УДК 004.056

***А. М. Медяна***
***А. В. Грицак***

# МОДЕЛЬ РИЗИК-ОРІЄНТОВАНОГО РАНЖУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ПРАВИЛА-ОРІЄНТОВАНОЇ КОРЕЛЯЦІЇ ПОДІЙ

Вінницький національний технічний університет

***Анотація***

*У дослідженні розглянуто підхід до виявлення та ранжування інцидентів інформаційної безпеки на основі нормалізації журналів подій, правила-орієнтованої кореляції подій і ризик-орієнтованого оцінювання. Актуальність дослідження обумовлена зростанням кількості подій безпеки в інформаційних системах і необхідністю автоматизованого визначення їх критичності для своєчасного реагування. Запропонований підхід передбачає приймання подій від агентів, нормалізацію журналів Windows Security та Sysmon, побудову корельованих інцидентів за набором правил і подальший розрахунок ризикового балу на основі показників ймовірності, впливу та експозиції активу. Результати роботи формують основу ризикового балу для пріоритезації інцидентів та підтримки прийняття рішень аналітиком безпеки.*

**Ключові слова:** інциденти інформаційної безпеки, кореляція подій, ризик-скоринг, ранжування інцидентів, Windows Security, кібербезпека.

**Abstract**

*This study examines a model for detecting and ranking information security incidents based on event log normalization, rule-oriented correlation, and risk-oriented assessment. The relevance of the study is due to the growing number of security incidents in information systems and the need for automated determination of their criticality for timely response. The proposed approach involves receiving events from agents, normalizing Windows Security and Sysmon logs, building correlated incidents based on a set of rules, and then calculating a risk score based on probability, impact, and asset exposure indicators. The results form the basis of the risk score for prioritizing incidents and supporting decision-making by security analysts*.

**Keywords:** information security incidents, event correlation, risk scoring, incident ranking, Windows Security, cybersecurity.

## Вступ

У сучасних інформаційних системах щоденно генерується велика кількість подій безпеки. До таких подій можуть належати спроби автентифікації, запуск процесів, права запуску програми, доступ до системних ресурсів, зміни конфігурації або мережеві взаємодії. Аналіз окремих подій не завжди дозволяє визначити факт порушення безпеки, однак сукупність взаємопов’язаних подій може свідчити про реалізацію потенційної атаки [1].

Тому важливим завданням сучасних систем моніторингу безпеки є не лише реєстрація подій, але й їх кореляція та подальше визначення критичності інцидентів. Особливу роль у цьому процесі відіграє оцінювання кіберризику, яке дозволяє визначити рівень загрози для інформаційної системи та встановити пріоритет реагування.

## Результати дослідження

Метою роботи є розробка моделі ризик-орієнтованого ранжування інцидентів інформаційної безпеки на основі кореляції подій.

Події безпеки можуть виникати у різних компонентах інформаційної системи. Окрема подія не завжди є ознакою загрози, проте певна послідовність або сукупність подій може свідчити про підозрілу активність.

З метою виявлення таких взаємозв’язків використовується механізм кореляції подій. Кореляція передбачає аналіз послідовності подій та їх характеристик, таких як час виникнення, джерело події, тип активності та задіяні об’єкти системи. Події, що мають спільні атрибути або виникають у певній логічній послідовності, можуть об’єднуватися в один інцидент інформаційної безпеки [2].

Візьмемо приклад, послідовність подій, що включає кілька невдалих спроб автентифікації, подальше підвищення привілеїв та запуск підозрілого процесу, може свідчити про спробу компрометації облікового запису або системи. Аналіз таких взаємозв'язків дозволяє виявляти складні сценарії атак, які не можуть бути визначені на основі окремих подій.

Кореляція подій забезпечує перетворення великого потоку окремих подій безпеки у більш узагальнені інциденти, що характеризують потенційні порушення інформаційної безпеки. Це дозволяє зменшити кількість незначних сповіщень та зосередити увагу на подіях, які мають найбільшу ймовірність бути пов'язаними з реальними загрозами [3].

Після виявлення події небезпеки на основі кореляції подій необхідно визначити рівень критичності події для інформаційної системи. У системах моніторингу безпеки велика кількість інцидентів може виникати одночасно, тому важливо мати механізм, який дозволяє оцінити рівень небезпеки кожного з них та визначити пріоритет реагування.

Оцінювання інциденту безпеки доцільно здійснювати з урахуванням кількох основних факторів. Першим таким фактором є ймовірність виникнення або реалізації загрози. Вона характеризує, наскільки імовірно, що зафіксована послідовність подій дійсно пов'язана з атакою або порушенням політики безпеки.

Другим фактором є потенційний вплив інциденту на інформаційну систему. Цей показник відображає можливі наслідки реалізації інциденту, наприклад втрату конфіденційності даних, порушення цілісності інформації або зниження доступності системи.

Третім важливим фактором є експозиція активу, тобто рівень його доступності та значущості для інформаційної системи. Наприклад, подія, що виникає на критичному сервері або системному компоненті, має значно більший рівень ризику, ніж аналогічна подія на звичайній робочій станції.

Рівень ризику події може розглядатися як результат поєднання трьох основних характеристик: ймовірності виникнення загрози, потенційного впливу та експозиції активу [4].

З урахуванням цього узагальнена модель оцінювання ризику може бути представлена у вигляді:

$$Risk = Likelihood \times Impact \times Exposure \quad (1)$$

де *Likelihood* - ймовірність виникнення або реалізації інциденту; *Impact* - потенційний вплив події на інформаційну систему; *Exposure* - рівень експозиції або значущості активу.

Кожен із зазначених параметрів може задаватися у вигляді дискретної шкали, наприклад від 1 до 5, що дозволяє отримати узагальнений ризиковий бал інциденту. Отримане значення ризику використовується для подальшого ранжування інцидентів та визначення їх пріоритету в системі моніторингу інформаційної безпеки.

Для більш точного врахування результатів кореляції подій оцінювання ризику доцільно виконувати для кожного інциденту окремо.

Модель ризику може бути представлена у вигляді:

$$Risk = Li \times Ii \times Ei \quad (2)$$

де $L_i$ - ймовірність виникнення і-го інциденту, що визначається на основі характеристик зафіксованих подій та результатів їх кореляції; $I_i$ - потенційний вплив і-го інциденту на інформаційну систему, який характеризує можливі наслідки реалізації загрози, зокрема порушення конфіденційності, цілісності або доступності інформації; $E_i$ - експозиція активу, що відображає рівень значущості або критичності об'єкта інформаційної системи, на якому зафіксовано інцидент.

Використання індексу і дозволяє оцінювати ризик для кожного інциденту окремо та формувати їх упорядкований список відповідно до рівня небезпеки. У практичних системах моніторингу інформаційної безпеки значення параметрів $L_i$, $I_i$ та $E_i$ можуть визначатися за допомогою дискретної шкали або експертної оцінки.

Отриманий ризиковий бал $Risk_i$ характеризує інтегральний рівень небезпеки інциденту. Чим більшим є значення цього показника, тим більш критичним вважається інцидент та тим вищим має бути його пріоритет у процесі реагування. Отже, розрахунок ризикового балу дозволяє виконувати автоматизоване ранжування інцидентів та сприяє ефективнішому управлінню подіями інформаційної безпеки.

У системах моніторингу інформаційної безпеки одночасно може фіксуватися значна кількість інцидентів, що виникають у різних компонентах інформаційної інфраструктури. Оскільки ресурси для реагування на такі події обмежені, важливим завданням є визначення їх пріоритетності. Для цього використовується механізм ранжування інцидентів, який дозволяє впорядкувати їх відповідно до рівня ризику.

Основою для ранжування є обчислений ризиковий бал $Risk_i$, що характеризує рівень небезпеки кожного інциденту. Однак абсолютні значення ризику можуть змінюватися залежно від кількості інцидентів та параметрів оцінювання, тому для забезпечення більш коректного порівняння доцільно застосовувати процедуру нормалізації.

Нормалізоване значення ризику має бути визначене як:

$$Risk_{norm} = \frac{Risk_i}{Risk_{max}} \quad (3)$$

де $Risk_i$ - значення ризику для і-го інциденту; $Risk_{max}$ - максимальне значення ризику серед усіх інцидентів, зафіксованих у системі.

Нормалізація дозволяє привести значення ризику до уніфікованого діапазону та забезпечити коректне порівняння інцидентів між собою. Отримані значення можуть використовуватися для формування впорядкованого списку інцидентів за рівнем їх критичності.

Для спрощення процесу реагування інциденти можуть бути додатково класифіковані за рівнями ризику.

Залежно від отриманого значення ризикового показника можуть виділятися такі категорії:

- низький рівень ризику, що характеризує події з незначним впливом на інформаційну систему;
- середній рівень ризику, що відповідає потенційно небезпечним подіям, які потребують аналізу;
- високий рівень ризику, що характеризує критичні інциденти, які вимагають негайного реагування.

Таке групування дозволяє суттєво спростити процес аналізу подій безпеки та зосередити увагу фахівців з кібербезпеки на найбільш критичних інцидентах.

У результаті ранжування формується пріоритетна черга інцидентів, яка використовується для організації подальших дій щодо їх дослідження та усунення.

## Висновки

Розглянуто підхід до виявлення та ранжування інцидентів інформаційної безпеки на основі кореляції подій та ризик-орієнтованого оцінювання. Проведено аналіз взаємопов'язаних подій безпеки, який дозволяє перетворити великий потік окремих журналів подій на узагальнені інциденти, які більш точно відображають потенційні загрози інформаційній системі.

Запропоновано модель оцінювання ризику інцидентів, що базується на врахуванні трьох ключових факторів: ймовірності виникнення загрози, потенційного впливу на інформаційну систему та експозиції активу.

На основі розрахованого ризикового балу реалізовано механізм ранжування інцидентів, що дозволяє визначити пріоритет їх аналізу та реагування. Застосування запропонованого підходу сприяє підвищенню ефективності систем моніторингу інформаційної безпеки та забезпечує більш оперативне виявлення і обробку критичних інцидентів.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Security auditing [Електронний ресурс] – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/security-auditing-overview
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems.
3. Хаос чи контроль? Як кореляція подій допомагає бізнесу тримати безпеку під контролем [Електронний ресурс] – Режим доступу до ресурсу: https://my-itspecialist.com/korelyatsiya-podiy-v-siem
4. Ризики інформаційної безпеки. Чому це важливо і як з ними працювати відповідно до ISO/IEC 27005? [Електронний ресурс] – Режим доступу до ресурсу: https://my-itspecialist.com/iso-iec-27005-risk-management

***Медяна Аліна Миколаївна*** — студентка групи 2КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, medanaa904@gmail.com .

**Грицак Анатолій Васильович** – кандидат технічних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com.

***Mediana Alina M.*** – student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, medanaa904@gmail.com.

***Hrytsak Anatoly V***. – *Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com.*