УДК 004.056.53

Федорієнко В. А. **(ORCID 0000-0002-0921-3390);**
Берестов Д. С., канд. техн. наук **(ORCID 0000-0002-3918-2978);**
Кульчицький О. С. **(ORCID 0000-0002-4901-0192);**
Шпура М. І., канд. військ. наук, ст. наук. співроб. (ORCID 0000-0002-3350-6003);
Онофрійчук О. А. **(ORCID 0000-0001-6495-2973)**

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Тенденції розвитку спеціального програмного забезпечення технології SIEM

Резюме. Досліджене поняття системи управління інформацією і подіями безпеки (Security Information and Events Management, SIEM), визначені завданнями, що покладаються на зазначений тип систем щодо безперервного моніторингу і управління безпекою інформації. Наведена архітектура та суть SIEM-систем. Розглянуто тенденції розвитку програмного забезпечення SIEM і варіанти його використання. Висунуті вимоги до SIEM-систем нового покоління. Проведене визначення ринку спеціального програмного забезпечення технології SIEM.

Ключові слова: SIEM; засоби захисту; інфраструктура; комп'ютерні мережі; моніторинг; DRMIS.

Постановка проблеми. Розвиток інформаційних технологій та збільшення потреб у швидкому отриманні необхідних даних, інформатизація суспільства, поширення програмної автоматизації різних гілок виконавчої влади, відповідність міжнародним стандартам вимагає від Міністерства оборони України та Збройних Сил України удосконалення системи управління. Це необхідно для підвищення якості та результативності у керуванні обороноспроможністю держави [1, 2]. Зважаючи на розвиток інформаційних технологій у світі та значний науково-технічний і фаховий потенціал вітчизняних виробників, дієвим шляхом відповідності до зазначених умов є створення цілісного комплексу інформаційної інфраструктури (ІІ) Міністерства оборони (МО) України [3].

Ураховуючи складність ІІ МО України, питання її захисту є вкрай важливими. З огляду на широкий обсяг різних за характером і змістом задач, доцільним є покладення в основу технології моніторингу інформаційної інфраструктури технології управління інформацією і подіями безпеки (Security Information and Events Management, SIEM). Технологія SIEM здобула широке розповсюдження в світі. Основною метою побудови і функціонування SIEM є управління (реалізованого через механізм активного моніторингу) рівня інформаційної безпеки в інформаційній інфраструктурі завдяки забезпеченню можливості в режимі, близькому до реального часу, маніпулювати інформацією про безпеку та здійснювати управління інцидентами і подіями безпеки.

Поряд із системною та функціональною інтеграцією інформаційних систем останнім часом стала активно розвиватися інтегральна інформаційна безпека (ІІБ), під якою розуміється такий стан умов функціонування людини, об'єктів, технічних засобів та систем, за якого вони надійно захищені від усіх можливих видів загроз під час безперервного процесу підготовки, зберігання, передачі і обробки інформації [2-4].

В умовах інтенсивного розвитку і впровадження інформаційних і телекомунікаційних технологій МО України, як і в провідних державах світу, приділяється особлива увага питанням забезпечення безпеки інформаційної інфраструктурі управління оборонними ресурсами. У Програмі розвитку Збройних Сил України до 2020 року та визначених цілях, закладених в Стратегічному оборонному бюлетені України [5], визначені завдання щодо управління плануванням оборонними ресурсами (Defence Resource Management Information System, DRMIS, стратегічна ціль 4).

Аналіз основних досліджень і публікацій. У площині дослідження технологій SIEM широко розкриті питання аналізу, кореляції, моделювання даних та візуалізації попереджень про порушення політики безпеки інформаційних систем у роботах [6-8].

Деякі питання дослідження щодо побудови захищенної інформаційної інфраструктури управління оборонними ресурсами для Міністерства оборони України,

зокрема технологій систем класу ERP (Enterprise Resource Planing), викладені у [8, 9]. Проте питання щодо особливостей розвитку спеціальних програмних засобів, що потенційно можуть входити до складу центру управління інформаційною безпекою інформаційної інфраструктури Міністерства оборони України, досліджені поверхнево. Отже, аналіз тенденцій розвитку програмного забезпечення SIEM, що належить до сукупності програмних засобів для захисту інформаційної інфраструктури цього центру, є актуальною задачею.

Метою статті є аналіз основних тенденцій та вимог до програмних продуктів технології SIEM, які можуть висуватися до центру управління інформаційною безпекою інформаційної інфраструктури Міністерства оборони України.

Виклад основного матеріалу. Основні вимоги замовників до системи побудованій за технологією SIEM є моніторинг безпеки та підготовка звітності відповідно до систем, користувачів, даних і додатків.

Наявність вразливостей у комп'ютерних системах, різноманітність видів комп'ютерних атак, їх непередбачуваний характер, територіальна і тимчасова розподіленість засобів захисту мережевої інфраструктури призводить до зміщення пріоритетів на користь технології проактивного захисту інформації, які здійснюють безперервний моніторинг і управління безпекою інформації у комп'ютерних мережах і системах. В основі таких технологій лежить своєчасний збір даних про події безпеки, що фіксуються в записах журналів аудиту комп'ютерної інфраструктури, їх зберігання в спеціалізованому сховищі та подальша обробка. Така обробка включає кореляцію, моделювання, вироблення попереджень і рішень щодо протидії атакам і відновлення безпеки інформації. Відповідно, під окремою системою, що реалізує технологію моніторингу і управління безпекою інформації, розуміється "система управління інформацією і подіями безпеки" (Security Information and Events Management, SIEM) [5, 6].

Поняття SIEM-системи. З огляду на характер і зміст задач захисту інформаційної інфраструктури МО України, є доцільним включити до проєкту базисних систем концепцію SIEM-системи. Для цього розглянемо докладніше зміст поняття SIEM. Основною метою побудови і функціонування SIEM-систем є управління інформацією і подіями безпеки через забезпечення можливості у режимі, близькому до реального часу, маніпулювати інформацією про безпеку та здійснювати проактивне управління інцидентами і подіями безпеки.

Технологія SIEM містить дві складові:

SIM – управління журналами, аналітика та звітність про відповідність рівню безпеки;

SEM – моніторинг і керування інцидентами в режимі реального часу для подій, пов'язаних із безпекою від мереж, пристроїв безпеки, систем та додатків.

Для досягнення цієї мети SIEM-система, на прикладі системи управління оборонними ресурсами DRMIS, повинна мати можливість успішного вирішення такого комплексу завдань:

збору, обробки та аналізу подій безпеки, що надходять у систему з множини гетерогенних джерел;

виявлення в режимі реального часу атак і порушень критеріїв і політик безпеки;

оперативного оцінювання захищеності інформаційних, телекомунікаційних та інших критично важливих ресурсів;

аналізу та управління ризиками безпеки DRMIS;

проведення розслідувань інцидентів;

виявлення розбіжності критично важливих ресурсів і бізнес-процесів з внутрішніми політиками безпеки і приведення їх у відповідність;

прийняття ефективних рішень щодо захисту інформації;

формування звітних документів.

Основними вихідними даними, які використовуються SIEM-системою для вирішення зазначених завдань, є записи різних журналів (logs), де протоколюються події в DRMIS, так звані, "події безпеки". Ці події відображають такі дії користувачів і програм, які можуть вплинути на безпеку. Із загальної кількості подій безпеки SIEM-система має знаходити такі, які свідчать про атаки чи інші небажані дії в DRMIS, причому традиційні методи пошуку такої інформації досить трудомісткі.

Архітектура SIEM-системи. Як правило, SIEM-система має архітектуру, що містить такі елементи, як агенти, сховище даних, сервер додатків. Відповідно, ці елементи є складовими захищеної інформаційної інфраструктури [6].

Агенти виконують збір подій безпеки, їх первісну обробку і фільтрацію. Зібрана і відфільтрована інформація про події безпеки надходить у сховище даних або репозиторій, де вона зберігається у внутрішньому форматі

уявлення з метою подальшого використання і аналізу сервером додатків. Сервер додатків реалізує основні функції захисту інформації. Він аналізує інформацію, збережену в репозиторії, і обробляє її для вироблення попереджень або управлінських рішень щодо захисту інформації.

Отже, в SIEM-системі можна виділити три архітектурних рівня її побудови (рис. 1) [10]: 1 - збір даних; 2 - управління даними; 3 - аналіз даних.

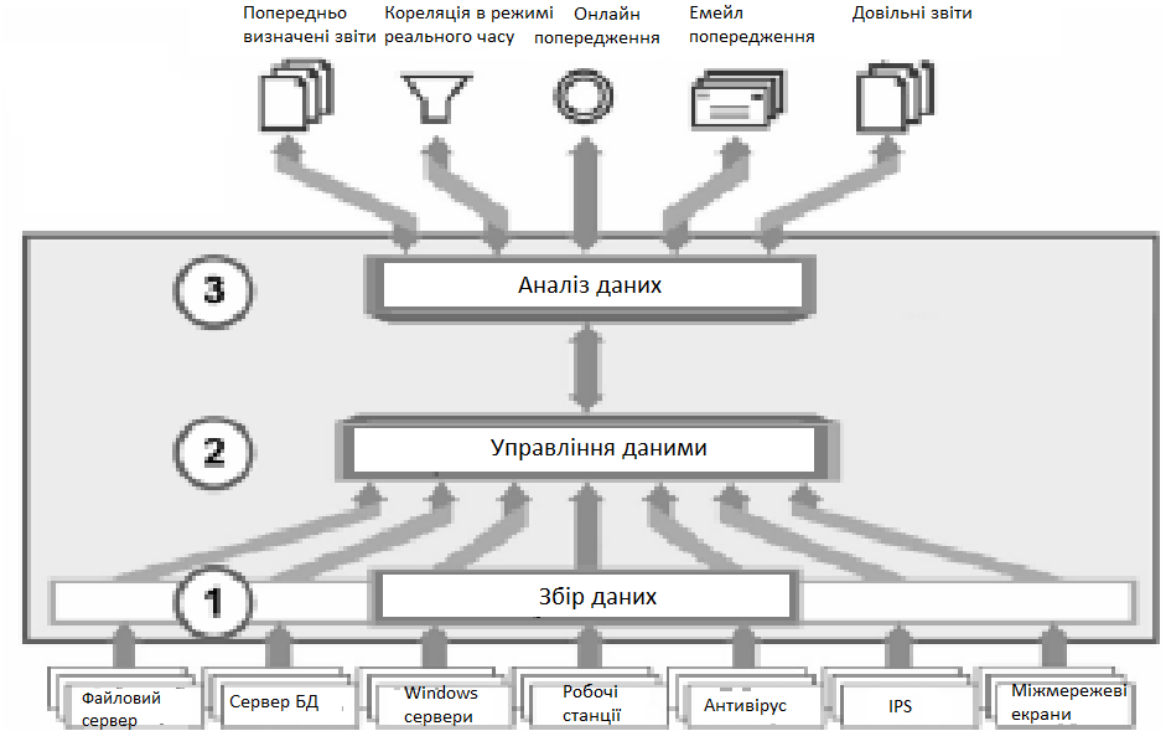

Рис. 1. Архітектура типової SIEM-системи

На першому рівні (рис. 1) збір даних здійснюється від джерел різних типів. До таких належать: файлові сервери, сервери баз даних, Windows-сервери, міжмережеві екрани (МСЕ), робочі станції, системи протидії атакам (Intrusion Prevention Systems, IPS), антивірусні програми тощо. Перелік прикладів можливих джерел даних DRMIS про події безпеки схематично наведено на рис. 2.

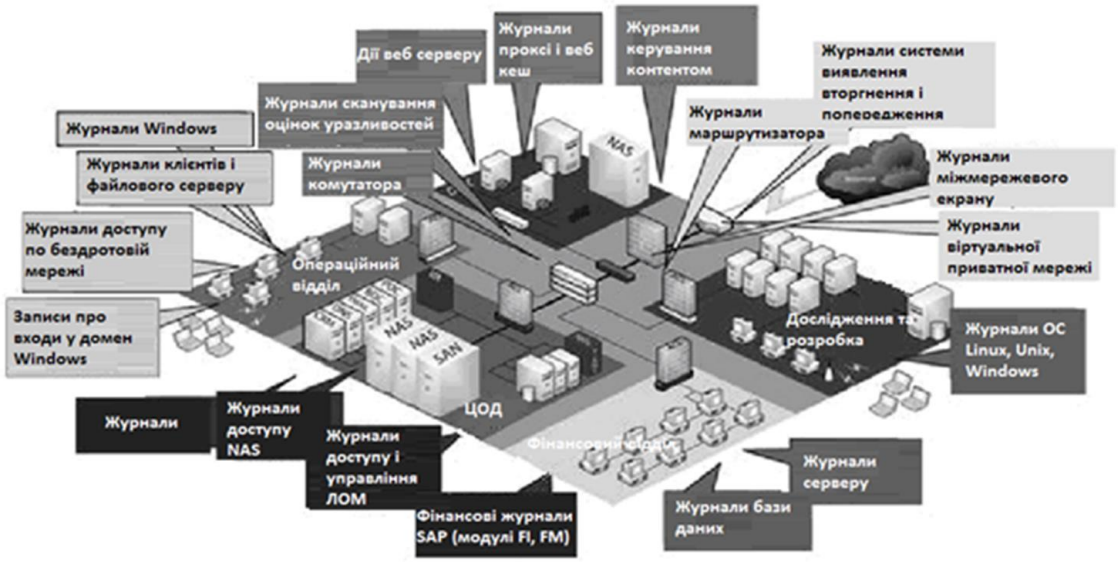

Рис. 2. Приклади джерел даних про події безпеки

На другому рівні (рис. 1) здійснюється управління даними про події безпеки, які зберігаються в репозиторії. Дані, що зберігаються в репозиторії, видаються за запитами моделей аналізу даних. Результатами обробки інформації в SIEM-системі,

одержуваними на *третьому рівні*, є звіти в умовній і довільній формі, оперативна (on-line) кореляція даних про події, а також попередження, що виробляються в режимі on-line і (або) передаються по електронній пошті.

Тенденції SIEM. Системи управління інформаційною безпекою та подіями безпеки визначається потребою аналізувати ці події в режимі реального часу для раннього виявлення цілеспрямованих атак і порушень даних, а також для збирання, зберігання, аналізу, дослідження та звітування про подібні події відповідно до напрацьованих інцидентів, положень кримінального кодексу та відповідність нормативним актам.

Інструменти SIEM агрегують ці події, створені засобами безпеки, мережевою інфраструктурою, системами та додатками. Зазначимо, що інструменти SIEM також можуть обробляти різні форми даних, такі як Net Flow, мережеві пакети, контекстну інформацію про користувачів, активи, загрози та вразливості, які можуть бути знайдені всередині або за межами підприємства (організації), і які можуть корисно поповнити журнали та вихідні дані. Усі ці дані нормалізуються, для того, щоб події, дані та контекстна інформація з різних джерел могли бути корельовані та проаналізовані для конкретних цілей, а саме: управління загрозою, моніторинг безпекових подій у мережі (SEM), моніторинг активності користувачів, звітування та реагування. Інструменти забезпечують взаємозв'язок подій у режимі реального часу для моніторингу безпеки, включають запити та аналітику побудовану на основі історичного аналізу та здатні надати звітну підтримку для розслідування випадків порушення відповідності.

Тенденції SIEM представлені удосконаленням деяких механізмів та інструментів у програмному забезпеченні SIEM виробниками технологій виходячи із видозмінення загроз та реагування на них. Зокрема, SIEM-система нового покоління орієнтується на інфраструктуру сервісів, у якій обробка подій безпеки відрізняється інтелектуальністю, високою масштабованістю, багаторівністю і багатодоменністю. До того ж має бути реалізовано випереджаюче управління безпекою, а так само надійний і стійкий збір даних про події.

Тенденції SIEM визначають *варіанти застосування сучасних SIEM-систем*. Технологія SIEM зазвичай використовується для підтримки трьох основних варіантів використання:

1. Розширене виявлення загрози - моніторинг, сповіщення в режимі реального часу і довгостроковий аналіз та звітність про тенденції і поведінку щодо активності користувачів, доступу до даних та активності додатків. Виявлення загрози включає в себе інтеграцію загроз та бізнес-контексту, у поєднанні з ефективними спеціальними можливостями запитів.

2. Основний моніторинг безпеки - управління журналами, звітування про відповідність та базовий моніторинг окремих елементів контролю безпеки в режимі реального часу.

3. Розслідування та реагування на інциденти – використання інформаційних панелей і можливостей візуалізації, а також підтримка робочого процесу та документації для ефективного виявлення, розслідування і реагування на інциденти.

Вимоги, яким має задовольняти SIEM-система нового покоління можна розділити на три групи:

1) розширення рівнів застосування;

2) розширення можливостей по оцінці та кореляції подій;

3) розширення технічних можливостей.

Як наслідок, можна сформулювати такі загальні функціональні вимоги до SIEM-систем нового покоління:

висока надійність;

міжрівнева кореляція;

висока масштабованість;

гнучкість і динамічність механізмів реагування;

зручність користувача;

довірливість;

економічність;

синергетичність;

реалізація;

виконання моделювання та оцінювання ризиків;

зворотний зв'язок і моніторинг.

Огляд ринку SIEM. За оглядом аналітичної компанії Gartner [11, 12], її клієнти-користувачі програмних продуктів SIEM, зосереджені на випадках використання цієї системи для безпеки, причому відповідність нормативним документам, зазвичай, є вторинною вимогою. З кращих практик респондентів Gartner, процес організації безпеки являє собою поліпшення можливостей щодо виявлення зовнішніх і внутрішніх загроз та управління інцидентами, що часто призводить до використання системи рівня

SIEM. Як наслідок, існують певні вимоги щодо діяльності користувачів та моніторингу доступу до ресурсів для хост-систем і програм.

На рис. 3 наведений, так званий, магічний квадрант Гартнера (Gartner's Magic Quadrant), який відображає ступінь задоволення зазначених вимог.

Рис. 3. Рейтингування програмних платформ управління інформаційною безпекою та подіями безпеки за методологією Gartner

Відповідно до звітів компанії Gartner (рис. 3) в число лідерів увійшли такі SIEM-системи: IBM, Splunk, LogRhythm і McAfee [11]. Ринок SIEM продовжує домінувати порівняно небагатьма великими постачальниками – Micro Focus (включаючи ArcSight) [13], IBM, McAfee (раніше – Intel Security) і Splunk, які дають понад 60 % доходу від ринку. Менші постачальники SIEM, як правило, орієнтовані на певні сегменти ринку.

Провідні постачальники SIEM продовжують зосереджуватися на цілеспрямованому виявленні атак та порушення за допомогою включення інтелекту загроз, аналітики, профілювання та виявлення аномалій, а також моніторингу кінцевої точки і мережної активності.

Провідні програмні продукти SIEM мають інтеграцію з великими платформами даних завдяки наявним власним адаптерам, або опцій з відкритим вихідним кодом (Hadoop). Низка постачальників із внутрішніми можливостями досліджень (моніторингу та аналізу) безпеки (IBM, McAfee, RSA і Trustwave) забезпечують інтеграцію із власним інтелектуальним контентом стосовно загрози. Постачальники, які мають SIEM і MSSP (EventTracker, IBM та Trustwave), є маркетинговими розробками, що впроваджують технології SIEM, які включають в себе низку послуг моніторингу. Rapid7 і FireEye пропонують сервіси SIEM.

Аналізуючи ринок SIEM програмних продуктів можна стверджувати, що попит на технологію SIEM залишався сильним за останні три роки. Ринкова вартість SIEM продуктів зросла з 2 млн до 201 млрд дол. США у 2015 році, і до 2 167 млрд дол. США у 2016 році [14]. Управління загрозою є основною функціональністю, а загальний моніторинг і відповідність вимогам залишаються вторинною. На третьому місці – звітність про дотримання вимог орієнтованих на безпеку.

Вважається, що ринок SIEM є зрілим і досить конкурентоспроможним. Найбільша область незадоволеної потреби – ефективне виявлення цілеспрямованих атак і порушень. Організації не в змозі виявляти раннє порушення, серед них понад 80 % порушень. Ситуацію можна поліпшити, використовуючи інформацію про загрозу, профілювання поведінки та ефективну аналітику. Постачальники SIEM продовжують збільшувати свою підтримку можливостей

аналізу поведінки, а також інтеграції з сторонніми технологіями.

Висновки. Таким чином, використання спеціального програмного забезпечення технології SIEM значно підвищить рівень інформаційної безпеки в інформаційно-телекомунікаційної інфраструктурі. У роботі проведений аналіз основних тенденцій та вимог до програмних продуктів технології SIEM, які можуть висуватися до центру управління інформаційною безпекою інформаційної інфраструктури Міністерства оборони України.

Отже, програмні рішення технології SIEM мають відповідати таким критеріям:

підтримки збирання та аналізу подій у реальному часі від зовнішніх систем, пристроїв безпеки та мережевих пристроїв у поєднанні з контекстною інформацією загроз, користувачів, активів та даних;

забезпечення довгострокового зберігання даних, контекстних даних та аналітики;

надання попередньо визначених функцій, які можуть бути налаштовані, щоб відповідати вимогам замовника (організації);

максимальної простоти для розгортання та підтримки.

Надалі доцільно визначити особливості організації, перелік основних функцій та завдань щодо створення центру управління інформаційною безпекою інформаційної інфраструктури Міністерства оборони України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України № 80/94-ВР від 05.08.1994 зі змінами. [Електронний ресурс] // Міністерство оборони України. – 2014. – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
2. Постанова КМ України “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” № 373 від 29 березня 2006 року. [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/ control/uk/publish/ article?art_id=47960&cat_id=38834.
3. Про затвердження Концепції інформатизації Міністерства оборони України. Наказ МО України № 650 від 17.09.2014 [Електронний ресурс] // Міністерство оборони України. – 2014. – Режим доступу до ресурсу: www.mil.gov.ua/content/other/ MOU650_2014.pdf.
4. Information and Event Management (SIEM) Implementation / Miller, Harris, Harper та ін.]. – New York: McGraw–Hill Companies, 2011. – 465 с.
5. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” [Електронний ресурс]: указ [видано Президентом України 06 червня 2016 р. №240/2016]. – Режим доступу: http://www.president.gov.ua/ documents/2402016-20137.
6. Kotenko I., Chechulin A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing, Besanson, France, Nov. 20-23, 2012 / Los Alamitos, California. IEEE Computer Society, 2012. – P. 94-101.
7. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода/ И. В.Котенко, И. Б. Саенко, О. В. Полубелова, А. А. Чечулин. // Тр. СПИИРАН. – 2013. – №26. – С. 23–30.
8. Кондратенко Ю. В. Візуальний аналіз політик безпеки в ERP-системах / Ю. В. Кондратенко, І. Г. Зотова, В. В. Грицюк // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2018. –№ 1. – С. 68-73. – Режим доступу: http://nbuv.gov.ua/UJRN/ Znpcvsd_2018_1_13.
9. Шляхи створення захищеної ІТ-інфраструктури Збройних Сил України / Ю. А. Кірпічніков, Ю. В. Кондратенко, Д. С. Берестов [та ін.] // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2015. – № 1. – С. 140-144. – Режим доступу: http://nbuv.gov.ua/UJRN/ Znpcvsd_2015_1_24.
10. Modeling modern network attacks and countermeasures using attack graphs / [K. Miller, M. Chu, R. Lippmann та ін.]. // Annual Computer Security Applications Conference. – 2009. – С. 117–126.
11. Kavanagh K. M. Magic Quadrant for Security Information and Event Management [Електронний ресурс] / K. M. Kavanagh, T. Bussa // Gartner Reprint. – 2018. – Режим доступу до ресурсу: https://www.gartner.com/doc/reprints?id=1-4LC8PAW&ct=171130&st=sb.
12. Reviews for Security Information and Event Management (SIEM) [Електронний ресурс] // Gartner, Inc. – 2018. – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/security-information-event-management/vendors.
13. Shenk J. ArcSight Logger Review. [Електронний ресурс] / J. Shenk // A SANS Whitepaper. – 2009. – Режим доступу до ресурсу: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview.
14. Gartner “Прогноз: інформаційна безпека у світі у 2015-2021 рр.”, оновлене видання 2017 року

Стаття надійшла до редакційної колегії 24.05.2019

Федориенко В. А.;
Берестов Д. С., канд. техн. наук;
Кульчицкий А. С.;
Шпура Н. И., канд. воен. наук, ст. науч. сотрудник;
Онофрийчук О. А.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Тенденции развития специального программного обеспечения SIEM

Резюме. Исследовано понятие системы управления информацией и событиями безопасности (Security Information and Events Management, SIEM), определены задачи, возлагаемые на указанный тип систем относительно непрерывного мониторинга и управления безопасностью информации. Приведенная архитектура и суть SIEM-систем. Рассмотрены тенденции развития программного обеспечения SIEM и варианты его использования. Выдвинуты требования к SIEM-системе нового поколения. Проведено определение рынка SIEM.

Ключевые слова: SIEM; средства защиты; инфраструктура; компьютерные сети; мониторинг; DRMIS.

V. Fedoriienko;
D. Berestov, PhD (Technical);
O. Kulchitskiy;
N. Shpura, PhD (Military), senior researcher;
O. Onofriychuk

Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

Trends in the development of SIEM software

Resume. It was explored the concept of security information and events management (SIEM), defining the tasks assigned to the specified type of systems for continuous monitoring and information security management. There are architecture and essence of SIEM systems in this article. The trends of SIEM software development and variants of its use are considered. Requirements have been made for SIEM-systems of the new generation. The definition of the SIEM market is carried out.

Keywords: SIEM; security; infrastructure; computer networks; monitoring; DRMIS.