https://www.sworldjournal.com/index.php/swj/article/view/swj19-01-029
DOI: 10.30888/2663-5712.2023-19-01-029

УДК 004.056.5

SYSTEM NETWORK SECURITY MONITORING IN THE SIEM-EDR-NDR TRIAD

СИСТЕМНИЙ МОНІТОРИНГ МЕРЕЖЕВОЇ БЕЗПЕКИ В ТРІАДІ SIEM-EDR-NDR

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Fedorchenko V.V. / Федорченко В.В.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *У роботі розглянуто ідею побудови системи захисту інформації, методи та засоби безпекового моніторингу мережі, сучасні підходи захисту інформації в рамках SOC та ідею системного моніторингу мережі в рамках моделі тріади SIEM-EDR-NDR. Проаналізовані та класифіковані поточні загрози інформаційній безпеці (ІБ). Згадані принципи побудови системи ІБ. Наведено приклади ефективного використання систем SOC і SIEM-EDR-NDR для забезпечення безпеки мережі. Розглянута взаємодія трьох компонентів тріади SOC між собою та їх взаємодоповнення.*

Ключові слова: *Інформаційна безпека, загрози ІБ, системний моніторинг, мережева безпека SIEM, EDR, NDR, SOC.*

Вступ.

Згідно стандарту ISO/IEC 27005 [1–3] роботи з підготовки системи захисту інформаційно-комп'ютерних мереж (ІКМ) рекомендується проводити так: дослідити активи, що потребують захисту; дослідити потенційні загрози та їх джерела; дослідити можливі вразливості активів; сформулювати політики безпеки; підготувати рекомендації щодо засобів захисту ІКМ; оцінити вартість запропонованих рішень (рис. 1). Червоним кольором виділені ті пункти, де відбувається моніторинг мережевої безпеки.

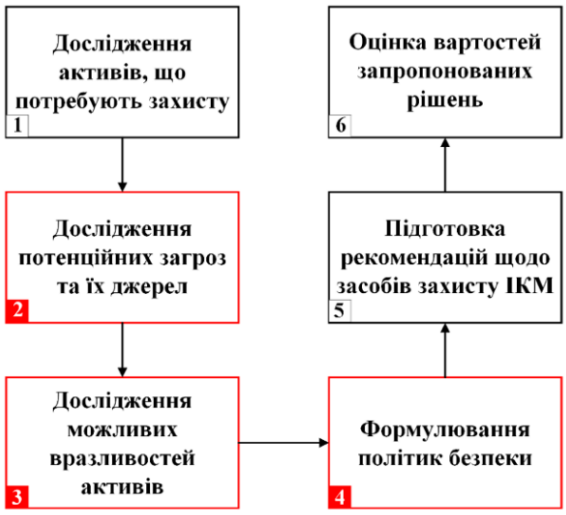

Рисунок 1 – Узагальнений план підготовки системи захисту ІКМ
Авторська розробка

За визначенням, активами є все, що має цінність для компанії і має бути захищеним [1]. Активами є: приміщення, де розміщена ІКМ; інформація, яка обробляється і зберігається в мережі; засоби ІКМ: програмні і технічні (сервери, мережеві і кінцеві пристрої, засоби і лінії зв'язку тощо) [2]. Всі активи повинні бути ідентифіковані і облікові. Експерти мають визначити цінність активів (низька, середня, висока) відносно їхньої втрати чи пошкодження. На рис. 2 зображена загальна схема дослідження активів, що потребують захисту.

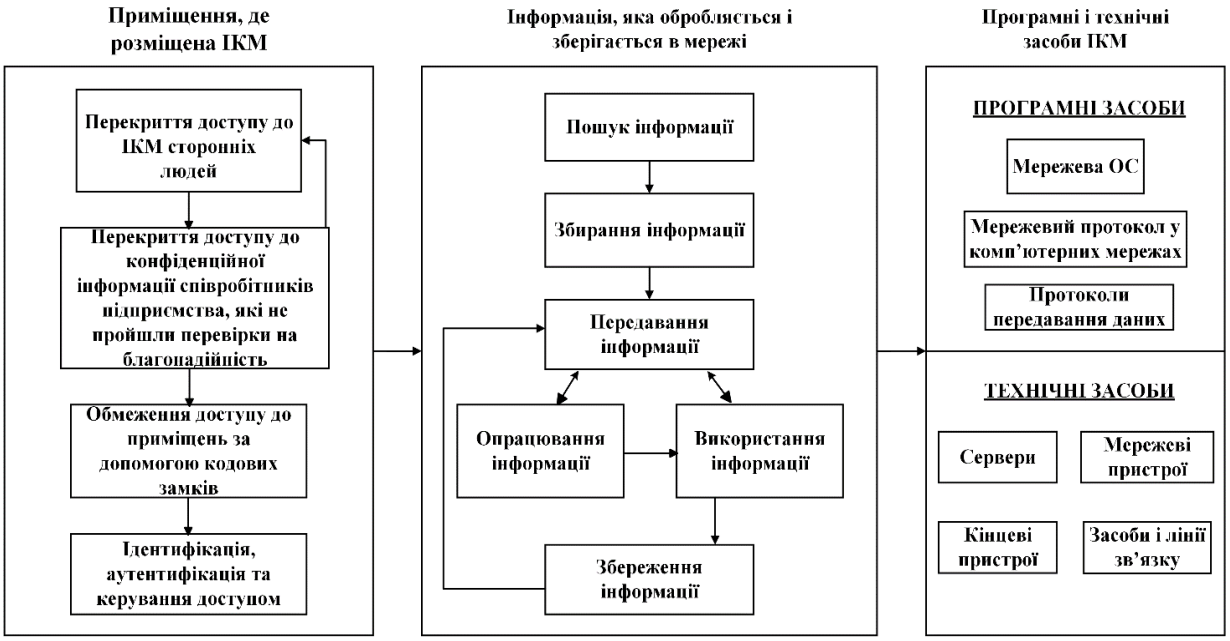

Рисунок 2 – Узагальнена схема дослідження активів для їх захисту

Авторська розробка

Інформаційна безпека (ІБ) – це комплекс заходів для забезпечення ЗІ від загроз [4]. Загроза має потенціал заподіяння шкоди активам. Необхідно ідентифікувати як випадкові і навмисні загрози та їх джерела. Типові загрози ІБ можуть бути класифіковані [5]: за аспектом ІБ, на який спрямовані загрози; за розміщенням джерела загроз; за ступенем впливу на ІКМ; за природою виникнення. Джерелами загроз можуть бути суб'єкти (особи), та об'єктивні прояви (конкуренти чи злочинці). Джерела загроз мають такі цілі: ознайомлення з даними, що охороняються, їх модифікація і знищення для завдання прямої матеріальної шкоди. Далі зв'яжемо кожен актив із відповідними видами загроз. Результатом аналітичної обробки опрацьованих літературних джерел [4, 6] стала схема загальної класифікації загроз ІБ (рис. 3).

Уразливість – це нестача активу або заходів захисту, яка може бути використана зловмисником [6]. Із їх загального переліку можна виділити такі: людський фактор; уразливості ОС; віддалений доступ; зовнішні мережеві підключення; засоби захисту та моніторингу; ПЗ.

Після дослідження активів захисту системи, їх потенційних загроз і вразливостей, формуються політики ІБ ІКМ. Згідно зі стандартом ISO/IEC 27002 [4], політика ІБ – це цільовий пакет нормативних, організаційно-розпорядчих та експлуатаційних документів, що охоплюють сфери організації, управління та

контролю безпеки і експлуатації засобів захисту. Цей пакет складається з документів трьох рівнів.

На 1-му рівні формується головний документ – «Концепція інформаційної безпеки», який визначає цілі і принципи системи ЗІ в ІКМ, а також вимоги і загальні правила управління ІБ. Документи 2-го рівня розробляються на підставі «Концепцій» і містять: порядок поводження з конфіденційною інформацією, основні правила дій користувачів та їх відповідальність; технічні вимоги до програмно-апаратних засобів захисту, включно із системним ПЗ. На підставі документів 2-го рівня розробляються документи 3-го рівня, які містять [4]: конкретизовані і доповнені посадові інструкції; експлуатаційні документи засобів захисту інформації (ЗІ). Отже, основною ціллю забезпечення інформаційної безпеки є ЗІ від випадкового чи навмисного втручання. Водночас ІБ також покликана зберігати неперервність бізнесу.

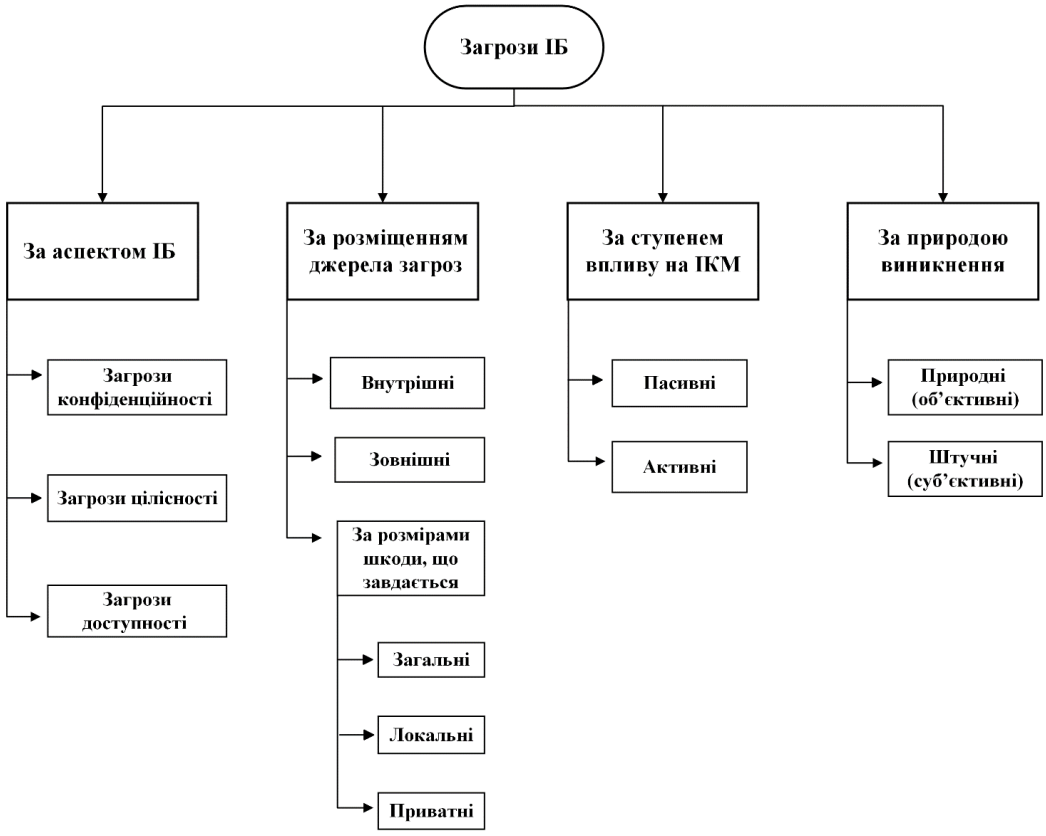

Рисунок 3 – Узагальнена класифікація загроз ІБ

Авторська розробка

У таблиці 1 вказані основні загальноприйняті принципи побудови системи ІБ. Примітка: в таблиці 1.1 використані такі скорочення: СЗ – система захисту; BYOD – Bring Your Own Device, особисті мобільні пристрої, яким дозволений доступ до ІКМ; PDCA – Plan-Do-Check-Act, модель безперервного поліпшення процесів.

Під час формування принципів політики ІБ враховують основні вимоги щодо інформації і за моделлю CIA (Confidentiality-Intengrity-Availabity): конфіденційність; цілісність; доступність. Для виконання політик ІБ реалізується ціла низка заходів.

Таблиця 1 – Принципи побудови системи інформаційної безпеки

Назва принципу	***Суть принципу***
Комплексний підхід	СЗ інформації повинна бути комплексною, охоплювати організаційні заходи, технічні та програмні засоби.
Системний підхід	Всі заходи і засоби захисту повинні бути пов'язані, узгоджені і забезпечувати цілісність системи.
Багаторівневість	Згідно із завданням тут повинен бути реалізований принцип поглибленого багаторівневого захисту .
Тотальність	Система захисту повинна охоплювати всі активи, всі вузли та кінцеві пристрої ІКМ, у тому числі BYOD.
Достатня надійність	Створення механізмів захисту, щоб вартість зламу системи була дорожчою за саму інформацію.
Повнота контролю	Будь-яке звернення до інформації має охоплювати всі рівні контролю: інформацію, ПЗ, апаратуру, персонал.
Цикл Демінга «PDCA»	Цикл моделі «PDCA» передбачає обов'язкові етапи: 1) Встановлення цілей та політик СЗ (Plan); 2) Реалізацію і впровадження СЗ (Do); 3) Оцінку, контроль, моніторинг і аналіз роботи СЗ (Check); 4) Покращення (удосконалення і розвиток) СЗ (Act).

Авторська розробка

1 Поняття, методи та засоби безпекового моніторингу мережі.

На виконання політики ІБ в компанії створюється система захисту ІКМ, яка призначена здійснювати неперервний моніторинг мережевої безпеки. В процесі цього моніторингу виявляються та усуваються кіберзагрози у мережі. Він здійснюється відповідним ПЗ: ідентифікації та аутентифікації користувачів; управління доступом користувачів; захисту від шкідливого ПЗ; контролю цілісності інформації.

У комплексному захисті мережі особливе місце займають спеціалізовані мережеві засоби захисту такі, як системи управління інформацією про моніторинг мережі (англ. SIEM – Security Information and Event Management) [8], системи виявлення загроз кінцевим точкам мережі (англ. EDR – Endpoint Detection and Response) [8], а також новітні системи мережевої безпеки, які забезпечують автоматизований моніторинг, виявлення, аналіз та реагування на складні кіберзагрози (англ. NDR – Network Detection and Response) [8].

Ідентифікація є засобом, яким користувач надає системі заявлену ідентичність. Автентифікація – це метод визначення дійсності цієї заявки. Зокрема, ідентифікація та аутентифікація досягаються за рахунок: інформації користувача (паролі та протоколи аутентифікації); власності користувача (модулі пам'яті, PIN-коди карток); особи користувач (біометричні дані).

Контроль та управління правом доступу убезпечують незаконне проникнення на об'єкти захисту та несанкціоноване використання ресурсів. У зальному розрізняють кілька рівнів контролю доступу: контроль доступу під час входу у систему; контроль доступу до окремих об'єктів (файлів, папок, баз даних тощо); контроль доступу до окремих пристроїв системи.

Моделі керування доступом поділяються на: дискреційне (виборче) управління; обов'язковий (мандатний) метод керування; рольова модель. Дискреційний контроль доступу (DAC – Discretionary Access Control) [7]. Передбачає право адміністратора об'єкта визначати та контролювати всіх, хто має доступ до системи, ґрунтуючись на ідентифікаційній інформації про суб'єктів (ключі доступу), допущених до контрольованої системи. Мандатний контроль доступу (MAC – Mandatory Access Control) [7]. Є найбільш обмежувальною формою доступу, оскільки надає контроль та керування системою лише адміністратору. Тут користувачам не дозволяється підвищувати рівень доступу до ресурсів, встановлений адміністратором. Модель рольового керування доступом (RBAC – Role-Based Access Control) [7]. Передбачає розподіл функцій персоналу з урахуванням типу діяльності. Тут достатньо встановити ступінь допуску для ролі, яку виконує типовий користувач ресурсу.

Засоби захисту від шкідливого ПЗ аналізує дані, що можуть зазнавати загроз: знищення інформації та (або) її носія; несанкціоноване отримання конфіденційної інформації; модифікація інформації; створення помилкових повідомлень; блокування доступу до інформації або ресурсів системи; несанкціоноване використання інформаційних ресурсів системи тощо.

Наведемо кілька ефективних сканерів: Advanced IP Scanner, Wireshark, Solarwinds, Tripwire, Nessus, Vulnerability Manger Plus, Splunk тощо.

Засоби контролю цілісності засновані на алгоритмах підрахунку контрольних сум і здійснюється за двома напрямками: контроль цілісності наборів даних; контроль цілісності програмного середовища. Активно використовується електронно-цифровий підпис (ЕЦП). За допомогою математично обґрунтованих алгоритмів обчислюється функція від конкретного підписаного повідомлення і обчислюється автором повідомлення на основі індивідуального ключа. ЕЦП залежить від кожного символу, тому неможливо змінити його або підмінити, не змінивши значення ЕЦП. За допомогою технології ЕЦП здійснюється підтвердження: дійсності електронного документа; контроль його цілісності; його авторство.

2 Сучасні підходи до організації захисту інформації в рамках SOC.

Ефективний та постійний ЗІ в ІКМ може здійснюватися спеціалізованими центрами і фахівцями з кібербезпеки, зокрема, це центри SOC. SOC – Security Operations Center, Ситуаційний центр інформаційної безпеки, є структурним підрозділом, що безперервно моніторить системи.

Центр SOC – це не тільки технічні системи, які в режимі реального часу передають аналітикам SOC повідомлення від засобів захисту, а й експерти, які можуть відрізнити помилкове спрацювання захисного засобу від справжнього, і здатні зрозуміти, чи є кілька явно пов'язаних між собою повідомлень від засобів захисту ланками одного ланцюга, що означає комп'ютерне зараження. У прийнятті рішень їм допомагають SIEM – системи управління інформацією про безпеку та події інформаційної безпеки. Основне завдання SOC-центру – реагування на інциденти ІБ. У SOC-центрі вхідні дані безперервно обробляються SOC-командою таких фахівців. Тож, основними завданнями SOC-центрів є: моніторинг та аналіз вторгнення в режимі реального часу; запобігання

кіберзагрозам на випередження: безперервно сканувати комп'ютерні мережі та аналізувати інциденти безпеки; швидка реакція на підтверджені інциденти та виключення помилкових спрацьовувань.

3 Ідея системного моніторингу в рамках тріади SIEM-EDR-NDR.

З метою удосконалення роботи SOC-Центру провідна дослідницька компанія Gartner розробила нову концепцію таких центрів – SOC Visibility Triad. Це мережево-орієнтована структура, яка розроблена для створення комплексного та завершеного підходу до стратегії кібербезпеки. Об'єднавши три основні принципи – виявлення та реагування на кінцеві точки, виявлення та реагування мережі і керування інформацією про безпеку та подіями – компанії можуть досягти рівня захисту кібербезпеки, який раніше був недосяжним.

Коли три компоненти тріади SOC об'єднуються, команди SOC отримують повну інформацію про мережу своєї компанії, що значно покращує ефективність виявлення загроз і реагування на них. Тріада видимості SOC складається з трьох окремих компонентів: SIEM, EDR і NDR. Кожен із цих компонентів гармонійно працює разом, доповнює один одного, щоб створити цілісну та завершену систему кібербезпеки, яка захищає кожен аспект ІКМ.

У цій тріаді система SIEM відстежує, реєструє, ідентифікує та аналізує сповіщення кібербезпеки, які впливають на мережу організації. Це досягається в режимі реального часу шляхом збору та зіставлення даних з усіх джерел даних мережі. Зрештою, це забезпечує повне уявлення про ІКМ, дозволяючи SOC-Центру оперативно досліджувати та усувати кіберзагрози.

Якщо SIEM використовується самостійно без можливостей EDR і NDR, то він може пропустити експлойти та уразливості, які не відображаються в журналах SIEM, що може призвести до виникнення сліпої зони.

EDR зосереджується на зборі й аналізі даних із кінцевих точок ІКМ. Система EDR поєднує збір даних із моніторингом загроз у реальному часі та можливостями автоматизованого усунення загроз кінцевим вузлам. Сама EDR не забезпечує глибину захисту, не запобігає бічному переміщенню трафіку та ізольовано захищає лише невелику частину мережевої інфраструктури.

NDR об'єднує тріаду SOC, надаючи повну інформацію про стан мережі та захищаючи її від внутрішніх і зовнішніх атак. NDR також має унікальну перевагу захисту від зловмисників, які переміщуються збоку в мережі, значно зменшуючи здатність зловмисника завдати шкоди після успішного зламу. NDR дозволяє командам SOC і безпеки швидко аналізувати дані мережі із внутрішньої та зовнішньої точки зору. Це обмежує кількість часу для зловмисника в мережі, і зменшує ймовірність зламу.

Висновки.

В цій роботі було розглянуто ідею побудови системи захисту інформації, методи та засоби безпекового моніторингу мережі, сучасні підходи захисту інформації в рамках SOC, поточні загрози інформаційної безпеки, ідею системного моніторингу мережі в рамках моделі тріади SIEM-EDR-NDR та взаємодія трьох компонентів тріади SOC між собою та їх взаємодоповнення.

Були запропоновані приклади ефективного використання систем SOC і SIEM-EDR-NDR для забезпечення безпеки мережі.

Це дає можливість вдосконалити системний моніторинг мережевої безпеки та запобігти майбутнім загрозам інформаційної безпеки.

Література:

1. Таченко І. А., Коробейнікова Т. І. & Захарченко С. М. (2021) Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки. Scientific Collection «InterConf», (84), 417-432. https://doi.org/10.51582/interconf.7-8.11.2021.

2. Tachenko I. & Korobeinikova T. (2021) The basic aspects of assessment and risk remediation technological chain. "Information protection and information systems security": coll.of scientific papers with Proceedings of the VIII-th International Scientific and Technical Conference (Vol. 1, p. 17-19). November 11, 2021, Lviv: NULP.

3. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України (2021). Вилучено із: https://zakon.rada.gov.ua/laws/show/v0365500-11.

4. Про засади інформаційної безпеки України (Закон України) (2014). Вилучено із: https://ips.ligazakon.net/document/JG3TH00A.

5. Захарченко С.М., Трояновська Т. І., Бойко О.В. (2017). Побудова захищених мереж на базі обладнання компанії Cisco. Вінниця: ВНТУ – 133 с.

6. Гребенюк А.М., Рибальченко Л.В. (2020). Основи управління інформаційною безпекою: навч. посібник. Дніпро: ДДУВС – 144 с.

7. Класифікація загроз інформаційній безпеці (2020). Вилучено із: https://er.dduvs.in.ua/bitstream/.

8. What is the SOC visibility triad? (2023). – Вилучено із: https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/.

Abstract. *The paper considers the idea of building an information protection system, methods and means of network security monitoring, modern approaches to information protection within SOC and the idea of system network monitoring within the framework of the SIEM-EDR-NDR triad model. Analyzed and classified current threats to information security (IS).The mentioned principles of building an IS system. Examples of effective use of SOC and SIEM-EDR-NDR systems to ensure network security are provided. The interaction of the three components of the SOC triad with each other and their complementarity is considered*

Key words: *Information security, IS threats, system monitoring, network security SIEM, EDR, NDR, SOC.*

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 05.05.2023 р.