DOI 10.51369/2707-7276-2024-1(37)-11
УДК 35.004

ГОРДІЄНКО Сергій Борисович
КОБУС Олена Сергіївна

ПИТАННЯ ВДОСКОНАЛЕННЯ ПРОЦЕСІВ ВИЯВЛЕННЯ І ОБРОБКИ ПОДІЙ ТА ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Своєчасні виявлення подій та обробка можливих інцидентів інформаційної безпеки (ІБ) є найактуальнішим питанням в умовах інформаційної боротьби та воєнної агресії.

У статті відзначається особлива актуальність питань створення систем моніторингу ІБ для вирішення завдань у процесі роботи компаній, що активно нарощують арсенал засобів безпеки задля забезпечення інформаційної безпеки на об'єктах критичної інфраструктури. Розкривається сутність способів реагування на події та інциденти ІБ та їхньої обробки, удосконалення процесів виявлення й обробки подій та інцидентів інформаційної безпеки, підтримки ефективного функціонування систем моніторингу подій ІБ.

Розглядається послідовність операцій обробки подій та інцидентів ІБ, що реалізуються на етапі процесу управління інцидентами ІБ із застосуванням алгоритму першої оцінки та попереднього рішення про події та другої оцінки з підтвердженням можливого інциденту інформаційної безпеки.

Особлива увага звертається на те, що в процесі аналізу потенційного або реального негативного впливу необхідно підтвердити, які наслідки мали місце для бізнесу організації внаслідок інциденту ІБ.

Надано практичні рекомендації щодо вдосконалення процесів виявлення подій та обробки інцидентів ІБ, підтримки ефективного функціонування систем моніторингу подій ІБ, зокрема проведення таких заходів: забезпечення належної організації процесу управління інцидентами ІБ, що передбачає розробку та впровадження політики й процедур управління інцидентами ІБ, підготовку персоналу, який буде відповідати за виявлення та реагування на інциденти ІБ; упровадження систем моніторингу ІБ, здатних виявляти широкий спектр подій та інцидентів ІБ і забезпечувати їхню ефективну обробку; створення ефективного алгоритму реагування на інциденти ІБ, що визначатиме порядок дій, які необхідно виконати для усунення виявлених подій та інцидентів ІБ; проведення регулярних навчань і тренінгів із питань виявлення та реагування на інциденти ІБ, що допоможе персоналу набути необхідних знань і навичок.

Ключові слова: *джерело загрози, події та інциденти ІБ, процес реагування на інциденти ІБ, система моніторингу подій, система управління інцидентами ІБ, системи обробки і кореляції подій.*

Постановка проблеми. Не так давно розв'язання питання створення систем моніторингу подій інформаційної безпеки (далі – ІБ) передбачало вирішення тільки базових завдань. Наприклад, підключалися типові джерела подій ІБ: зазвичай, мережеві засоби захисту, комунікаційне обладнання й операційні системи (далі – ОС), для яких необхідно було забезпечити централізоване довготривале зберігання даних журналів аудиту та налаштувати низку окремих повідомлень щодо класичних інцидентів.

Сповіщення про три спроби входу за 10 хв (підбір пароля), мережева авторизація користувача на робочій станції, невдала спроба входу від імені користувача, установленого за замовчуванням, і десятки подібних умов – приклади правил спрацьовування інцидентів, якими комплектувалася більшість проєктів систем моніторингу ІБ.

Останніми роками на ринку послуг зі створення систем моніторингу ІБ уже активніше вирішуються завдання, з якими стикаються компанії, що нарощують арсенал засобів безпеки.

Усі засоби захисту (антивірусні системи, міжмережеві екрани, системи захисту систем управління базами даних (СУБД) і Web-сервісів, сканери вразливостей та ін.) налаштовані й ефективно працюють, ведеться запис подій ІБ в журнали аудиту кожної системи, але між ними немає єдиного сполучуваного ланцюга та відповідно єдиної прозорої картини того, що відбувається в ІБ-інфраструктурі.

Найчастіше при такому підході знижується оперативність реагування на інциденти ІБ, практично неможливо визначити джерело загрози та знайти відповідальних за виникнення інциденту. Також ускладнюються отримання повної і достовірної інформації про реалізацію загроз ІБ в режимі online, демонстрація ефективного аналізу подій ІБ під час сертифікації та перевірок, стратегічне планування розвитку ІБ.

Централізований моніторинг подій ІБ дає можливість службам безпеки діяти проактивно, ефективно використовувати комплекс засобів захисту й оперативно виявляти інциденти.

Аналіз останніх досліджень і публікацій. Питання вдосконалення процесів виявлення подій та обробки інцидентів інформаційної безпеки, підтримки ефективного функціонування систем моніторингу подій ІБ, створення й застосування дієвого алгоритму реагування на інциденти ІБ з їх подальшою обробкою досліджувала низка фахівців: Р. Андерсон [15], Д. Ґір [11], М. Крістодореску [14], В. Лі [12], Д. Спаффорд [16], Б. Шнайер [9].

Зокрема Росс Андерсон, видатний дослідник у галузі комп'ютерної безпеки та криптографії, зробив значний внесок у сферу економіки безпеки, аналізуючи стимули й поведінку, які впливають на рішення щодо безпеки в організаціях. Робота Р. Андерсона сприяла кращому розумінню економічних факторів, які впливають на політику та практику інформаційної безпеки, що дало змогу розробити ефективніші системи безпеки. Джин Спаффорд, відомий як «Спаф», є провідною фігурою в дослідженнях кібербезпеки, особливо у сферах виявлення вторгнень і реагування на них. Він брав участь у розробленні перших систем виявлення вторгнень (IDS) і зро-

бив внесок у розуміння методів безпечної розробки програмного забезпечення. Брюс Шнайер, як криптограф і експерт з безпеки, вивчає проблематику дизайну безпеки та моделювання загроз. Його роботи допомогли популяризувати концепцію «театру безпеки» й визначили важливість реалістичної оцінки загроз та управління ризиками. Венке Лі, відомий своїми дослідженнями в галузі мережевої безпеки та виявлення вторгнень, розробляє методи на основі машинного навчання для виявлення шкідливого програмного забезпечення й інших мережевих загроз. Ден Ґір, експерт з кібербезпеки, вивчаючи питання управління ризиками й інформаційною безпекою, також бере участь у розробленні фреймворків, які дають змогу організаціям ефективніше оцінювати ризики й управляти ними. Наукові розвідки Міхая Крістодореску спрямовані на вирішення питань забезпечення безпеки мобільних і хмарних обчислювальних систем, виявлення шкідливого програмного забезпечення, зокрема з використанням статичного й динамічного аналізу та на основі поведінки.

Водночас потребує подальшого дослідження ціла низка питань: удосконалення можливостей IDS для боротьби зі зростаючою складністю атак, включаючи використання машинного навчання та штучного інтелекту для підвищення точності виявлення та зменшення кількості помилкових спрацьовувань; удосконалення методів моделювання загроз; розроблення практичніших інструментів для оцінювання ризиків у різних організаційних контекстах; підвищення масштабованості й точності моделей машинного навчання у сфері безпеки, особливо при обробці великих обсягів даних і виявленні складних, прихованих атак; розроблення надійніших економічних моделей, які враховують складний і глобальний характер кіберзагроз.

Мета статті – удосконалення алгоритму процесів виявлення й обробки подій та інцидентів інформаційної безпеки, визначення шляхів ефективного функціонування систем моніторингу подій ІБ, а також ступеня економічної доцільності застосування певних безпекових заходів стосовно прояву можливих інцидентів інформаційної безпеки.

Виклад основного матеріалу. У сучасну цифрову епоху поширення інформаційних технологій та інтернету призвело до експоненціального зростання кіберзагроз, що робить інформаційну безпеку критично важливою проблемою для організацій по всьому світу. Процеси виявлення подій та обробки інцидентів інформаційної безпеки є фундаментальними компонентами стратегії кібербезпеки організації. Однак ці процеси пов’язані з певними проблемами, починаючи від складності ландшафту загроз і завершуючи обмеженнями сучасних технологій і методологій.

Однією з головних проблем у виявленні подій та обробці інцидентів інформаційної безпеки є природа кіберзагроз, що швидко еволюціонує. Сучасні постійні загрози, уразливості «нульового дня» та складне шкідливе програмне забезпечення – це лише кілька прикладів загроз, які постійно адаптуються, щоб уникнути виявлення. Традиційні заходи безпеки, такі як антивірусне програмне забезпечення

на основі сигнатур і брандмауери, часто виявляються недостатніми проти цих сучасних загроз. Це зумовлює необхідність упровадження досконаліших технологій.

Машинне навчання (ML) і штучний інтелект (AI) стали потужними інструментами в арсеналі кібербезпеки. Ці технології здатні аналізувати величезні обсяги даних, виявляти закономірності й аномалії, які можуть свідчити про порушення безпеки. Наприклад, алгоритми виявлення аномалій можуть відстежувати мережевий трафік і поведінку користувачів, щоб виявити відхилення від норми, які можуть свідчити про атаку. Однак упровадження ML і AI у систему кібербезпеки також пов'язане з певними проблемами, такими як потреба у великих наборах даних для навчання та ризик ворожих атак, спрямованих на обман цих систем.

Інтеграція аналізу великих даних у процеси кібербезпеки дає змогу аналізувати різноманітні й об'ємні набори даних, включаючи журнали, мережевий трафік і дії користувачів. Аналітика великих даних може покращити виявлення загроз шляхом співставлення інформації з різних джерел, надаючи більш повне уявлення про потенційні загрози. Проте управління й обробка великих даних потребують значних обчислювальних ресурсів і досвіду, що може стати перешкодою для багатьох організацій.

SIEM-системи займають центральне місце в сучасних операційних центрах безпеки (SOC). Вони агрегують і аналізують дані про безпеку з усієї інфраструктури організації, забезпечуючи моніторинг та оповіщення в режимі реального часу. SIEM-системи можуть бути високоефективними у виявленні інцидентів безпеки, але вони також створюють проблеми, такі як управління помилковими спрацьовуваннями, складність конфігурації та необхідність постійного налаштування для адаптації до нових загроз.

Хоча технології відіграють вирішальну роль у виявленні й обробці подій безпеки, людський фактор не менш важливий. Ефективність заходів із кібербезпеки часто залежить від досвіду та здатності приймати рішення фахівців із кібербезпеки, які експлуатують ці системи. Однією з найважливіших проблем у сфері кібербезпеки є дефіцит навичок. Існує дефіцит кваліфікованих фахівців із кібербезпеки, які володіють технічними навичками та знаннями, необхідними для управління складними системами безпеки й ефективного реагування на інциденти. Цей дефіцит посилюється через швидкий розвиток загроз кібербезпеці, тому потрібні безперервні навчання та адаптація.

Людські помилки є основною причиною інцидентів безпеки. Помилки можуть виникати на різних етапах – від конфігурації систем безпеки до реагування на тривожні сигнали. Для мінімізації людських помилок необхідні програми навчання та підвищення обізнаності, але тільки їх недостатньо. Організації також повинні впроваджувати надійні політики й автоматизовані системи, щоб зменшити залежність від ручних процесів і ризик помилок [4].

Щоб ефективно реагувати на інциденти, потрібні добре підготовлені та скоординовані IRT – групи, що

здатні швидко виявляти, локалізувати та пом'якшувати наслідки інцидентів безпеки. Однак створення та підтримка роботи IRT є складним завданням, для виконання якого необхідні спеціальні навички, чіткі канали зв'язку, а також чітко визначені ролі й обов'язки. Крім того, плани реагування на інциденти необхідно регулярно оновлювати та тестувати, щоб забезпечити їхню ефективність у реальних умовах.

Організаційні політики та структури управління є основою процесів виявлення подій та обробки інцидентів інформаційної безпеки [1]. Ці політики визначають межі, у яких здійснюється діяльність із безпеки, і забезпечують відповідність законодавчим і нормативним вимогам.

Організації повинні встановити чіткі політики та процедури для виявлення та реагування на події, пов'язані з інформаційною безпекою. Ці політики мають визначати ролі й обов'язки різних зацікавлених сторін, включаючи IT-персонал, персонал служби безпеки та керівництво. Вони також описують процеси виявлення інцидентів, звітування, ескалації та вирішення. Чіткі політики допомагають забезпечити скоординоване й ефективне реагування на інциденти безпеки, зменшуючи плутанину та затримки.

Відповідність законодавчим і нормативним вимогам є критично важливим аспектом інформаційної безпеки [5–7]. Організації повинні дотримуватися правил захисту даних, визначених у Загальному регламенті захисту даних (GDPR) і Законі про переносимість і відповідальність за медичне страхування (HIPAA), які передбачають конкретні заходи щодо безпеки даних і звітності про інциденти. Недотримання цих норм може призвести до серйозних штрафів і репутаційних втрат.

Сильна культура безпеки має важливе значення для ефективності заходів із кібербезпеки. Ця культура повинна пронизувати всі рівні організації – від вищого керівництва до рядових співробітників. Свідома культура безпеки заохочує працівників дотримуватися найкращих практик безпеки, повідомляти про підозрілі дії та підтримувати ініціативи з безпеки. Для формування такої культури потрібні: постійне навчання, комунікація, прихильність керівництва.

Характер ландшафту кібербезпеки динамічний і складний, тому необхідний цілісний та адаптивний підхід до виявлення подій та обробки інцидентів інформаційної безпеки. Цей підхід передбачає інтеграцію технологій, людського фактору й організаційної політики в єдину стратегію.

Інтегрована архітектура безпеки об'єднує різні технології та процеси безпеки в єдину систему. Така інтеграція покращує видимість, координацію та ефективність виявлення і реагування на події безпеки. Наприклад, інтеграція SIEM-систем з інструментами виявлення та реагування на кінцеві точки (EDR), системами виявлення вторгнень (IDS) і платформами розвідки загроз дає комплексне уявлення про ландшафт безпеки і можливість ефективніше реагувати на інциденти.

Безперервний моніторинг є життєво важливим для підтримання актуального розуміння середовища безпеки. Організації повинні регулярно переглядати й оновлювати свої систе-

ми безпеки, політики та процедури, щоб реагувати на нові загрози та вразливості. Цей процес безперервного вдосконалення повинен включати регулярне оцінювання безпеки, тестування на проникнення та аудити для виявлення слабких місць і сфер, які потребують удосконалення.

Співпраця та обмін інформацією є критично важливими компонентами адаптивної стратегії безпеки. Організації повинні співпрацювати з колегами по галузі, державними установами та організаціями з кібербезпеки для обміну інформацією про загрози, кращими практиками й отриманими уроками. Участь у центрах обміну та аналізу інформації (ISAC) й інших спільних форумах може підвищити обізнаність про ситуацію та забезпечити раннє запобігання новим загрозам.

Ускладнення архітектури та збільшення кількості елементів систем моніторингу подій ІБ пов'язані із зростанням числа джерел, що до них підключаються, так як проєкти часто охоплюють відразу кілька майданчиків, розташованих у різних містах.

Архітектура ІТ-рішення зазвичай включає компоненти для збирання, первинної фільтрації і агрегації подій, ядро системи для обробки та кореляції подій, СУБД для оперативної роботи й систему зберігання даних для ведення архіву журналів аудиту, а також компоненти, необхідні для адміністрування, роботи зі звітами й оповіщенням про інциденти ІБ.

Ключовою перевагою системи моніторингу подій ІБ є можливість виявлення складних інцидентів ІБ, складених із ланцюжків подій від багатьох ІТ-компонентів. Механізм кореляції подій, реалізований у багатьох рішеннях цього класу, потребує опрацювання з боку фахівців, які розуміють логіку реалізації загроз ІБ. Лише в деяких компаніях після впровадження систем моніторингу створюється штат аналітиків, здатних реалізувати правила кореляції подій.

Від опрацювання цієї частини рішення залежить, наскільки ефективним буде процес виявлення нетипових інцидентів, які можуть представляти для бізнесу найбільші ризики.

В умовах зростання складності загроз ІБ закономірною стала і зміна вимог, що пред'являються до систем моніторингу. Разом із централізованим збиранням і зберіганням журналів аудиту обширного переліку пристроїв і програм, оповіщенням про інциденти ІБ, а також реалізацією нормативних вимог системи моніторингу подій ІБ мають вирішувати нові завдання:

– підготовка рекомендацій щодо налаштування опцій аудиту в кінцевих системах;

– категоризація подій і пріоритезація інцидентів;

– аудит і моніторинг подій ІБ на всіх рівнях триланкової архітектури додатків (рівні даних СУБД, дій користувачів у бізнес-додатках або на Web-сервері);

– підготовка пропозицій щодо проведення оперативно-розшукових заходів у відповідь на інцидент, що виник;

– збирання свідчень порушень для розслідування інцидентів;

– контроль розслідування інцидентів і виявлення порушників;

– збільшення ефективності управління ризиками ІБ і виявлення необхідних додаткових заходів захисту.

Для їхньої реалізації потрібно не тільки створювати систему моніторингу подій ІБ, а й забезпечити її роботу супутніми технологіями аудиту, вибудувати процеси управління подіями й інцидентами, розвинути компетенції співробітників служби ІБ компаній. Відповіддю на виникнення нових завдань, збільшення технологій обробки подій і вибудовування процесів ІБ стала поява проєктів із створення центрів управління інцидентами ІБ (Cyber Incident Response Center – CIRC), де система моніторингу є важливою, але не єдиною ланкою рішення [17].

Події ІБ виявляє безпосередньо особа, яка помітила дещо, що викликає занепокоєння і має технічний, фізичний чи процедурний характер [2]. Виявлення може здійснюватися, наприклад, датчиками вогню або за допомогою охоронної сигналізації шляхом передачі сигналів тривоги в заздалегідь визначені місця для подальшого здійснення людиною попередньо спланованих дій. Технічні події ІБ виявляються автоматично, наприклад, це можуть бути сигнали тривоги, які подають засоби аналізу записів журналів реєстрації, засоби виявлення вторгнень (ЗВВ), антивірусні програми, у кожному випадку стимульовані заздалегідь установленими параметрами.

Виявлення подій – це процес виявлення та фіксації подій, що мають відношення до безпеки в IT-середовищі організації. Ці події можуть варіюватися від безпечних дій, таких як вхід користувача в систему, до потенційно зловмисних дій, таких як спроби несанкціонованого доступу або виявлення шкідливого програмного забезпечення. Обробка інцидентів, з іншого боку, включає в себе кроки, що вживаються після того, як подія була ідентифікована як потенційний інцидент безпеки. Це, зокрема: аналіз події, локалізація загрози, усунення причини, відновлення після будь-якої шкоди, документування процесу для подальшого використання і вдосконалення.

Виявлення подій має вирішальне значення для раннього виявлення загроз. Постійний моніторинг мережевого трафіку, поведінки користувачів і системних журналів дає змогу виявити потенційні загрози до того, як вони переростуть у серйозні інциденти безпеки. Такі методи, як виявлення аномалій, виявлення на основі сигнатур та евристичний аналіз, відіграють ключову роль у виявленні відхилень від нормальної поведінки, які можуть свідчити про загрозу безпеці.

Безперервний моніторинг і виявлення дають можливість організаціям підтримувати проактивну позицію безпеки. Замість того, щоб реагувати на інциденти після того, як вони завдали шкоди, організації можуть протидіяти загрозам на стадії їхнього зародження. Такий проактивний підхід значно зменшує вікно можливостей для зловмисників, мінімізуючи потенційний вплив порушень безпеки. Виявлення подій має важливе значення для дотримання різних нормативних вимог і стандартів, таких як GDPR, HIPAA та ISO/IEC 27001 [10; 13]. У цих нормах часто передбачаються постійний моніторинг і звітування про події безпеки.

Ефективне виявлення подій гарантує, що організації можуть створювати точні та своєчасні звіти, демонструючи дотримання нормативних вимог. Обробка інцидентів є наріжним каменем ефективної стратегії реагування на інциденти. Вона охоплює весь життєвий цикл управління інцидентами – від виявлення й аналізу до локалізації, ліквідації та відновлення.

Чітко розроблений план реагування на інциденти забезпечує систематичне управління інцидентами, зменшуючи хаос і плутанину під час порушення безпеки. Основною метою обробки інцидентів є мінімізація впливу та збитків, спричинених інцидентами безпеки. Швидко локалізувавши й усунувши загрози, організації можуть запобігти подальшій компрометації своїх систем і даних.

Ефективна обробка інцидентів також включає процедури для відновлення нормальної роботи та зменшення будь-яких залишкових збитків. Обробка інцидентів дає цінну інформацію про природу й походження інцидентів безпеки. Аналізуючи інциденти та документуючи процес реагування, організації можуть виявити слабкі місця у своїй системі безпеки та вжити коригувальних заходів.

Інтеграція виявлення подій та обробки інцидентів у межах СУІБ є життєво важливою для цілісної та комплексної стратегії безпеки. Така інтеграція забезпечує безперебійний потік інформації та дії, що дають змогу організаціям швидко й ефективно реагувати на загрози безпеці. Централізований підхід до моніторингу та реєстрації подій має важливе значення для ефективного виявлення подій. Системи управління інформацією та подіями безпеки (SIEM) відіграють ключову роль в агрегуванні та кореляції даних із різних джерел, забезпечуючи цілісне уявлення про ландшафт безпеки організації.

SIEM-системи полегшують аналіз і оповіщення в режимі реального часу, забезпечуючи своєчасне виявлення потенційних загроз. Автоматизація є ключовим компонентом сучасних стратегій реагування на інциденти. Використовуючи автоматизацію, організації можуть упорядкувати робочий процес обробки інцидентів, скоротити час реагування та мінімізувати залежність від ручного втручання.

Інструменти автоматизації можуть виконувати такі завдання, як: локалізація загрози, ізоляція уражених систем і початковий аналіз, звільняючи персонал служби безпеки для виконання складніших завдань. Безперервне вдосконалення є фундаментальним принципом СУІБ. Установивши зворотний зв’язок між виявленням події та обробкою інциденту, організації можуть постійно вдосконалювати свої заходи безпеки.

Регулярний перегляд звітів про інциденти, аналіз першопричин та оцінювання після інциденту дають цінну інформацію для підвищення ефективності процесів виявлення та реагування. Величезні обсяги даних, що генеруються системами виявлення подій, можуть бути приголомшливими. Організації повинні впроваджувати ефективні методи управління й аналізу даних, щоб отримати значущі висновки. Високий рівень хибних спрацьовувань може призвести до втоми від тривог, тоді справжні загрози ігнору-

ватимуться. Точне налаштування алгоритмів виявлення та використання розширеної аналітики загроз може пом'якшити цю проблему. Обмеженість ресурсів, як кадрових, так і технологічних, може перешкоджати ефективному виявленню подій та обробці інцидентів. Визначення пріоритетів для критично важливих активів і підходи, засновані на оцінюванні ризиків, можуть допомогти оптимізувати розподіл ресурсів.

Якщо проводити регулярні тренінги з програмами підвищення обізнаності з персоналом служби безпеки, то він буде добре підготовлений до протидії новим загрозам та ефективно використовуватиме інструменти виявлення та реагування. Ефективна комунікація та співпраця різних команд, таких як ІТ, служба безпеки та керівництво, мають важливе значення для скоординованого реагування на інциденти безпеки. Проведення регулярних аудитів та оцінювань механізмів виявлення подій та обробки інцидентів гарантує, що вони залишатимуться надійними й відповідатимуть мінливому ландшафту загроз.

Різні категорії користувачів виявляють інциденти ІБ і події ІБ різними способами. Так, фахівці підрозділу ІБ можуть виявити події ІБ та інциденти ІБ таким чином:

– отримуючи повідомлення від засобів захисту інформації (ЗЗІ);

– вивчаючи результати проведення аналізу захищеності активів організації з використанням інструментальних засобів;

– аналізуючи журнали реєстрації подій серверів, активного мережевого обладнання, прикладного програмного забезпечення (ПЗ), баз даних (БД) тощо;

– переглядаючи дані систем відеоспостереження та контролю доступу й ін.

Співробітники підрозділів, відповідальних за підтримку інформаційної інфраструктури, виявляють інциденти ІБ шляхом здійснення регулярного моніторингу уразливостей і загроз ІБ для інформаційних систем (далі – ІС), за які вони відповідальні. Основними джерелами відомостей для адміністраторів ІС є:

– сайти та новини розсилки виробників ПЗ;

– новинні сайти й розсилки третіх сторін;

– БД уразливостей;

– повідомлення про доступні оновлення ПЗ;

– інші повідомлення про уразливість, оновлення або загрози ІБ.

Рядові користувачі виявляють інциденти ІБ за допомогою спостереження за роботою систем, сервісів і мереж, з якими вони працюють, а також за роботою інших користувачів і служб організації.

Після того, як інцидент ІБ (або подія ІБ, схожа на інцидент ІБ) був виявлений, про нього повідомляється за встановленими каналами співробітникам, відповідальним за прийом та обробку повідомлень про інциденти інформаційної безпеки.

Незалежно від причини виявлення події ІБ, особа, помітивши щось незвичайне або оповіщення автоматичними засобами, несе відповідальність за ініціювання процесу виявлення й оповіщення.

Такою особою може бути будь-який представник персоналу організації, який працює постійно або за контрактом.

З метою звернення уваги на ситуацію, що виникла, він повинен дотримуватися процедур і використовувати форму звіту про події ІБ, певну систему управління інцидентами ІБ (СУІБ). Отже, важливо, щоб увесь персонал організації був ознайомлений із рекомендаціями, що стосуються оповіщення про можливі події ІБ, включаючи форми звіту, мав доступ до них і знав співробітників, яких необхідно оповіщати про кожний випадок появи події ІБ, що сприяє функціонуванню СУІБ.

Обробка конкретної події ІБ залежить від того, що вона собою являє, а також від наслідків і впливів, до яких ця подія може призвести. Ухвалення рішення про спосіб обробки події ІБ для багатьох працівників організації виходить за межі їхньої компетенції. Співробітник, який інформує про подію ІБ, повинен заповнити форму звіту таким чином, щоб у ній було якомога більше інформації, доступної йому в той момент. За необхідності він зв'язується зі своїм керівником. Бажано, щоб була форма звіту в електронному вигляді (наприклад, була надіслана електронною поштою або представлена на вебсайті організації) і її можна було передати в захищеному вигляді в групу забезпечення експлуатації (ГЗЕ), працюючу, за можливості, 24 години на добу сім днів на тиждень, а копію – керівникові групи реагування на інциденти ІБ (ГРІБ).

Для звіту про подію ІБ важлива не лише точність змісту, а й своєчасність заповнення. Уточнення змісту звіту не є достатньою причиною для затримки подання форми. Якщо співробітник, який повідомляє, не впевнений у даних, що заносяться до якогось поля, то вони позначаються особливим чином, а уточнення надсилається дещо пізніше. Також важливо розуміти, що деякі механізми електронного оповіщення (наприклад, електронна пошта) самі є часто цілями атаки.

Коли стає очевидним, що подію ІБ буде переведено в категорію особливо значного інциденту ІБ, і за наявності реальних проблем або думки про наявність проблем з установленими за замовчуванням механізмами електронного оповіщення (наприклад, через електронну пошту), включаючи можливі атаки на систему та зчитування звіту несанкціонованими особами, починаючи з ранніх стадій дослідження такої події ІБ, використовуються альтернативні засоби зв'язку – телефон, текстові повідомлення тощо.

У більшості випадків ГЗЕ повідомляє про подію ІБ для подальшої обробки відповідними особами, однак у деяких – подію ІБ за допомогою місцевого керівництва можна обробити на місці. Іноді подію ІБ можна швидко розпізнати як помилкову тривогу або успішно вирішити. У таких випадках форму звіту необхідно заповнити та надіслати місцевому керівництву, а також ГЗЕ і ГРІБ для її реєстрації в БД. Тоді особа, яка повідомляє про закриття події ІБ, надає інформацію, необхідну для заповнення форми звіту про інцидент ІБ. Далі цю форму заповнюють і відправляють до визначеної інстанції.

Як наголошується в стандартах, обробка повідомлень – важливий елемент управління інцидентами ІБ, що включає в себе сортування, визначення типу події ІБ, типу та ступеня серйозності інциденту ІБ (якщо подія ІБ визнається такою) й ін.

Саме за допомогою ефективної реалізації цього процесу можна зрозуміти, що саме відбувається в організації, та своєчасно оцінити потенційний вплив події ІБ на бізнес організації.

Відповідальний співробітник, який прийняв повідомлення про подію ІБ, проводить первісну оцінку й визначає, чи є воно повідомленням про подію ІБ або інцидент ІБ, повідомленням про уразливість або не належить до ІБ зовсім.

Оцінювання проводиться на основі отриманих відомостей про подію ІБ, експертної думки спеціаліста, який прийняв повідомлення, і прийнятих в організації класифікації інцидентів ІБ і шкали їхньої значущості.

Зазвичай інциденти ІБ поділяються за типами, наприклад, інциденти фізичної безпеки, програмно-технічні інциденти й ін. Крім того, вводиться класифікація за ступенем серйозності, щоб, насамперед, оцінити загальну ситуацію, а також визначити часові межі та пріоритети реагування на інциденти ІБ.

Якщо отримана інформація не є подією ІБ, реєструючий таке повідомлення співробітник, виходячи з аналізу повідомлення, передає цю інформацію на вхід в інші процеси управління, які здаються йому найбільше підходящими.

Якщо отримана інформація є просто подією ІБ (а не інцидентом ІБ), реєструючий таке повідомлення співробітник фіксує його в належному вигляді. Тоді подальша робота щодо події ІБ у межах процесу управління інцидентами ІБ непотрібна.

Якщо немає можливості покласти виконання завдання прийому та первинної обробки інцидентів ІБ на співробітників підрозділів ІБ, до цієї діяльності залучаються співробітники технічної підтримки або навіть ті, хто не володіє глибокими знаннями у сфері ІБ. Однак тоді буде потрібно детальне опрацювання класифікації інцидентів ІБ, а також розроблення докладних пам’яток із прикладами.

Послідовність операцій оброблення подій та інцидентів ІБ, що реалізуються на етапі процесу управління інцидентами ІБ, представлена на рис. 1.

Згідно з розробленою послідовністю дій, здійснюваних у зв’язку з виявленням події ІБ, особа, яка приймає повідомлення, підтверджує отримання заповненої форми звіту, вводить її в БД та аналізує.

Далі посадова особа отримує будь-які уточнення від особи, яка повідомила про подію ІБ, і збирає іншу необхідну додаткову доступну інформацію як від особи, котра повідомила про подію, так і з будь-якого іншого джерела. Потім представник ГЗЕ проводить оцінювання для визначення, чи підходить ця подія під категорію інциденту ІБ або є хибною. Якщо подія ІБ визначається як помилкова, заповнюється форма звіту, вона передається ГРІБ для запису в БД і подальшого аналізу, а також для створення копії для особи, яка повідомила про подію, та її місцевого керівника.

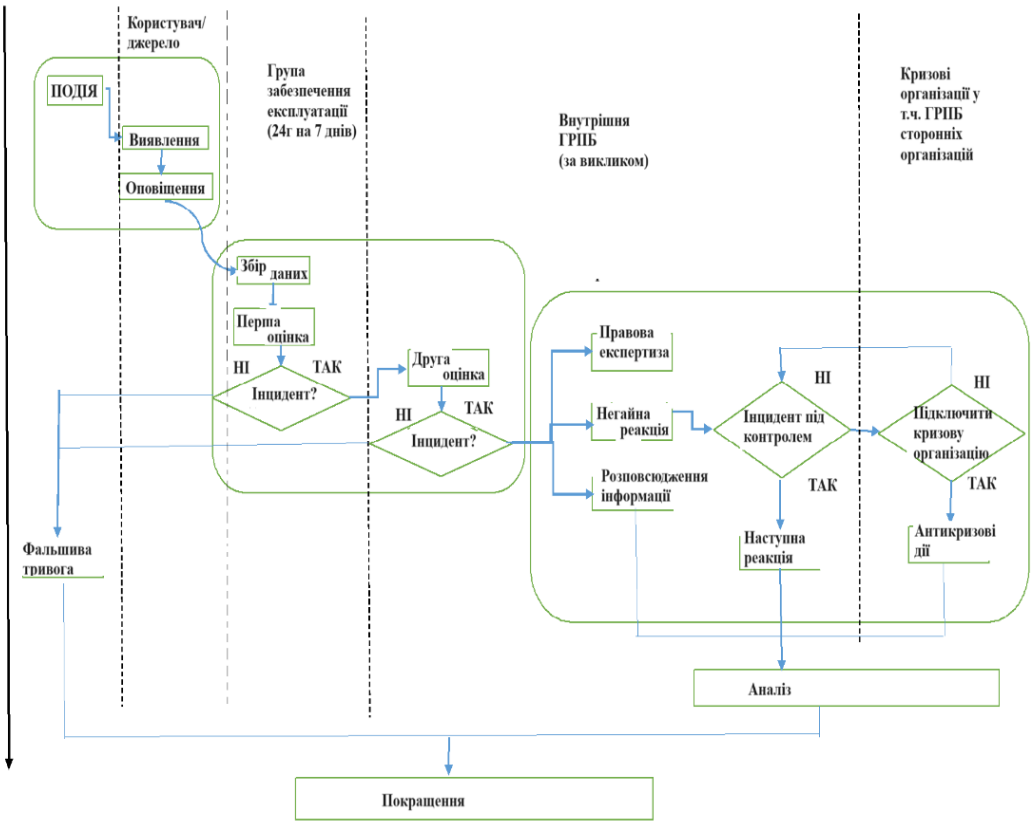

Рисунок 1 – Послідовність оброблення подій та інцидентів інформаційної безпеки в організації

Зібрані на цьому етапі інформація й інші свідчення можуть знадобитися в майбутньому при дисциплінарному або судовому розгляді. Особа, яка виконує завдання із збирання та оцінювання інформації, повинна добре знати вимоги до збирання та збереження свідчень інцидентів ІБ.

Додатково до дати й часу дій необхідно повністю документувати таке:

– проведені заходи (включаючи використані кошти) та їхні цілі;

– місце зберігання свідчення наявності події ІБ;

– спосіб архівування свідчень (якщо це доцільно);

– спосіб верифікації свідчень (якщо це необхідно);

– деталі зберігання матеріалів і подальшого доступу до них.

Якщо подія ІБ визначена як імовірний інцидент ІБ, а співробітник ГЗЕ має відповідний рівень компетентності, то проводиться подальше оцінювання. У результаті можуть знадобитися коригувальні дії, наприклад, ідентифікація додаткових «аварійних» захисних заходів і звернення за допомогою щодо їх реалізації до відповідальної особи.

Подія ІБ може бути класифікована за прийнятою в організації шкалою значущості як інцидент ІБ, причому значний. Про це інформують безпосереднього керівника ГРІБ. Може знадобитися оголошення «кризової

ситуації», і, як наслідок, повідомлення керівника забезпечення безпеки бізнесу (ЗББ) про можливу активізацію плану ЗББ з одночасним інформуванням керівника ГРІБ і вищого керівництва. Однак найімовірніша ситуація передачі інциденту ІБ безпосередньо в ГРІБ для подальшого оцінювання та виконання заздалегідь запланованих дій.

Незалежно від того, яким буде наступний крок, співробітник ГЗЕ заповнює форму звіту за можливості найбільш докладно. Ця форма містить інформацію в описовому вигляді і, наскільки це можливо, характеризує таке:

– що являє собою інцидент ІБ;

– що стало його причиною, чим або ким він був викликаний;

– на що він впливає або може вплинути;

– фактичний або потенційний вплив (збиток) інциденту ІБ на бізнес організації;

– ймовірну значущість / незначність інциденту ІБ (за шкалою серйозності, прийнятої в організації);

– як інцидент ІБ оброблявся до цього часу й відповідна оцінка правильності й ефективності дій із реагування на інцидент ІБ.

Отже, матеріали щодо інциденту ІБ, зазвичай, включають:

– перелік усіх активів організації, порушених в інциденті ІБ;

– загрози ІБ, реалізовані проти активів організації, й уразливості, що дали змогу реалізувати конкретні загрози ІБ;

– передбачувані джерела загроз інформаційній безпеці;

– дії і мотивацію зловмисника;

– використовувані для захисту порушених активів ЗЗІ;

– дії, вживані з реагування на інцидент ІБ.

Передусім визначається, який наслідок може бути при потенційному або фактичному негативному впливі інциденту ІБ на бізнес організації в результаті:

– несанкціонованого розкриття інформації;

– несанкціонованої модифікації інформації;

– відмови від наявної інформації;

– недоступності інформації та/ або сервісу;

– знищення інформації і/або сервісу.

Приклади наслідків:

• фінансові збитки / переривання бізнес-операцій;

• збиток комерційним і економічним інтересам;

• збиток інформації, яка містить персональні дані;

• порушення правових і нормативних зобов'язань;

• збої операцій з управління та бізнес-операцій;

• втрата престижу організації.

Як показують кращі практики в цій сфері, правильно проведене оцінювання інциденту ІБ дає такі результати:

– готується висновок про захищеність порушених активів, а також про причини виникнення інциденту інформаційної безпеки;

– визначається ефективність процесу реагування на інциденти ІБ;

– оцінюються правильність і своєчасність дій і рішень співробітників,

відповідальних за реагування на інциденти ІБ;

– складається висновок про збитки, завдані інцидентом ІБ, включаючи матеріальні збитки, збиток репутації, а також витрати на відновлення працездатності активів, залучених до інциденту ІБ, у повному обсязі;

– готується висновок про ефективність і правильність дій співробітників, відповідальних за активи, їхнє адміністрування тощо, а також визначається, наскільки точно виконувалися інструкції та приписи;

– виробляються рекомендації щодо запобігання інцидентам ІБ у майбутньому й удосконалення процедури реагування на інциденти ІБ.

Щодо подій ІБ, що належать до інцидентів ІБ, використовуються відповідні рекомендації з категорування потенційних або фактичних впливів для внесення їх до звіту по інцидентах ІБ. Якщо інцидент ІБ відбувся, то звіт містить деталі вжитих захисних заходів (наприклад, для запобігання повторному виникненню подібного інциденту ІБ) і отриманих уроків.

Після найдетальнішого, у міру можливості, заповнення форма звіту подається ГРІІБ для введення в БД і подальшого аналізу.

Якщо розслідування проводиться більше тижня, то зазвичай складається проміжний звіт.

Співробітник групи забезпечення експлуатації, який оцінює інциденти інформаційної безпеки, має бути озброєний різними знаннями, мати навички й інструменти для ефективного реагування на загрози. У таблиці 1 представлено основні елементи, якими має володіти такий співробітник.

Таблиця 1 – Основні елементи, якими має володіти співробітник ГЗЕ

Знання та навички			
1	Технічні знання	**Кібербезпека**	Глибокі знання про загрози, методи атак та способи захисту
		Мережеві технології	Розуміння роботи мереж, протоколів, брандмауерів, IDS/IPS систем
		Операційні системи	Знання різних ОС (Windows, Linux, macOS) та їхніх особливостей безпеки
		Безпека додатків	Розуміння принципів безпечної розробки програмного забезпечення (SDLC), вразливостей (OWASP Top 10)
2	Аналітичні навички	**Ідентифікація інцидентів**	Здатність швидко і точно виявляти інциденти інформаційної безпеки
		Аналіз логів і даних	Уміння працювати з журналами подій, аналізувати їх для виявлення аномалій

		Зворотний аналіз	Здатність проводити зворотний аналіз шкідливого ПЗ, аналіз трафіку, розборка інцидентів
3	Управлінські навички	**Координація та комунікація**	Здатність ефективно спілкуватися з іншими членами команди та керівництвом
		Вироблення стратегій	Розробка та впровадження політик і процедур для зниження ризиків та реагування на інциденти
		Оцінка ризиків	Вміння оцінювати рівень ризику інциденту та вживати відповідних заходів
Інструменти та технології			
1	Засоби моніторингу та управління інцидентами	SIEM-системи (Security Information and Event Management)	Наприклад, Splunk, ArcSight, QRadar
		Системи управління журналами (Log Management)	Наприклад, ELK Stack, Graylog
		Системи управління подіями (Incident Management)	Наприклад, ServiceNow, JIRA
2	Антивірусні та антишкідливі засоби	Антивірусне ПЗ	Наприклад, Symantec, McAfee, Kaspersky
		Антиспам та антифішинг ПЗ	Засоби для виявлення та блокування шкідливих електронних листів
3	Інструменти для аналізу трафіку та логів	Сканери мережевої безпеки	Наприклад, Wireshark, tcpdump
		Інструменти для аналізу логів	Наприклад, LogRhythm, SolarWinds
4	Інструменти для зворотного аналізу та дослідження шкідливого ПЗ	Інструменти для зворотного аналізу	Наприклад, IDA Pro, Ghidra
		Пісочниці для аналізу шкідливого ПЗ	Наприклад, Cuckoo Sandbox, FireEye
5	Системи управління доступом та автентифікацією	Системи багатофакторної автентифікації (MFA)	Наприклад, Duo Security, RSA SecureID
		Інструменти управління	Наприклад, Okta, Microsoft Azure AD

		ідентичностями (IAM)	
Безперервне навчання та сертифікація			
1	Сертифікації	CISSP (Certified Information Systems Security Professional) CISM (Certified Information Security Manager) CEH (Certified Ethical Hacker) OSCP (Offensive Security Certified Professional)	
2	Навчальні програми та курси	Курси з кібербезпеки	Наприклад, курси від SANS, Cybrary, Coursera
		Конференції та семінари	Участь у заходах із кібербезпеки, таких як Black Hat, DEF CON, RSA Conference

Тобто співробітник ГЗЕ, який оцінює інцидент ІБ на основі інструкцій, що містяться в документації СУІБ, має бути обізнаний про таке: 1) коли і кому необхідно направляти матеріали про інцидент ІБ; 2) при здійсненні всіх дій, виконуваних ГЗЕ, необхідно виконувати документовані процедури контролю змін.

За наявності проблем або думки про те, що існують проблеми з установленими за замовчуванням механізмами електронного оповіщення (наприклад, з електронною поштою), включаючи випадки атаки на ІС і зчитування несанкціонованими особами звіту про інцидент ІБ, застосовуються альтернативні засоби зв'язку – нарочиті, телефон, текстові повідомлення, а також кур'єри. Ці засоби використовуються, починаючи з ранніх стадій розслідування, коли стає очевидним, що подія ІБ буде переведена в категорію інциденту ІБ, особливо того, який уважається значним.

Друга оцінка та підтвердження інциденту ІБ або яке-небудь інше рішення щодо того, чи треба віднести подію ІБ до інциденту ІБ, входять в обов'язки ГРІІБ, що встановлено в стандартах [2].

Співробітник ГРІІБ, який приймає звіти, здійснює такі дії:

– підтверджує отримання форми звіту ГЗЕ;

– вводить цю форму в БД;

– звертається за уточненнями до ГЗЕ;

– аналізує зміст звіту;

– збирає додаткову необхідну інформацію про подію ІБ (якщо вона існує) від ГЗЕ, яка заповнила звітну форму про подію ІБ особи, або з якогось іншого джерела.

Якщо все ще є яка-небудь невизначеність щодо автентичності інциденту ІБ або повноти отриманої інформації, то співробітник ГРІІБ проводить друге оцінювання для визначення реальності чи хибності інциденту ІБ.

Якщо інцидент ІБ визначений як помилковий, заповнюється звіт про подію ІБ, він додається в БДСІІБ і передається керівнику ГРІІБ. Копії звіту передаються ГЗЕ, особі, яка повідомила про подію, та її місцевому керівникові.

Якщо інцидент ІБ визначений як реальний, то співробітник ГРІІБ, за необхідності залучаючи колег, проводить подальше оцінювання, метою якого є максимально швидке підтвердження:

– того, що являє собою інцидент ІБ, що стало його причиною, чим або ким він був викликаний, на що він вплинув або міг вплинути, фактичний або потенційний вплив на бізнес організації, вказівку на ймовірну значущість / незначність інциденту ІБ (за прийнятою в організації шкалою серйозності);

– навмисної технічної атаки порушника на деяку систему, сервіс і/або мережу, наприклад: глибини проникнення порушника та ступеня отриманого контролю над системою, сервісом і/або мережею; даних про інформацію, до якої він отримав доступ, чи були вони скопійовані, змінені або видалені; про те, яке ПЗ було скопійовано, змінено або зруйновано;

– навмисної фізичної атаки порушника на будь-яку ІС апаратної частини, сервісу і/або на мережу та/або на фізичне місце розташування, наприклад: масштаби прямих і непрямих наслідків завданої фізичної шкоди (за відсутності фізичного захисту доступу); прямих і непрямих наслідків стосовно інцидентів ІБ, побічно створених діями порушника (наприклад, чи став фізичний доступ можливим унаслідок пожежі, чи є уразливість ІС наслідком неправильного функціонування ПЗ, лінії зв'язку або помилки оператора);

– використовуваного дотепер способу обробки інциденту ІБ.

У процесі аналізу потенційного або реального негативного впливу необхідно підтвердити, якими є наслідки для бізнесу організації внаслідок інциденту ІБ:

– несанкціоноване розкриття інформації;

– несанкціонована модифікація інформації;

– відмова від наявної інформації;

– недоступність інформації та/ або сервісу;

– руйнування інформації та/або сервісу.

Для віднесення потенційних або фактичних впливів до певної категорії використовуються відповідні прийняті в організації рекомендації, які класифікують їх як інцидент ІБ, і вносяться до звіту щодо інциденту ІБ.

Отже, для ефективної обробки інцидентів потрібні відповідні дієві системи реагування й управління ними та чітке використання визначених алгоритмів дій відповідальними особами.

Висновки. Дослідження щодо вдосконалення процесів виявлення й обробки подій та інцидентів інформаційної безпеки заглиблюється в критично важливу сферу кібербезпеки. Оскільки цифровий ландшафт стає дедалі складнішим, із розповсюдженням пристроїв, даних і взаємопов'язаних систем, потрібні надійні й ефективні методи виявлення та реагування на події, пов'язані з безпекою.

Удосконалення систем виявлення є наріжним каменем покращання процесів інформаційної безпеки. Алгоритми штучного інтелекту та машинного навчання, навчені на великих масивах даних, спроможні розпізнавати тонкі ознаки компрометації, які можуть пропустити традиційні системи на основі сигнатур. Крім того, аналітика великих даних полегшує коре-

ляцію різних джерел даних, забезпечуючи повніше уявлення про ландшафт загроз і точніше їх виявлення.

Моніторинг у режимі реального часу й інтеграція розвідданих про загрози мають вирішальне значення для своєчасного та ефективного реагування на події, пов'язані з безпекою. Використання систем управління інформацією та подіями безпеки (SIEM) у поєднанні з каналами розвідки загроз розширює можливості виявлення та визначення пріоритетів загроз на основі їхньої серйозності та потенційного впливу. Розвіддані про загрози, отримані як із внутрішніх, так і зовнішніх джерел, надають цінний контекст, допомагаючи організаціям зрозуміти природу загроз і тактику, методи й процедури (ТТП), які використовують супротивники. Таке розуміння контексту має вирішальне значення для розробки цілеспрямованих та ефективних стратегій реагування.

Ефективна обробка інцидентів інформаційної безпеки потребує чітко визначених систем реагування та управління інцидентами. Дослідження показало, що важливими є класифікація та пріоритезація інцидентів, які дають можливість організаціям ефективно розподіляти ресурси та зосереджуватися на найкритичніших інцидентах. Структурована система реагування на інциденти сприяє скоординованим і своєчасним діям, зменшуючи потенційну шкоду та час відновлення, пов'язані з порушеннями безпеки.

На сьогодні вдосконалення процесів виявлення подій та обробки інцидентів інформаційної безпеки, підтримка ефективного функціонування систем моніторингу подій ІБ і дієвого алгоритму реагування на інциденти ІБ із їх подальшою обробкою є очевидним і найважливішим підходом, що дає змогу максимально використовувати можливості системи інформаційної безпеки об'єктів інформаційної діяльності із запобігання виникненню інцидентів інформаційної безпеки [3].

Удосконалення процесів виявлення й обробки подій та інцидентів інформаційної безпеки є складним і багатогранним завданням, вирішення якого потребує комплексного підходу. Технологічні досягнення, такі як машинне навчання, аналіз великих даних та SIEM-системи, є важливими інструментами в арсеналі засобів кібербезпеки. Однак потрібні ще й кваліфіковані фахівці з кібербезпеки, чітка організаційна політика та сильна культура безпеки. Цілісний та адаптивний підхід, що поєднує технології, людський фактор та організаційне управління, має вирішальне значення для ефективного управління мінливим ландшафтом загроз.

Організації повинні постійно оцінювати й удосконалювати свої заходи безпеки, щоб випереджати кіберзагрози. Це передбачає інвестиції в передові технології, розвиток і утримання талантів у сфері кібербезпеки, а також розвиток культури обізнаності та співпраці у сфері безпеки. Оскільки цифровий ландшафт продовжує розвиватися, неможливо переоцінити важливість надійних і стійких процесів виявлення й обробки подій та інцидентів інформаційної безпеки. Застосовуючи комплексний та адаптивний підхід, організації можуть краще захистити свої інформаційні активи й забезпечити їхні довгострокові безпеку та стійкість.

Виявлення подій та обробка інцидентів є невід'ємними компонентами системи управління інформаційною безпекою організації. Їхні інтеграція та ефективне впровадження відіграють ключову роль у підтримці проактивної позиції безпеки, мінімізації впливу інцидентів безпеки та забезпеченні відповідності нормативним вимогам. Використовуючи найкращі практики та постійно вдосконалюючи процеси роботи, організації можуть підвищити свою стійкість до кіберзагроз, що постійно змінюються.

Пояснення та регламент першої оцінки й попереднє рішення про події інформаційної безпеки дають можливість своєчасно та ефективно реагувати на події ІБ, які можуть бути віднесені до інцидентів ІБ.

Друга оцінка та підтвердження інциденту ІБ або яке-небудь інше рішення щодо того, чи треба віднести подію ІБ до інциденту ІБ, входять в обов'язки ГРІБ, що встановлено в стандартах. У процесі аналізу потенційного або реального негативного впливу інциденту підтверджується, які наслідки мали б місце для функціонування технологічних процесів на об'єктах інформаційної діяльності внаслідок визначеного інциденту ІБ.

Здатність організації швидко відновитися після виявленого інциденту ІБ безпосередньо пов'язана з ефективністю функціонування систем моніторингу подій ІБ, а також розумінням ступеня економічної доцільності застосування конкретних безпекових заходів стосовно прояву можливих інцидентів інформаційної безпеки.

Майбутні дослідження мають бути зосереджені на підвищенні масштабованості, точності й адаптивності систем виявлення, інтеграції нових технологій, таких як штучний інтелект і квантові обчислення, а також на розробці комплексних систем управління ризиками, що враховують динамічний характер кіберзагроз. Важливо проводити додаткові дослідження передових методів поведінкового аналізу, які враховують швидку еволюцію шкідливого програмного забезпечення та інші загрози, а також особливостей безпечної інтеграції цих методів у хмарні та мобільні середовища. Зважаючи на специфіку, інтенсивний розвиток сучасних інформаційних технологій, системний підхід до вирішення нагальних проблем у цій сфері, убачається головним своєчасне проведення безпекових заходів на об'єктах інформаційної діяльності, що належать до критичної інфраструктури [8].

Список використаних джерел

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

2. Богуш В. М., Бровко В. Д., Гордієнко С. Б., Козюра В. Д., Кудін А. М. Управління інформаційною безпекою та кібербезпекою організації : навчальний посібник : в 2 ч. Ч. 1: Основи менеджменту інформаційної безпеки та кібербезпеки. Київ : НА СБУ, 2023. 168 с.

3. Богуш В. М., Бровко В. Д., Гордієнко С. Б., Козюра В. Д., Кудін А. М. Управління інформаційною безпекою та кібербезпекою організації : навчальний посібник : в 2 ч. Ч. 2: Основи побудови системи і основних підсистем управління

інформаційною безпекою та кібербезпекою організації. Київ : НА СБУ, 2023. 208 с.

4. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. *Вісник Національного університету «Львівська політехніка»* «Автоматика, вимірювання та керування». 2013. № 756. С. 105–123.

5. ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT).

6. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT).

7. ДСТУ ISO/IEC TR 19791:2015 Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем (ISO/IEC TR 19791:2010, IDT).

8. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF (дата звернення: 24.01.2024).

9. Bruce Schneier. Harvard Kennedy School. URL: https://www.hks.harvard.edu/faculty/bruce-schneier (дата звернення: 05.02.2024).

10. General Data Protection Regulation (GDPR). Legal Text. URL: https://gdpr-info.eu/ (дата звернення: 11.01.2024).

11. Dan Geer. Harvard Kennedy School. Harvard Kennedy School. URL: https://www.hks.harvard.edu/about/dan-geer (дата звернення: 19.01.2024).

12. Data Mining Approaches for Intrusion Detection. The Advanced Computing Systems Association. URL: https://www.usenix.org/conference/7th-usenix-security-symposium/data-mining-approaches-intrusion-detection (дата звернення: 15.02.2024).

13. HIPAA Home. HHS.gov. URL: https://www.hhs.gov/hipaa/index.html (дата звернення: 05.01.2024).

14. Mihai Christodorescu. Google Scholar. URL: https://scholar.google.com/citations?user=jRnIqvkAAAAJ&hl=en (дата звернення: 03.02.2024).

15. Ross J. Anderson 1956–2024. The University of Edinburg. URL: https://informatics.ed.ac.uk/news-events/news/latest-news/ross-j-anderson-1956-2024 (дата звернення: 12.02.2024).

16. Spafford E. H., Zamboni D. Intrusion detection using autonomous agents. *Computer Netwoks*. 2000. Т. 34. № 4. С. 547–570. URL: https://doi.org/10.1016/s1389-1286(00)00136-5 (дата звернення: 12.02.2024).

17. What is a Computer Security Incident Response Center (CSIRC)? Group-IB. URL: https://www.group-ib.com/resources/knowledge-hub/csirc/ (дата звернення: 12.02.2024).

Стаття надійшла до редакції 12.03.2024

UDC 35.004

Hordiienko S. B., Kobus O. S.

ISSUES OF IMPROVING THE PROCESSES OF DETECTION AND PROCESSING OF INFORMATION SECURITY EVENTS AND INCIDENTS

Timely detection of events and processing of possible information security (IS) incidents is the most urgent issue in the conditions of information warfare and military aggression.

The article notes the special relevance of creating IS monitoring systems to solve tasks in the work process of companies that are actively expanding their arsenal of security tools to ensure information security at critical infrastructure facilities.

The essence of methods of responding to IS events and incidents and their processing, improving the processes of detection and processing of information security events and incidents, supporting the effective functioning of IS event monitoring systems is revealed.

The sequence of IS event and incident processing operations implemented at the stage of the IS incident management process using the algorithm of the first assessment and preliminary decision on events and the second assessment with confirmation of a possible information security incident is considered.

Particular attention is drawn to the fact that in the process of analyzing the potential or actual negative impact, it is necessary to confirm what consequences occurred for the organization's business as a result of the IS incident.

Practical recommendations are provided for improving the processes of identifying events and processing IS incidents, supporting the effective functioning of IS event monitoring systems, in particular, carrying out the following measures: ensuring the proper organization of the IS incident management process, which involves the development and implementation of IS incident management policies and procedures, training of personnel who will be responsible for identifying and responding to IS incidents; implementation of IS monitoring systems capable of detecting a wide range of IS events and incidents and ensuring effective processing of detected IS events and incidents; creation of an effective algorithm for responding to IS incidents, which will determine the order of actions that must be performed to eliminate detected IS events and incidents; holding regular exercises and trainings on detection and response to IS incidents, which will help staff acquire the necessary knowledge and skills to effectively detect and respond to IS incidents.

Key words: *a threat source, IS events and incidents, IS incident response process, event monitoring system, IS incident management system, event processing and correlation systems.*

DOI 10.511369/2707-7276-2024-1(37)-12
УДК 681.528.54

ДОМАРЄВ Валерій Валентинович
БОГУШ Володимир Михайлович

ВИКОРИСТАННЯ МАТЕМАТИЧНОГО АПАРАТУ НЕЧІТКИХ МНОЖИН ДЛЯ РОЗРОБЛЕННЯ МЕТОДІВ, ТЕХНОЛОГІЙ, МОДЕЛЕЙ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Зростаюча складність і взаємопов’язаність сучасних інформаційно-комунікаційних систем (ІКС) створюють значні виклики для їхньої безпеки. Традиційні заходи безпеки, часто засновані на бінарній логіці та детермінованих моделях, є недостатніми