УДК. 303.732.4:005.332.7:004.056 DOI: 10.31673/2412-4338.2025.014011

Легомінова Світлана Володимирівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0002-4433-5123

Якименко Юрій Михайлович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0002-6848-852X

Мужанова Тетяна Михайлівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0002-7435-0287

Капелюшна Тетяна Вікторівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0001-7490-6751

ВПЛИВ УПРАВЛІННЯ ІНЦИДЕНТАМИ НА ФУНКЦІОНУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Анотація. *У статті розглядаються розробка і реалізація процесу управління інцидентами інформаційної безпеки (ІБ) відповідно до кращих практик Політик безпеки ІБ. Визначені найбільш поширені інциденти ІБ.. Показані основні ключові процеси функціонування системи управління інформаційною безпекою (СУІБ), які включаються в документи Політики безпеки та виконуються на організаційному і технічному рівнях в будь-якої організації. Важливе місце у забезпеченні інформаційної безпеки організації відводиться саме процесам управління інцидентами, завдяки яким виникає необхідність у створенні і впровадженні та вдосконаленні системи управління інцидентами інформаційної безпеки (СУІБ), яка в свою чергу повинна входити в СУІБ як організаційно так і функціонально. СУІБ повинна виконувати в першу чергу основне завдання, пов'язане з організацією захисту від нових видів атак (комплексних атак, атак розподілених у часі і інші).*

Після того, як отримана підтримка від керівництва визначаються ключові особи процесу управління інцидентами і розподіл ролей між учасниками процесу. Були отримані результати досліджень, де визначені проблеми пов'язані з управлінням інцидентами.

Проаналізовані можливості SIEM-систем для використання в управлінні процесами, пов'язаними з інцидентами ІБ. Основні функції SIEM-систем зводяться до наступного: агрегація даних, кореляція подій від різних джерел, аналіз подій і сповіщення, моніторинг поведінки різних систем, сумісність з іншими системами управління безпекою, зберігання даних про події інформаційної безпеки. Запрпонований варіант об'єднання елементів структури системи SIEM у вигляді спеціальних модулів дозволить використовувати автоматизовані системи моніторингу та аналізу трафіку і тим самим допоможе виявляти та реагувати на загрози і інциденти в режимі реального часу.

Подальші дослідження можуть бути спрямовані на розробку нових методів прогнозування інцидентів та впровадження автоматизованих систем реагування на основі штучного інтелекту.

Розглянуто проблеми, які можуть виникати в організації і впливати на управління інцидентами інформаційної безпеки. До таких проблем слід віднести: відсутність підтримки керівництва, невідповідність структури організації цілям управління інцидентами, часта зміна членів групи реагування на інциденти ІБ (ГРІБ), недолік комунікаційного процесу під час спілкування, складність плану з управління інцидентами інформаційної безпеки.

Ключові слова: *інформаційна безпека, інформація, інциденти, захист, інформаційна система, DDoS-атаки, SIEM, СУІБ.*

Svitlana Lehominova
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0002-4433-5123

Yakymenko Yuryi
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0002-6848-852X

Muzhanova Tetiana
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0002-7435-0287

Tetiana Kapeliushna
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0001-7490-6751

IMPACT OF INCIDENT MANAGEMENT ON THE FUNCTIONING OF THE ORGANIZATION'S INFORMATION SECURITY MANAGEMENT SYSTEM

Abstract. *The article discusses the development and implementation of the information security incident management process (IS) in accordance with the best practices of the IS Security Policy. The most common IS incidents are identified. The main key processes of the functioning of the information security management system (ISMS) are shown, which are included in the Security Policy documents and are performed at the organizational and technical levels in any organization. An important place in ensuring the information security of the organization is given to the incident management processes, due to which there is a need to create and implement and improve the information security incident management system (ISMS), which in turn should be included in the ISMS both organizationally and functionally. The ISMS should primarily perform the main task associated with organizing protection against new types of attacks (complex attacks, attacks distributed in time, and others).*

After receiving support from management, key persons in the incident management process are identified and roles are distributed between the process participants. The results of the research were obtained, where the problems associated with incident management were identified.

The possibilities of SIEM systems for use in managing processes related to IS incidents were analyzed. The main functions of SIEM systems are as follows: data aggregation, correlation of events from different sources, event analysis and notification, monitoring the behavior of different systems, compatibility with other security management systems, storage of data on information security events. The proposed option of combining the elements of the SIEM system structure in the form of special modules will allow the use of automated traffic monitoring and analysis systems and thereby help to detect and respond to threats and incidents in real time.

Further research can be aimed at developing new methods for predicting incidents and implementing automated response systems based on artificial intelligence.

Problems that may arise in an organization and affect the management of information security incidents are considered. Such problems include: lack of management support, inconsistency of the organizational structure with the goals of incident management, frequent change of members of the IS incident response team (ISRT), lack of a communication process during communication, complexity of the information security incident management plan.

Keywords: *information security, information, protection, information system, SIEM, ISMS.*

1.Вступ. В сучасному цифровому світі питання інформаційної безпеки набуває все більшої актуальності. Кількість кіберзлочинів у світі та в Україні постійно зростає, що створює серйозні загрози для державних установ, бізнесу та окремих громадян. За даними Кіберполіції України та Deloitte, у 2023 році кількість кібератак на українські організації

зросла на 35% порівняно з попереднім роком. Основними загрозами залишаються фішингові атаки, програмне забезпечення-здирник (ransomware), DDoS-атаки та компрометація корпоративних мереж. Стрімке зростання кіберзлочинності ще обумовлено розвитком інформаційних технологій, поширенням віддаленої роботи та цифровізації бізнес-процесів.

Дослідженню процесів управління інцидентами ІБ присвячено багато публікацій. Також існує стандартизована міжнародна і національна нормативно-методологічна база, яка спрямована на вирішення питань з забезпеченням високого рівня інформаційної безпеки організацій. Найбільша частка спеціальних документів представлена стандартами, рекомендаціями і технічними звітами, в більшей частині розробленими в США, дозволяє практично виконувати їх вимоги у створенні і впровадженні систем управління інформаційною безпекою. Але актуальні питання, які пов'язані з управлінням такими процесами, як виявлення інцидентів ІБ і визначення шляхів усунення їх наслідків, залишаються складними і потребують поведення допоміжних досліджень в напрямку створення СУІБ у складі СУІБ та автоматизації самих процесів виконання, що дозволить покращити швидкість прийняття управлінських рішень і ефективність заходів безпеки в організації.

2. Постановка проблеми. В умовах, коли сучасні компанії та державні установи стикаються з постійним зростанням кількості інцидентів ІБ, саме відсутність ефективного управління такими інцидентами може призвести до витоку конфіденційних даних, фінансових втрат та репутаційних ризиків. СУІБ є невід'ємною частиною загальної стратегії захисту інформації і забезпечення ІБ організації. Вона включає в себе процеси управління ризиками, контролю доступу, забезпечення конфіденційності, цілісності та доступності даних. Однак особливе значення в СУІБ повинно відводитись процесам управління інцидентами ІБ завдяки створенню СУІІБ, яка дозволяє мінімізувати негативний вплив таких інцидентів на бізнес-процеси та репутацію організації. Цим підтверджується актуальність необхідності виконання дослідження. [1]

3. Аналіз останніх досліджень і публікацій. Різні наукові дослідження свідчать про зростаючу роль управління інцидентами ІБ, яке є ключовим елементом створеної СУІБ і визначають ефективність її функціонування. та обґрунтовується необхідність впровадження автоматизованих рішень. Згідно з дослідженням використання SIEM-систем можливо значно підвищити ефективність управління інцидентами за рахунок автоматичного збору, аналізу та кореляції подій безпеки. Дослідження підтверджують, що впровадження рішень класу SIEM дозволить на 60% скоротити час реакції на загрози та на 40% зменшити витрати на ліквідацію наслідків атак.

Так автором у статті [3] розглядається комплексна методика оцінки ефективності забезпечення ІБ, яка охоплює різні аспекти, включаючи технічні, організаційні, процедурні та людські фактори, враховуються різноманітні фактори, в тому числі з питань ІБ як фактор реагування на інциденти. Автор підтверджує актуальність і необхідність комплексного підходу щодо виявлення інцидентів ІБ, реагування на них, а також проведення аналізу інцидентів для того, щоб спланувати превентивні заходи захисту та вдосконалити процес забезпечення ІБ в цілому. Тільки створення ефективної системи управління інцидентами ІБ дозволить зменшити негативний вплив інцидентів на діяльність організації. В той же час не показано- як практично досягати цю ефективність.

В іншій роботі [5] розглядається підхід до організації процесу управління подіями ІБ для підприємства і пропонує комплексну деталізацію алгоритму підпроцесу управлінняяк "Обробка подій" відповідно до життєвого циклу подій ІБ. В той же час зовсім не показано яким чином вони переходять з подій в інциденти ІБ і що треба робити щоб не допускати їх повторення в майбутньому.

4. Мета і задачі дослідження. Метою дослідження є підвищення рівня впливу управління інцидентами на функціонування СУІБ організації за рахунок удосконалення СУІБ.

Для досягнення цієї мети потрібно виконати такі завдання:

- дослідити принципи управління інцидентами та їх реалізацію відповідно до міжнародних стандартів;
- провести аналіз реалізації СУІБ під впливом процесів управління інцидентами ІБ;
- розглянути проблеми виникнення інцидентів ІБ і шляхи боротьби з ними;
- проаналізувати методичні підходи до побудови СУІБ організації;
- оцінити переваги та недоліки різних SIEM-рішень;
- на основі аналізу використання існуючих засобів автоматизації захисту від інцидентів провести дослідження та розробити пропозиції щодо побудови СУІБ з використанням можливостей системи SIEM.

5. Виклад основного матеріалу. Однією з основних частин СУІБ є СУІІБ. Дані, що акумулюються в рамках процесів управління інцидентами ІБ, є необхідними для досить великої кількості інших процесів управління ІБ, наприклад для коректного проведення оцінки ризиків ІБ, моніторингу / аудиту ІБ, управління змінами, доступом і безперервністю бізнесу оцінки ефективності існуючих захисних заходів. Процес управління інцидентами інформаційної безпеки спрямований на ідентифікацію, аналіз, реагування та усунення загроз, які можуть вплинути на функціонування організації і призначений для виявлення, звітності, оцінки, реагування та взаємодії з іншими подіями безпеки. Іншими словами, процес управління інцидентами ІБ є своєрідним “мотором” життєвого циклу СУІБ [4].

Перелік принципів, який потрібно дотримуватися, щоб ефективно побудувати процеси управління інцидентами ІБ і оцінити їх вплив на ефективність функціонування СУІБ включає:

- безпека співробітників і відвідувачів;
- безперервний моніторинг активності в мережі і інформаційних системах;
- оперативність і автоматизація реагування на інциденти та мінімізація збитку;
- безпека активів і інформаційних ресурсів організації;
- оцінка і відновлення після інциденту;
- розслідування інциденту;
- вживання заходів по недопущенню повторення інциденту;
- використання найкращих практик (ISO 27035, NIST 800-61)

Серед найбільш поширених інцидентів інформаційної безпеки визначено [2]:

- DDoS-атаки (розподілені атаки типу “відмова в обслуговуванні”);
- шахрайство в системах дистанційного банківського обслуговування (ДБО);
- злом серверів і крадіжка конфіденційної інформації;
- витік важливих корпоративних даних;
- атака на репутацію шляхом розміщення наклепницької інформації в Інтернеті;
- фішингові атаки;
- використання шкідливого програмного забезпечення (ПЗ);
- вразливості у програмному забезпеченні.

В той же час перед службами ІБ в організаціях гостро постає питання створення і послідовного застосування правил реагування на всі випадки порушення ІБ, в тому числі і виявлення і реагування на інциденти. Такі знайомі випадки, як комп'ютер без пароля, забуті ключі на столі, пачка роздрукованих конфіденційних документів біля принтера - це тільки кілька прикладів проблем з безпекою, які можуть привести до витоку інформації. Накопичення таких випадків може довести до виникнення інциденту ІБ. Виходом із ситуації залишається тільки одне - впровадження СУІБ, заснованої на вимогах міжнародного стандарту ISO 27001 і національного ДСТУ ISO 27001.

Як показує практика і результати проведених наукових досліджень важливе місце у забезпеченні інформаційної безпеки організації відводиться саме процесам управління інцидентами, завдяки яким виникає необхідність у створенні і впровадженні та вдосконаленні СУІБ, яка в свою чергу повинна входити в СУІБ як організаційно так і функціонально [5].

СУІБ повинна в першу чергу дозволяти забезпечення виконання завдань, пов'язаних з організацією захисту від нових видів атак (комплексних атак, атак розподілених у часі і інші):

Для опису всіх процесів функціонування СУІБ, в тому числі і управління інцидентами безпеки при побудові їх систем управління в будь-якої організації використовується класична циклічна модель управління Шухарта-Демінга, як модель PDCA.

Такі компанії, як вендори: ArcSight, McAfee, IBM Qradar, Enterasys SIEM - кожна з них пропонує свої системи управління, базуючись на цієї моделі управління. [1;3] Після того, як отримана підтримка від керівництва, а менеджмент усвідомив необхідність і важливість управління інцидентами, визначаються ключові особи процесу управління інцидентами і розподіл ролей між учасниками процесу.

Після того, як визначені всі ключові ролі, їх функції, порядок ескалації і взаємодії, необхідно формалізувати та документувати сам процес управління інцидентами. Як і будь-який процес, управління інцидентами має бути циклічним та постійно удосконалюватися - шляхом тестування і циклічного поліпшення процесів, пов'язаних з управлінням інцидентами. Нижче показані проблеми, які можуть виникати в організації і впливати на управління інцидентами інформаційної безпеки.

Як показують результати досліджень [2;4;6] до проблем відносяться наступні:

Підтримка. ***Відсутність підтримки керівництва.***

- Більшість проблем виникає, якщо менеджер по ІБ діє самостійно, без залучення керівництва компанії і ключових бізнес- підрозділів;
- Нестача зустрічей і нарад.

Невідповідність. ***Структура організації не відповідає її цілям.***

- Бізнес працює в прискореному темпі і може значно змінитися протягом короткого періоду часу.
- Процес управління інцидентами може бути не в змозі впоратися зі швидкістю і характером змін, що відбуваються в організації.
- Керівництво, як правило, займається бізнес питаннями і може бути не в змозі витрачати час на управління інцидентами.
- Визначити будь-які критичні помилки і довести їх до керівництва компанії є відповідальністю менеджера по ІБ.

Плинність. ***Часта зміна членів групи реагування на інциденти ІБ (ГРІБ).***

- Розробка плану управління інцидентами може зайняти значну кількість часу при постійній взаємодії з різними зацікавленими в ньому сторонами.
- Керівник ГРІБ, як правило, або менеджер по ІБ, може зненацька покинути компанію, в результаті чого реалізація планів або вдосконалення процесу може бути зупинено. В такому випадку вдосконалення управління інцидентами може бути перенесеним на інший термін.

Спілкування. ***Недолік комунікаційного процесу.***

- Може привести до різного роду непорозумінь про необхідність управління інцидентами, планування, тестування.

Складність. ***Складність плану з управління інцидентами.***

- Пропонований план може бути хорошим і охоплювати багато питань, але це може виявитися занадто складним для сприйняття. Тим, кому він призначений можуть його не зрозуміти і як наслідок – його виконання буде неможливим. Тому слід приділяти значну увагу питанням тестування планів реагування на інциденти і їх відновленню.

В сучасних умовах функціонування СУІБ активно використовуються системи управління інцидентами та подіями інформаційної безпеки - SIEM як рішення безпеки.

SIEM-системи дозволяють централізовано виявляти аномальну активність у реальному часі та відстежувати події безпеки, аналізувати їх та автоматично реагувати на загрози, автоматично збирати та аналізувати логи з усіх компонентів IT-інфраструктури.

SIEM-системи завжди представлені додатками, приладами або послугами і використовується в основному для журналювания даних і генерації звітів. Основні функції SIEM-систем зводяться до наступного: агрегація даних, кореляція подій від різних джерел, аналіз подій і сповіщення, моніторинг поведінки різних систем, сумісність з іншими системами управління безпекою, зберігання даних про події ІБ. З відомих брендів (представлено в табл.1) для виконання таких функцій на практиці використовують SIEM-системи, які представлені в табл. 1 [6]. Проаналізувати та оцінiти переваги кожної з приведених SIEM-рішень можливо за допомогою аналізу їх основних характеристик - в порівнянні можливостей використання рішень від компаній вендорів по системам SIEM.

Таблиця 1

Основні SIEM-рішення

№	SIEM-система	Призначення та можливості
1	MaxPatrol SIEM	Моніторинг ІБ, комплексний аналіз загроз, аналіз поведінки користувачів
2	Fortinet SIEM	Кореляція подій, інтеграція з іншими засобами Fortinet, аналітика загроз
3	Security Capsule SIEM	Виявлення аномалій та аналіз подій ІБ, аномальне виявлення атак, управління логами,
4	Splunk Enterprise Security	Потужний аналітичний інструмент, гнучка інтеграція, машинне навчання
5	NeuroDAT SIEM	Реагування на загрози, виявлення аномалій за допомогою AI, аналіз поведінки користувачів
6	IBM Security QRadar	Інтелектуальний аналіз подій, висока ефективність кореляції подій
7	HP ArcSight	Централізований моніторинг, автоматизована обробка загроз, глибокий аналіз логів, масштабованість

Так, як приклад SIEM, показана структура інформаційної та кібербезпеки організації від компанії IBM Security QRadar на рис.1.

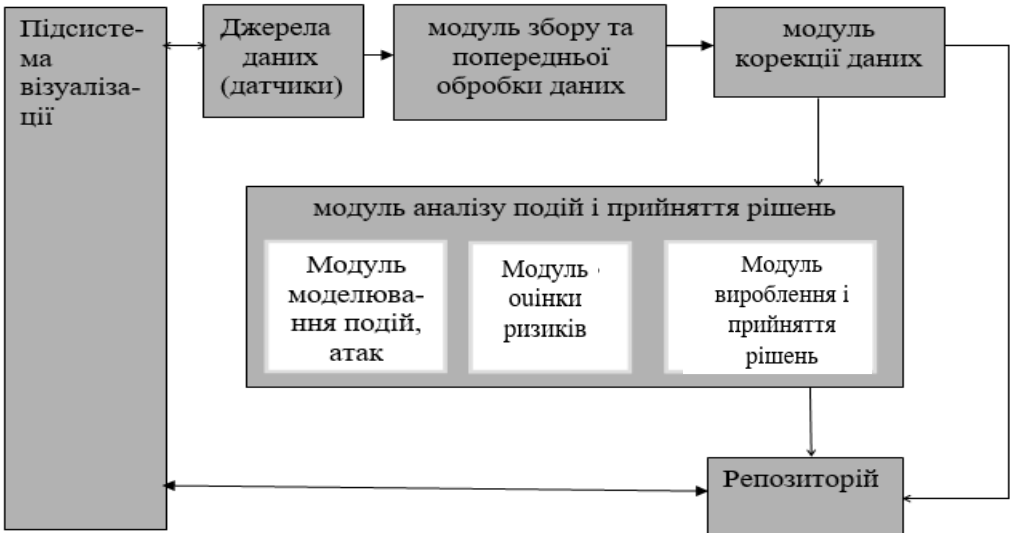

Рис. 1. Структура SIEM-системи інформаційної та кібербезпеки організації

SIEM-система IBM QRadar має відмінні можливості горизонтальної масштабованості, присутній функціонал аналізу мережевих потоків, а також можливість інтеграції з безліччю

додаткових модулів від IBM. Система забезпечення безпеки інформації може бути реалізована з використанням систем і окремих платформ: IBM QRadar SIEM, IBM QRadar Community Edition, IBM i2 Analyst's Notebook, IBM Security AppScan Standard, IBM Security Identity Manager, IBM Security Guardium. Саме ці системи забезпечення ІБ містять в собі більш надійні засоби управління. Елементи структури системи SIEM можна об'єднати і представляти у вигляді основних спеціальних модулів

6. Висновки та перспективи подальших досліджень. Отримані результати дослідження технічних впливів інцидентів на СУІБ показали, що вони можуть вимагати значних змін в інфраструктурі безпеки організації. Після інциденту може виникнути потреба в оновленні або заміні обладнання, впровадженні нових технологій захисту ІБ, таких як системи виявлення інцидентів та запобігання вторгнень (IDS/IPS). Інциденти ІБ також суттєво впливають на організаційні аспекти створення і функціонування СУІБ. Таким чином, управління інцидентами є однією з найважливіших процедур впливу на функціонування СУІБ. Як показують дослідження, висвітлення основних процесів управління інцидентами завжди пов'язано із організацією та супроводженням СУІБ.

Для покращення процесів управління інцидентами пропонується використання сучасних технологій моніторингу та захисту. Саме впровадження автоматизованих систем моніторингу на базі використання SIEM-системи та аналізу трафіку допоможе виявляти та реагувати на загрози і інциденти в режимі реального часу.

Подальші дослідження можуть бути спрямовані на розробку нових методів прогнозування інцидентів та впровадження автоматизованих систем реагування на основі штучного інтелекту.

Список використаних джерел

1. Якименко Ю. М., Мужанова Т.М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства. Економіка. Менеджмент. Бізнес.2020. №1(31). С. 64-69. URL: http://journals.dut.edu.ua/index.php/emb/article/view/2377/2277.

2. Панаско О., Бурмістров С. Практичні аспекти управління інцидентами інформаційної безпеки. Грааль науки. 2021. №5. С. 164-166. DOI:10.36074/grail-of-science.04.06.2021.030.

3. Ананченко О. Методика оцінки ефективності забезпечення інформаційної безпеки освітньої інформаційної системи. Кібербезпека: освіта, наука, техніка». 2023. №1(21). С. 297–308. DOI: https://doi.org/10.28925/2663-4023.2023.21.2973084.

4. Чернявський І. Р., Якименко Ю. М. Ризико-орієнтований підхід до управління інформаційною безпекою на підприємстві. Сучасний захист інформації. 2022. № 2(50). С. 38-44 URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2637.

5. Чубаєвський В. І. Економічна ефективність систем захисту корпоративної інформації: дис. докт. екон. наук: 08.00.04. Київ, 2023. 435 с.

6. Nabil M., Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. International Symposium on Networks, Computers and Communications (ISNCC). 2017. DOI: 10.1109/ISNCC.2017.8072035.

7. Бондарчук, А. П., Жебка, В. В. (2023). Захист гетерогенної телекомунікаційної мережі від впливу дестабілізуючих факторів. Телекомунікаційні та інформаційні технології, 2023. №(1), с. 4-16.

8. Чичкарьов, Є., Зінченко, О., Бондарчук, А., Асєєва, Л. Виявлення мережевих вторгнень з використанням алгоритмів машинного навчання і нечіткої логіки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2023. №3(19), с. 209-225.

9. Чичкарьов, Є., Зінченко, О., Бондарчук, А., Асєєва, Л. Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2023. №1(21), с. 234-251.