УДК 004.056.53 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/107-113

Федорієнко В. А. (0000-0002-0921-3390)
Кульчицький О. С. (0000-0002-4901-0192)
Розумний О. Д. (0000-0003-3225-8375)

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

Особливості спеціального програмного забезпечення управління подіями безпеки для системи DRMIS

Резюме. У статті визначено особливості спеціального програмного забезпечення управління подіями безпеки SIEM для єдиної інформаційної системи управління оборонними ресурсами (DRMIS) у рамках функціонування центру управління інформаційною безпекою в інформаційних системах SOC. Запропонована система обробки даних та експертних оцінок дасть змогу визначити захищеність інформаційної системи під час побудови програмної компоненти системи захисту інформації. Розкрито особливості найбільш застосованих моделей оцінювання захищеності за визначеними метриками.

Ключові слова: спеціальне програмне забезпечення SIEM; обробка даних; кібернетичний простір; інформаційна безпека; події інформаційної безпеки.

Постановка проблеми. Проведення злочинних заходів щодо втручання у функціонування роботи державних інформаційних систем для їх блокування та витоку інформації зумовлюють перегляд та уточнення основних принципів і підходів до захисту інформаційної інфраструктури Міністерства оборони (МО) України в умовах загроз у кібернетичному просторі.

Першим кроком захисту інформаційної інфраструктури вважається використання спеціально програмного забезпечення (СПЗ) системи менеджменту інформаційною безпекою та моніторингу подій (Security Information and Event Management, SIEM). *Другим кроком* – розгляд цієї системи як програмної складової центру управління інформаційною безпекою (Security Operation Center – SOC), що є досить поширеним рішенням для великих організацій, підприємств, урядових та оборонних відомств. Центр безпеки або SOC виконує функції вчасного і швидкого реагування на події під час спроби впливу на працездатність і цілісність системи управління. Такі кроки є доцільними для забезпечення функціонування єдиної інформаційної системи управління оборонними ресурсами (DRMIS) Міністерства оборони України.

Програмна компонента SIEM, яка є ключовим СПЗ SOC базується на принципах своєчасного оповіщення щодо змін стану інформаційної безпеки на основі менеджменту подій. Тут під *подією* розуміється потенційний результат певних дій, які за допомогою впливу на інформацію або інші компоненти інформаційної системи можуть прямо або опосередковано призвести до заподіяння шкоди даним, а також ставлять під загрозу захищеність інформаційних ресурсів того чи іншого об’єкта чи суб’єкта інформаційної діяльності. Залежно від величини ризику інформаційній безпеці, за своїм наслідком події можна кваліфікувати, як ті, що призводять до загрози інформаційній безпеці, порушення цілісності, конфіденційності та доступності інформації.

У статті зосереджено увагу на дослідженні особливостей СПЗ менеджменту інформаційної безпеки та моніторингу подій під час побудови програмної компоненти системи захисту інформації центру безпеки у DRMIS у складі інформаційної інфраструктури МО України.

Аналіз останніх досліджень і публікацій. Дослідженням особливостей роботи запропонованих систем управління подіями під час захисту інформаційних систем присвячені роботи [1–5], у яких розкриті застосовані моделі оцінки захищеності за визначеними метриками.

Питання застосування методів експертного оцінювання моніторингу подій у процесі побудови програмної компоненти системи захисту інформації центру безпеки під час підтримки прийняття рішення стосуються досліджень І. Котенко [2]. У джерелах наукових праць [6–8], процес експертного оцінювання якості захисту інформаційних систем описується за визначеними критеріями з урахуванням сфери компетентності експертів та ваг кожного з експертів. У роботі [3] задачу щодо підбору системи управління подіями та визначення якості захищеності інформаційних систем пропонується вирішити на основі узагальненої ієрархічної моделі. Проте питання щодо особливостей СПЗ для управління подіями безпеки для системи DRMIS інформаційної інфраструктури МО України досліджені поверхнево.

Метою статті є аналіз особливостей системи управління подіями безпеки технології SIEM у складі SOC для обґрунтування рекомендацій щодо їх реалізації у системі DRMIS Міністерства оборони України.

Виклад основного матеріалу. Уперше поняття управління інформаційною безпекою та моніторингу подій (SIEM) було введене Марком Ніколетта та Амріта Вільямсом з компанії Gartner у 2005 році. Вони описали функціональність збору, аналізу та подання інформації від мережевих пристроїв і пристроїв безпеки, додатків ідентифікації (управління обліковими даними) та доступу, інструментів підтримки політики безпеки і відстеження вразливостей, операційних систем, баз даних і журналів додатків, а також відомостей про зовнішні загрози для здійснення раціонального управління інформаційною безпекою та підтримки прийняття рішень.

Технологія SIEM складається з двох сегментів. *Перший* – сегмент систем управління безпекою (SEM*)* – здійснює моніторингом у реальному часі та управлінням подіями шляхом співставлення їх відповідності (кореляції), повідомленням для відображення результатів на кінцевих пристроях. *Другий* – сегмент управління інформаційною безпекою (SIM) – забезпечує довготривале зберігання, аналіз і звітність за накопиченими даними. У міру зростання потреб у додаткових можливостях функціональність технології SIEM безперервно розширюється і доповнюється. Узагалі, SIEM-система – це програмна компонента технології захисту, яка виконує такі функції:

аналіз події та створення попередження за певних аномаліях: мережевого трафіку, несподіваних дій користувача, невпізнаних пристроях тощо;

перевірка системи захисту на відповідність стандартам захищеності;

створення гнучких інформативних звітів (наприклад, щоденний звіт про інциденти, щотижневий звіт порушників, звіт щодо працездатності пристроїв і т. ін.);

проведення моніторингу подій від пристроїв, серверів, критично важливих систем і створення відповідних оповіщень для визначених осіб;

проведення збору доказової бази за інцидентами;

за наявності сканера вразливостей, SIEM-система частково впливає на зміну ризиків.

Відповідно до звіту світової аналітичної компанії Gartner до лідерів виробників технології SIEM увійшли системи: IBM, Splunk, LogRhythm і McAfee. Ринок SIEM продовжує домінувати порівняно небагатьма постачальниками – Micro Focus, IBM, McAfee і Splunk, які дають понад 60 % доходу від ринку. Інші постачальники SIEM, як правило, орієнтовані на певні сегменти ринку. Огляд ринку та загальні тенденції розвитку технології SIEM наведені у роботі [9].

Технологія SIEM покладена в основу SOC, який, зі свого боку, відповідальний за виконання завдання щодо підтримки прийняття рішення стосовно інформаційної та кібербезпеки на організаційному та технічному рівнях. Центр безпеки є об’єктом, де корпоративні інформаційні системи (вебсайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп’ютери та інше кінцеве обладнання) контролюється, оцінюється та захищається. Тобто, SOC є комплексом програмно-технічних засобів, кваліфікованого персоналу та процесів їхньої взаємодії.

Передумовами щодо можливості використання організаційно SOC на основі СПЗ SIEM стали появи різного роду загроз інформаційній безпеці. Зокрема, найбільша з них – масштабна хакерська атака з боку Росії проти України у 2017 році з компрометації системи оновлення програмного забезпечення для подання звітності до контролюючих органів та обміну юридично значущими первинними документами між контрагентами в електронному вигляді (M.E.Doc) з

використанням різновиду вірусу “Petya”. Ця атака спричинила порушення роботи українських державних підприємств, установ, банків, медіа тощо. Унаслідок атаки було заблоковано діяльність таких підприємств, як аеропорт “Бориспіль”, ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств. Зараженню піддалися інформаційні системи Міністерства інфраструктури, Кабінету Міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв’язку України.

Зазвичай SOC базуються на СПЗ системи безпеки інформації та SIEM, яка агрегує та корелює дані із системних каналів безпеки, мережевого каналу передачі даних та системи оцінювання вразливостей і складається з:

підсистеми управління, ризику та дотримання (Governance, Risk and Compliance, GRC);

підсистеми оцінки та моніторингу вебсайтів, прикладних програм і сканерів баз даних;

інструментів тестування проникнення;

підсистеми виявлення вторгнень (Intrusion Detection System, IDS);

підсистеми запобігання вторгненню (Intrusion prevention system, IPS);

підсистеми управління журналами;

аналітичної підсистеми поведінки в мережі та налагодження інтелектуальної безпеки Cyber threat;

підсистеми бездротового запобігання вторгненню;

брандмауерів, корпоративних антивірусних баз та уніфікованого управління загрозами (Unified Threat Management, UTM).

Основна увага приділяється управлінню повноваженнями користувачів і служб, сервісів директорій та іншим змінам конфігурації, а також забезпеченню аудиту та моніторингу журналів, реакцій на інциденти.

Загальна технологічна схема проходження подій, які призвели до порушення інформаційної безпеки із попередженням пріоритету події та її впливу на систему захисту за їх функціональними рівнями наведена на рис. 1.

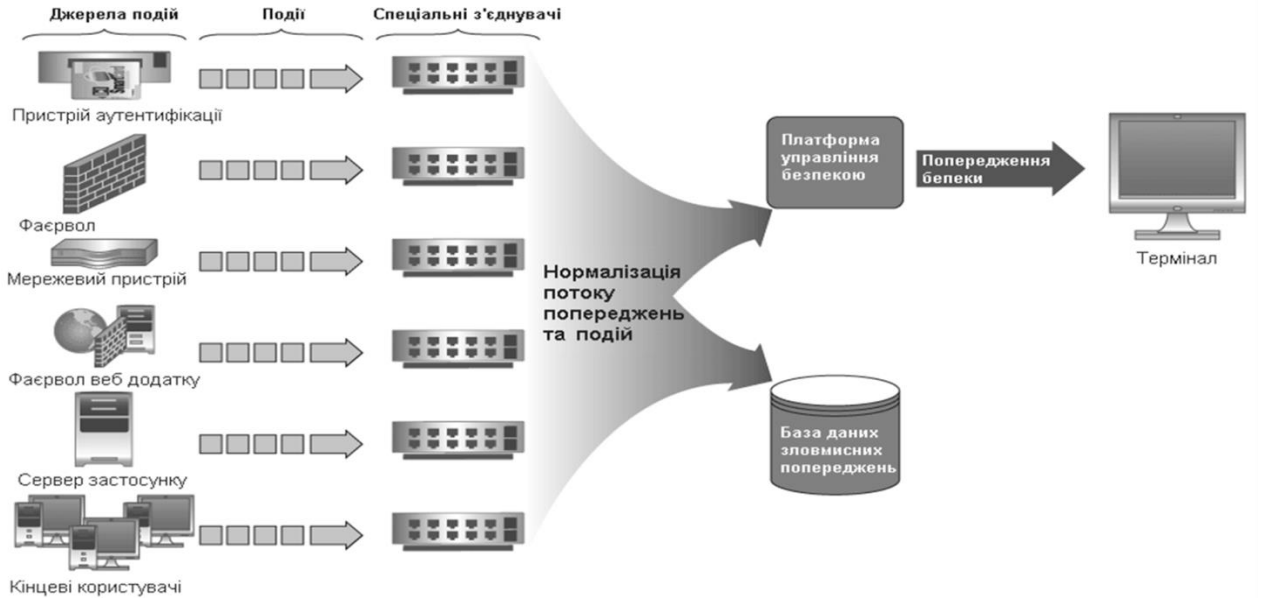

Рис. 1. Технологія SIEM, як основа програмних рішень SOC

Збір даних про події з боку порушників здійснюється від джерел різних типів. Приклади можливих джерел даних про події, які впливають на безпеку інформаційної системи наведено на рис. 1. *Джерела подій* представлені пристроями захисту входу в систему, записами у системних журналах та діями користувачів. Через зазначені джерела подій можливі вторгнення порушника (фізичної особи чи зловмисного програмного коду) в інформаційну систему. Джерела фіксують події, які дають змогу виявити ознаки порушення інформаційної безпеки та завдяки спеціальним з’єднувачам нормалізувати потік попереджень і подій. Наприклад, порушники намагаються ввійти в інформаційну систему в обхід стандартних процедур входу. На такі події технологія SIEM формує базу даних порушників (база даних зловмисних попереджень) для аналітиків безпеки та для моніторингу установи (організації) загалом.

Під час створення інформаційних систем нормативно-правовою базою [4] передбачено виконання комплексу заходів щодо захисту інформації. Одним із таких заходів є розроблення моделі загроз і моделі порушника. Після аналізу потенційних загроз безпеці, використання системи SIEM та обраного способу захисту з'являється можливість щодо автоматичного використання зазначених моделей за допомогою моніторингу попереджень подій Як наслідок, система дасть змогу ідентифікувати порушників за встановленими сценаріями. Пропонується класифікувати таких порушників інформаційної безпеки на внутрішніх і зовнішніх.

Зовнішні порушники підрозділяються на дві категорії: категорія I (особи, які не мають права доступу до контрольованої зони інформаційної системи) і категорія II (особи, які мають право постійного або разового доступу до контрольованої зони інформаційної системи). До зовнішніх порушників категорії I відносяться колишні співробітники та сторонні особи, які діють в ініціативному порядку. До зовнішніх порушників категорії II відносяться представники злочинних організацій.

До *внутрішніх порушників* відносяться співробітники з різними правами доступу до компонентів системи, персонал, який не має легітимного доступу до компонентів системи, і особи зі сторонніх організацій, які мають прямий або непрямий доступ до компонентів інфраструктури.

Зважаючи на визначені загрози та розроблені моделі порушника розроблюються вимоги до системи захисту інформації в інформаційних системах МО України.

Під час дослідження були визначені завдання, структура та шляхи побудови системи захисту інформації в інформаційній інфраструктурі МО України на основі запропонованого концептуального програмного технологічного рішення SIEM.

Рекомендовані заходи, які визначають можливість упровадження системи захисту інформації в інформаційній інфраструктурі МО України слід вважати:

забезпечення побудови максимально деталізованих ланцюжків та схем взаємозв'язку між подіями;

визначення фізичного і логічного поділу даних за різними сховищами з поділом повноважень за доступом;

визначення достатньої кількості інтеграційних механізмів до зовнішніх систем інцидент-менеджменту, звітності та візуалізації для отримання даних;

забезпечення стабільної роботи унаслідок зростання навантаження в потоці подій, під час роботи великої кількості кореляційних правил та здійсненні ретроспективних пошуків і формування звітності.

Як правило, SIEM-система має архітектуру "агенти – сховище даних – сервер додатків", яка розгортається поверх захищеної інформаційної інфраструктури. Це дає підстави в SIEM-системі виділити три основні функціональні рівні в її побудові – збір, обробка та аналіз даних (рис. 2):

На першому рівні збір даних здійснюється від джерел різних типів. До таких належать: файлові сервери, сервери баз даних, Windows-сервери, міжмережеві екрани, робочі станції, системи протидії атакам (Intrusion Prevention Systems, IPS), антивірусні програми тощо.

На другому рівні здійснюється обробка даних про події безпеки, які зберігаються в репозиторію. Дані, що зберігаються в репозиторію видаються за шаблонними запитами, які вбудовані в аналітичний інструментарій системи. Запити можуть бути сформовані користувачем та виконуватися інтерактивно або в автоматичному фоновому режимі виконання програм.

На третьому рівні результатами обробки даних у SIEM-системі є звіти у стандартній чи довільній формі, оперативна (on-line) кореляція даних про події, а також попередження, що виробляються в режимі on-line і (або) передаються електронною поштою.

Реалізація зазначених функціональних рівнів SIEM-системи здійснюється на основі виконання комплексу різних механізмів функціонування, а саме серверів, робочих станцій, антивірусу тощо. У SIEM-системах першого покоління до таких механізмів, як правило, відносяться нормалізація, фільтрація, класифікація, агрегація, кореляція і пріоритезація подій, а також генерація звітів і попереджень. У SIEM-системах нового покоління до їх числа додані – аналіз подій, інцидентів та їх наслідків, а також процес підтримки прийняття рішень із його візуалізацією.

Розподіл зазначених механізмів за трьома рівнями ієрархії SIEM-системи наведено на рис. 2.

Рис. 2. Узагальнена ієрархічна модель SIEM-системи (за трьома рівнями)

З рис. 2 видно, що відносна величина складності обробки даних є пропорційна кількості подій. Тобто, зі зростанням кількості подій зменшується якість їх моніторингу, а саме, на *якість* моніторингу подій безпеки SIEM впливають правила нормалізації, способи налаштування джерел, пакети з правилами виявлення загроз, інструкції з активації джерел, описів правил детектування, рекомендації про реагування, у разі спрацювання правил. Це пояснюється застосуванням більшої кількості механізмів (інструментів) на кожному наступному (вищому) рівні обробки, що виокремлює найбільш значущі події, які достатні для проведення різних типів аналізу, візуалізації, прийняття рішення тощо.

На рис. 3 наведено підсистеми функціональної моделі SIEM, які відповідають трьом функціональним рівням: збору даних (охоплює підсистему збору даних, може охоплювати підсистему сховища), обробку даних (охоплює підсистему обробки) та аналізу даних (охоплює підсистеми аналізу, сховища та вигляду).

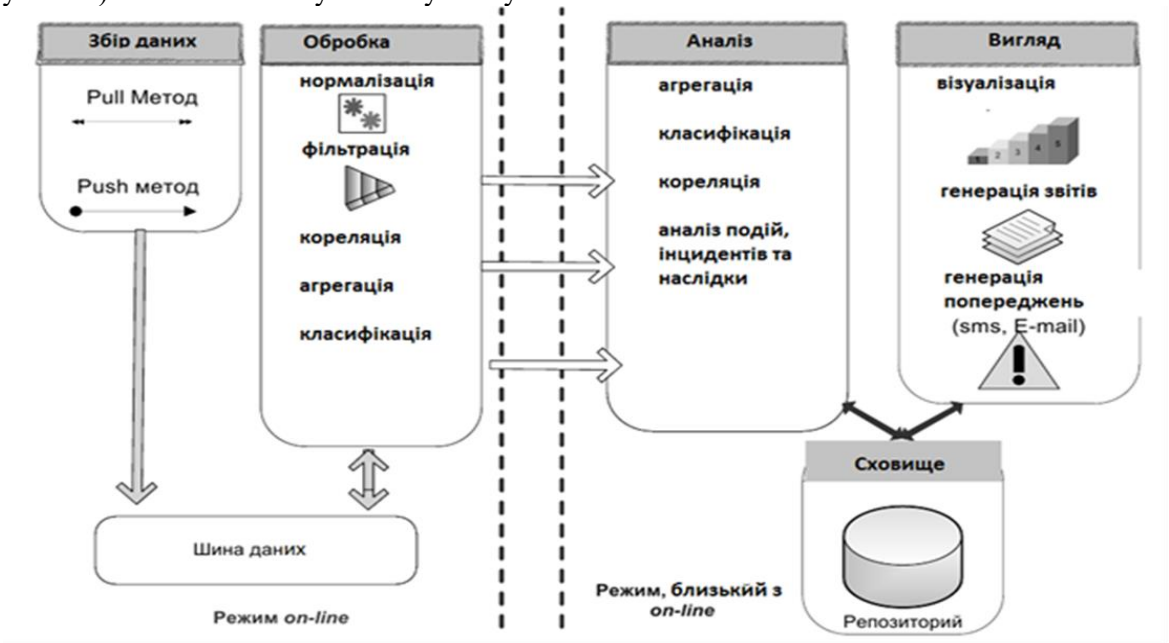

Рис. 3. Функціональна модель SIEM-системи (п'ять підсистем)

Як видно з рис. 3, в SIEM-системі можна виділити п'ять основних функціональних підсистем: збір даних, обробка, зберігання, аналіз, вигляд. До того ж перші дві функціонують у режимі online, інші – у близькому до нього. Дамо коротку характеристику цим підсистемам.

Підсистема збору даних. Для отримання інформації від джерел використовуються два основні методи: Push-(натисни) і Pull-(тягни). Суть методу Push полягає в тому, що джерело саме посилає дані записів своїх журналів подій в SIEM-систему. У методі Pull система сама здійснює процес отримання даних з журналів подій у SIEM-систему.

Підсистема обробки даних. Основні функції підсистеми полягають у зборі, видачі, накопиченні, збереженні та обробці великих

обсягів інформації. Збір інформації проводиться різного роду периферійними засобами, наприклад, через канали зв'язку за допомогою модемів, локальних та глобальних комп'ютерних мереж, різного роду датчиків тощо.

Підсистема аналізу даних. Призначена для організації моделювання даних, забезпечення процедур їх перетворення та поєднаного аналізу шляхом генералізації, агрегації, встановлення параметрів і обмежень за допомогою моделюючих функцій.

Підсистема зберігання даних – це сховище з програмно-апаратним рішенням з організації надійного зберігання інформаційних ресурсів та надання гарантованого доступу до неї споживачам. Ця підсистема може бути як частиною, так і основою підсистеми збору даних.

Підсистема вигляду. Візуалізація подій мережі призначена для консолідації і обробки інформації про роботу обладнання мережі. Перевага системи складається в формуванні візуальної картини стану роботи обладнання в режимі реального часу. Підсистема дає змогу:

реєстрації, редагування і перегляду подій, які надходять від різних об'єктів мережі;

формування, узгодження і обробки заявок на планові роботи в мережі;

централізованого зберігання переліку обладнання мережі;

доступу споживачів до головного і регіональних сховищ бази даних обладнання і подій у мережі;

візуалізації подій у мережі на електронних картах;

формування різноманітної статистики та звітності роботи обладнання;

настроювання і застосування ключових показників ефективності для моніторингу роботи обладнання мережі;

формування і зберігання звітів про події мережі, планових і аварійно-відбудовних роботах;

виводу інформації на екран монітору.

Пропонуються рекомендації щодо реалізації СПЗ управління подіями безпеки (SIEM) для функціонування єдиної інформаційної системи управління оборонними ресурсами DRMIS інформаційній інфраструктурі МО України:

1. Відповідальні особи за управління безпекою та управління ризиками мають визначити вимоги до програмно-технічного комплексу системи SIEM та форм звітності (визначення вимог має включати критерії для подальших етапів розгортання).

2. Проєкт реалізації СПЗ має включати рішення груп відповідальних за аудит, адміністрування, ідентифікацію, інформаційні технології, програмування.

3. Організація чи установа має надати опис топології розміщення мережі та системи, а також оцінені показники подій для подальшого вироблення рішення для конкретного варіанта розгортання системи.

4. Проєкт реалізації СПЗ має включати вимоги до поетапного розгортання та вдосконалення.

Типовим прикладом готового програмного продукту управління подіями безпеки є IBM TSIEM (Tivoli Security Information and Event Manager), який в області подання та зберігання подій використовує запатентовану методику W7 (Who, did What, When, Where, Where-from, Where to and on What). Відповідно, всі події трансформуються у єдиний формат, зрозумілий адміністраторам безпеки, аудиторам і управлінцям. Також, програмний продукт IBM TSIEM володіє розвиненими можливостями щодо формування звітів і моніторингу активності користувачів.

SIEM-система нового покоління [9] 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 також надійний і стійкий збір даних про події.

Висновок. Отже, у статті було визначено роль і місце СПЗ управління подіями безпеки для функціонування єдиної інформаційної системи управління оборонними ресурсами DRMIS. Під час визначення програмної компоненти центру безпеки інформаційної інфраструктури та під час дослідження проблематики пошуку програмних рішень щодо створення SOC були надані рекомендації щодо реалізації СПЗ управління подіями безпеки з актуалізацією дослідження сучасних підходів за напрямом моніторингу та управління безпекою інформації. У результаті були досліджені рівні програмного компоненту системи захисту інформації в інформаційних системах, запропоноване технологічне рішення та шляхи побудови щодо впровадження системи захисту інформації в інформаційній інфраструктурі МО України.

Подальші дослідження слід присвятити аналізу програмно-технічної та організаційної складових SOC.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Information and Event Management (SIEM) Implementation / Miller, Harris, Harper та ін. New York: McGraw–Hill Companies, 2011. 465 с.
2. 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.
3. 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.
4. Information and Event Management (SIEM) Implementation / Miller, Harris, Harper та ін. New York : McGraw–Hill Companies, 2011. 465 с.
5. 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.
6. Magic Quadrant for Security Information and Event Management / K. M. Kavanagh, T. Bussa // Gartner Reprint. 2018. URL: https://www.gartner.com/doc/reprints?id=1-4LC8PAW&ct=171130&st=sb (дата звернення: 19.02.2021).
7. Reviews for Security Information and Event Management (SIEM). 2018. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendors (дата звернення: 19.02.2021).
8. Shenk J. ArcSight Logger Review. *A SANS Whitepaper*. 2009. URL: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview (дата звернення: 18.02.2021).
9. Тенденції розвитку спеціального програмного забезпечення технології SIEM / В. А. Федорієнко, О. С. Кульчицький та ін. // Збірник Наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2019. № 2 (66). С. 82–88.

Стаття надійшла до редакційної колегії 24.02.2021

Features of special software for ensuring secure events management of DRMIS system

Annotation

Carrying out criminal measures to interfere in the functioning of state information systems to block and leak information, lead to a revision and clarification of the basic principles and approaches to protecting the information infrastructure of the Ministry of Defense (MO) of Ukraine in cyber threats.

This article focuses on the study of the features of SDR information security management and event monitoring in the construction of the software component of the information protection system of the security center in a single information system for defense resources management DRMIS as part of the information infrastructure of the Ministry of Defense of Ukraine.

An event is a potential result of certain actions that, by influencing information or other components of an information system, may directly or indirectly cause data harm, as well as endanger the security of information resources of an object or subject of information activity.

The purpose of the article is to analyze the features of the security event management system of SIEM technology in the SOC to substantiate the recommendations for their implementation in the DRMIS system of the Ministry of Defense of Ukraine.

The first step in protecting the information infrastructure is the use of special software (SPZ) of the Information Security and Event Management (SIEM) system.

The second step is to consider this system as a software component of the Security Operation Center SOC, which is a fairly common solution for large organizations, businesses, government and defense agencies. The Security Center or SOC performs the functions of timely and rapid response to events in an attempt to affect the performance and integrity of the management system. Such steps are appropriate to ensure the functioning of the Unified Defense Resources Management Information System (DRMIS) of the Ministry of Defense of Ukraine.

Keywords: special SIEM software; Data Processing; cyberspace; informational security; information security events.