застосування SIEM, Honeypots, Honeynets, EndPoint Protect, Sandboxes, тощо.

Останнім кроком етапу 2 є визначення можливих *даних про противника*, його *стратегій та цілей*. Для цього аналітики TI використовують методи полювання на загрози (Threat Hunting), проводять мережеві розслідування, застосовуючи інструменти OSINT. Інструменти OSINT також можуть застосовуватися впродовж всього виконання етапу 3 для пошуку даних про противника та можливі загрози.

Етап 3. Зловмисники мають різні мотиви, цілі, способи, інструменти. Для їх ідентифікації потрібно:

1) зібрати та охарактеризувати всі докази за допомогою стандартів опису загроз (індикатори компрометації, мережеві дані та інструменти противника);

2) на основі зібраних даних та інструментів кібератаки визначити тактики, техніки та процедури, згідно яких зловмисники реалізують свої цілі і вжити заходів щодо реагування на інциденти;

3) показати, яка мета зловмисників та яким чином вони будуть досягати бажаного, в найкращому випадку ідентифікувати зловмисника або групу зловмисників.

Для виконання цих завдань слід застосовувати різні моделі виявлення та реагування на вторгнення, а саме: Q – модель, Діамантову модель.

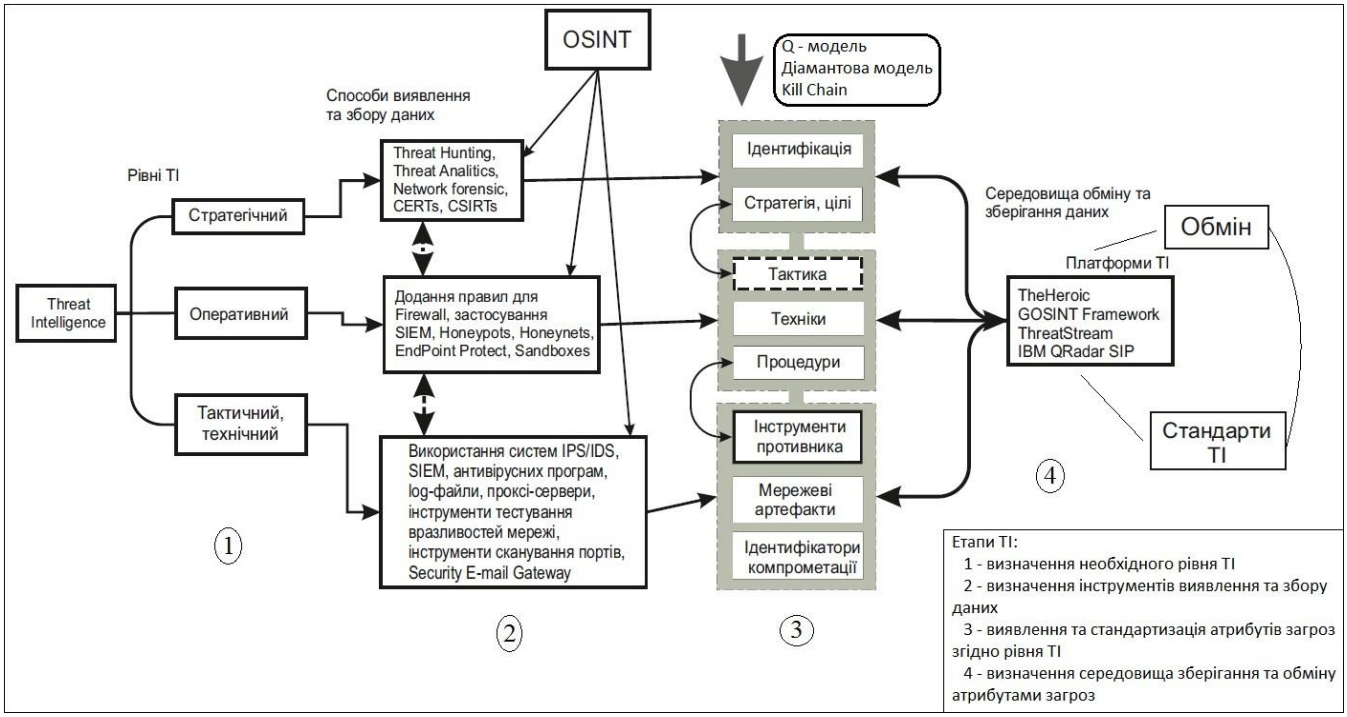

Рис. 3 Методика TI

Етап 4. Даний етап передбачає визначення середовища зберігання та обміну атрибутами загроз, зібраними даними на етапі 3. Для цього, згідно порівняльного аналізу пропонується застосувати платформи TI, які забезпечуватимуть збір, аналіз, обробку та обмін даними про зловмисників й загрози, що значно полегшить роботу аналітиків, які займаються питаннями забезпечення кібербезпеки.

Формалізація обміну даними забезпечується за допомогою спеціальних стандартів, які розглянуті в табл. 3.

ВИСНОВКИ

Побудовані КСЗІ, системи інформаційної безпеки та СУІБ на об'єктах інформаційної діяльності, в яких обробляються державні інформаційні ресурси, обов'язковість яких визначено у [20] вимагають підвищення їх ефективність за рахунок використання комп'ютеризованих методів та засобів, саме ці засоби автоматизують процеси збору, виявлення, обробки даних щодо нових загроз, їх блокування та подальшого вивчення з метою вироблення загальних рекомендації щодо захисту від них, що в даний час постає як нагальна проблема. Саме тому, в даній статті були проведені наступні дослідження. А саме:

Було розглянуто сутність ТІ як нового типу розвідки, коли більшість даних зберігаються у кіберпросторі. Визначено, що розвідка поділяється на три рівні: тактичний (технічний), оперативний та стратегічний, а також показано представлення рівнів розвідки різними організаціями забезпечення кібербезпеки. Було проаналізовано основні моделі виявлення вторгнень зловмисників.

За допомогою онтології показано як порушник застосовує тактики, техніки та процедури для цільових кібератак.

Варто відмітити, що в якості одного з найважливіших інструментів проведення інформаційних операцій виступає так звана "розвідка за відкритими джерелами".

Приведено основні стандарти, які забезпечують опис та формалізацію обміну індикаторами компрометації кібератак.

Визначено призначення найбільш відомих платформ кіберрозвідки як середовища збору індикаторів, їх зберігання, а також інструменту визначення тактик, цілей, стратегій зловмисника. Також показано можливість роботи цих платформ на рівнях розвідки загроз. На основі проведеного аналізу було розроблено методику ТІ для задач оперативного виявлення та блокування загроз державним інформаційним ресурсам, що може покращити продуктивність роботи аналітиків кібербезпеки та підвищити захищеність ресурсів та інформаційних систем.

ЛІТЕРАТУРА

[1] *Звіт Cisco із кібербезпеки. 2018*. [Електронний ресурс] – https://www.cisco.com/c/uk_ua/products /security/security-reports.html.

[2] *Что такое threat intelligence и как применять. 2021*. [Електронний ресурс] – https://rvision.pro/blog-posts/chto-takoe-threat-intelligence-i-v-che mego-tsennost.

[3] *Exploring the opportunities and limitations of current Threat Intelligence Platforms*. Public version 1.0, ENISA, December 2017, 2017. – 42 p.

[4] *ЗУ "ПІро основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII*. [Електронний ресурс] – https://zakon.rada.gov.ua/laws /show/ 2163-19#Text.

[5] Dave Shackleford. *Who's Using Cyberthreat Intelligence and How?* SANS Institute. InfoSec Reading Room. February 2015, 2015. – 26 p.

[6] Valentina Palacín. *Practical Threat Intelligence and Data-Driven Threat Hunting*. Packt Publishing Ltd. February 2021, 2021. – 398 p.

[7] *What is Threat Intelligence. 2021*. [Електронний ресурс] – https://www.forcepoint.com/cyber-edu/ threat-intelligence.

[8] *Національний центр кібербезпеки. 2021*. [Електронний ресурс] – https://www.ncsc.gov.uk.

[9] *National Institute of Standards and Technology. 2021*. [Електронний ресурс] – https://www.nist. gov.

[10] *Самая высокопроизводительная платформа информационной безопасности в отрасли 2021*. [Електронний ресурс] – https://www.fortinet. com/ru.

[11] *Threat Intelligence: Collecting, Analysing, Evaluating. MWR InfoSecurity Ltd. 2021*. [Електронний ресурс] – https://www.ncsc.gov.uk/content//files/protected_files/guidance_files//MWR_Threat_Intelli gence_whitepaper-2015.pdf.

[12] A. Zhylin, M. Hudyncev and M. Litvinov, "Functional model of cybersecurity situation center", *Information Technology and Security*, vol. 6, no. 2, 2018. – pp. 51-67, 2018.

[13] О. Потій, А. Семенченко, Д. Дубов, О. Бакалинський, Д. Мялковський, "Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України", *Захист інформації*, том 23, №1, січень-березень 2021, 2021. – С. 47-59.

[14] Thomas Rid, Ben Buchanan (2015). Attributing Cyber Attacks. The Journal of Strategic Studies, Vol. 38, Nos. 1–2, 2015. – pp. 4-37.

[15] *Applying the Diamond Model for Threat Intelligence*. 2021. [Електронний ресурс] – https://threatconnect.com/ blog/ diamond-model-threat-intelligence -star-wars/.

[16] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Ph.D. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation, 2010. – pp. 1-14.

[17] *MITRE ATT&CK. 2021.* [Електронний ресурс] – https://attack.mitre.org/.

[18] *Standards and tools for exchange and processing of actionable information.* // European Union Agency for Network and Information Security, 2017. – 51 p.

[19] *What is a Threat Intelligence Platform (TIP)? 2018.* [Електронний ресурс] – https://www.anomali.com/ resources/what-is-a-tip.

[20] *Постанова КМУ "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19 червня 2019 р. № 518.* [Електронний ресурс] – https://zakon.rada.gov.ua/laws/show/518-2019-% D 0%BF#Text.

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ЗА СЧЕТ ПРИМЕНЕНИЯ ПЛАТФОРМЫ THREAT INTELLIGENCE

С развитием информационных технологий увеличились потребности по решению задачи защиты информации, поскольку она стала важнейшим стратегическим ресурсом. В то же время, увеличивается уязвимость современного информационного общества к недостоверной информации, несвоевременного поступления информации, промышленного шпионажа, компьютерной преступности, и тому подобное. В таком случае скорость обнаружения угрозы в контексте добывания системной информации о злоумышленников и возможных техник и инструментов реализации кибератак с целью их описания и оперативного реагирования на них является одной из актуальных задач. В частности, стоит задача в применении новых систем сбора информации о киберсобытии, реагирование на них, хранение и обмен этой информацией, а также на ее основе способов и средств поиска злоумышленников с помощью комплексных систем или платформ. Для решения задач такого типа исследуется перспективное направление Threat Intelligence как новый механизм получения знаний о кибератаки. Определены Threat Intelligence в задачах обеспечения киберзащиты. Проведен анализ индикаторов кибератак и инструменты их получения. Проведено сравнение стандартов описания индикаторов компрометации и платформ их обработки. Разработана методика Threat Intelligence в задачах оперативного обнаружения и блокировки киберугроз государственным информационным ресурсам. Эта методика дает возможность улучшить производительность работы аналитиков кибербезопасности и повысить защищенность ресурсов и информационных систем.

Ключевые слова: Threat Intelligence, государственные информационные ресурсы, защищенность, угрозы, злоумышленники, индикаторы кибератак, киберзащита.

INCREASING THE SECURITY OF GOVERNMENT INFORMATION RESOURCES AT THE EXPENSE OF USING THE THREAT INTELLIGENCE PLATFORM

With the development of information technology, the need to solve the problem of information security has increased, as it has become the most important strategic resource. At the same time, the vulnerability of the modern information society to unreliable information, untimely receipt of information, industrial espionage, computer crime, etc. is increasing. In this case, the speed of threat detection, in the context of obtaining systemic information about attackers and possible techniques and tools for implementing cyberattacks in order to describe them and respond to them quickly is one of the urgent tasks. In particular, there is a challenge in the application of new systems for collecting information about cyber events, responding to them, storing and exchanging this information, as well as on its basis methods and means of finding attackers using integrated systems or platforms. To solve this type of problem, the promising direction of Threat Intelligence as a new mechanism for gaining knowledge about cyberattacks is studied. Threat Intelligence in cyber security tasks is defined. The analysis of cyberattack indicators and tools for obtaining them is carried out. The standards of description of compromise indicators and platforms of their processing are compared. The technique of Threat Intelligence in tasks of operative detection and blocking of cyberthreats to the state information resources is developed. This technique makes it possible to improve the productivity of cybersecurity analysts and increase the security of resources and information systems.

Key words: Threat Intelligence, public information resources, security, threats, attackers, cyber attack indicators, cyber defense.

Жилін Артем Вікторович, кандидат технічних наук, доцент, професор спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
E-mail: zhylinartem@gmail.com.
Orcid ID: 0000-0002-4959-612X.

Жилин Артем Викторович, кандидат технических наук, доцент, профессор специальной кафедры № 5 Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".

Zhylin Artem Viktorovych, Candidate of Technical Sciences, Associate Professor, Professor at the Special Department № 5 of the Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky".

Ніколаєнко Богдан Анатолійович, кандидат технічних наук, старший викладач спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
E-mail: nikolaenko_iszzi@ukr.net.
Orcid ID: 0000-0002-6888-5947.
Николаенко Богдан Анатольевич, кандидат технических наук, старший преподаватель специальной кафедры № 3 Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".
Nikolaenko Bohdan Anatoliyovych, Candidate of Technical Sciences, Senior Lecturer at the Special Department № 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky".

Бакалинський Олександр Олегович, кандидат технічних наук, заступник директора Департаменту кіберзахисту, начальник відділу Адміністрації Держспецзв'язку, Київ.
E-mail: baov@meta.ua.
Orcid ID: 0000-0001-9712-2036.
Бакалинский Александр Олегович, кандидат технических наук, заместитель директора Департамента киберзащиты, начальник отдела Администрации Госспецсвязи, Киев.
Bakakynskyi Oleksandr Olehovich, Candidate of Technical Sciences, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine, Kyiv, Ukraine.

DOI: 10.18372/2410-7840.23.16403
УДК 621.327:681.5

РОЗРОБКА МЕТОДУ КРИПТОКОМПРЕСІЙНОГО КОДУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ПЛАВАЮЧОЇ НЕДЕТЕРМІНОВАНОЇ СХЕМИ ОБРОБКИ

Володимир Бараннік, Сергій Сідченко, Валерій Бараннік, Дмитро Бараннік, Сергій Шульгін, Сергій Туренко

В процесі управління об'єктами кризової інфраструктури та під час їх охорони використовуються цифрові відеозображення. Їх обсяги постійно зростають та до них висуваються вимоги щодо збереження максимальної якості при необхідності забезпечення конфіденційності. Тому, актуальною є науково-прикладна проблема, яка полягає в підвищенні конфіденційності відеоінформації в умовах забезпечення її достовірності та доступності. Для її вирішення отримав подальше вдосконалення однокаскадний метод криптокомпресійного кодування зображень в диференційованому базисі на основі використання технології нерівноважного позиційного кодування. Відмінність даного методу від відомих полягає в наступному. По-перше, плаваюча схема кодування організується в межах всієї площині зображення, коли у формуванні кодових величин інформаційної складової беруть участь елементи зображення, що належать різним блокам відеоданих. Для цього розроблена схема лінеаризації координат з чотиривимірного представлення елементу в двовимірної матриці, які визначають координати блоку в площині зображення та координати елементу в цьому блоці, в одновимірну координату для взаємно-однозначного уявлення цього елемента у векторі. По-друге, додатково використовуються два ступеня невизначеності, які складаються з недетермінованої довжини криптокомпресійних кодограм і недетермінованої кількості елементів, що беруть участь в їх формуванні. Це дозволяє підвищити криптостійкість та доступність відеоданих без втрати достовірності.

Ключові слова: *криптокомпресійне представлення, захист інформації, шифрування, кодування, компресія, конфіденційність, зображення.*

ВСТУП

Останнім часом відеозображення широко використовуються для прийняття рішень в процесі управління об'єктами кризової інфраструктури та під час їх охорони. Обсяги зображень постійно зростають і до них висуваються вимоги щодо збереження максимальної якості.

При цьому висуваються вимоги щодо забезпечення конфіденційності відеоданих. Тому, необхідно вирішити актуальну науково-прикладну проблему, яка полягає в підвищенні конфіденційності відеоінформації в умовах забезпечення її достовірності та доступності. Існують різні підходи щодо забезпечення конфіденційності зображень, серед яких: