КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.5158
УДК 004.065

Єрмошин Валерій Віталійович
начальник департаменту інформаційної безпеки
ПрАТ НЕК «Укренерго», Київ, Україна
ORCID ID: 0000-0003-3747-0471
yermoshyn.vv@ua.energy

КОНТРОЛЬ ПАРАМЕТРІВ КІБЕРБЕЗПЕКИ ЯК МЕХАНІЗМ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ТА ПРОГНОЗУВАННЯ СИТУАЦІЇ

Анотація. Діюче на сьогодні в Україні правове поле визначає набір заходів з кіберзахисту та потребу в плануванні їх подальшого розвитку, що дозволяє сформувати та описати загальний підхід до забезпечення кібербезпеки у вигляді системного процесу. Актуальною при цьому є потреба в формуванні конкретних параметрів кібербезпеки які дозволяють кількісно оцінювати кіберзахисту не лише як управлінський процес, а і як реальну систему захисту з своїми особливостями функціонування та недоліками. На підставі наявного у автора досвіду запропоновано підхід до формування параметрів кібербезпеки як механізму оцінювання ефективності захисту за кількісною оцінкою по відношенню до кожного з розглянутих параметрів та подальше використання їх як інструменту прогнозування ситуації з кібербезпеки. Запропоновані автором параметри пов'язані з зовнішнім інформаційно-комунікаційним периметром організації, системами автентифікації користувачів, забезпечення їх віддаленої роботи, використання засобів електронної пошти, а також реалізованим в організації захистом кінцевих точок та захистом веб-технологій. Запропоновані автором параметри кібербезпеки мають технічну направленість і місять опис який дозволяє визначати їх кількість та умовно нормальну поведінку. За обліком статистичних даних та з врахуванням умовно нормальної поведінки по визначеним автором параметрам запропоновано проводити оцінювання і кіберризиків. Автором запропоновано оптимальні періоди спостереження по відношенню до визначених параметрів кіберзахисту та зазначено про залежність їх інформативності та об'єктивності спостереження з накопиченням даних за параметром часу. Також автором запропоновані до розгляду індикативні значення яке дозволяють проводити оцінку ефективності що в свою чергу дозволяє проводити певне прогнозування ситуацій з кіберзахисту в цілому.

Ключові слова: кібербезпека; оцінювання ефективності захисту.

ВСТУП

З початком збройної агресії рф значно зросла кількість кібератак як дій які передують або відбуваються паралельно з кінетичними атаками. Саме тому відповідальні за напрямок органи приділяють кіберзахисту значну увагу і правове поле галузі модернізується та активно змінюється. Так з початку війни за напрямком пов'язаним з питаннями кібербезпеки вийшло більше 10 документів (постанови Кабінету міністрів України та накази Держспецзв'язку). Сформоване на сьогодні правове поле визначає набір заходів з кіберзахисту та бажані результати кіберзахисту що дозволяє сформувати та описати загальний підхід до забезпечення кібербезпеки у вигляді системного процесу. Тобто використання зазначеного правового поля дозволяє оцінювати поточний та цільовий рівні кіберзахисту але не визначає конкретних параметрів кібербезпеки які дозволяють кількісно оцінювати вже функціонуючу систему кіберзахисту та спрогнозувати її стійкість та реальну спроможність до моменту порушення функціонування об'єкту інформаційної інфраструктури за рахунок кібернападу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Як показує практика спостережень параметрами кібербезпеки за яким доцільно вести спостереження є:

- Кількості спрацювань по блокуванню мережевих атак на периметрі;
- Кількості отримання шкідливих файлів на поштову скриньку співробітників;
- Кількість брутфорс атак (підбор паролю) на облікові записи;
- Кількість брутфорс атак (підбор паролю) на VPN мережу — якщо використовується;
- Кількість спам листів які мають в своєму тілі посилання на шкідливі ресурси;
- Спроб сканувань периметру підприємства (розвідки);
- Кількість унікальних спрацювань на віруси, трояни і т. і.;
- Кількість спрацювань антивірусного захисту;
- Кількість СПАМ листів заблокованих на почтовому шлюзі безпеки;
- Заблоковано WAF (web application firewall).

За статистичними даними по указаним вище параметрам можна проводити оцінювання кіберризиків. Тобто поточне значення параметру може свідчити про спробу реалізації тієї чи іншої кіберзагрози. Раптове збільшення параметру може свідчити про підготовку або проведення кібератаки, а раптове зниження про перенесення атаки на інший напрямок або зміну підходу до її реалізації.

Опис наведених параметрів кібербезпеки наведено в табл. 1.

Таблиця 1

Опис параметрів кібербезпеки

Параметр кібербезпеки	Опис параметру
Кількості спрацювань по блокуванню мережевих атак на периметрі	Сумарна кількість спрацювань на NGFW правил IDS/IPS які пов'язані з типом сервісу (подія яка не відноситься до сервісу не генерується — наприклад на правило яке відслідковує події з веб додатком не може бути спрацювань пов'язаних з атакою на поштові сервіси), на периметрі та з середини на зовні
Кількості отримання шкідливих файлів на поштову скриньку співробітників	Сумарна кількість спрацювань на NGFW та Email Gateway на сигнатури файлів які класифіковані як шкідливі
Кількість брутфорс атак (підбор паролю) на облікові записи користувачів (в тому числі і за рахунок помилок користувачів)	Сумарна кількість невдалих входів в систему авторизації через ввід неправильного паролю до облікового запису.
Кількість брутфорс атак (підбор паролю) на VPN мережу (в тому числі і за рахунок помилок користувачів)	Сумарна кількість невдалих під'єднань до VPN мереж через введення неправильного імені користувача або паролю до нього під час підключення до VPN мережі.
Кількість спам листів які мають в своєму тілі посилання на шкідливі ресурси	Сумарна кількість листів які були заблоковані на поштовому шлюзі правилами які перевіряють на вміст шкідливого вкладення в листі та/або вміст з посиланням на шкідливі ресурси.
Спроб сканувань периметру підприємства (розвідки)	Сумарна кількість спрацювань на NGFW правил IDS/IPS на периметрі по відфільтрованим правилам які відповідають за сканування, та відслідковування аномальної кількості підключень до периметру

Кількість унікальних спрацювань на віруси, трояни і т.д.	Сумарна кількість спрацювань на NGFW сигнатурного аналізу файлів (весь трафік окрім поштового) — мережевий контроль.
Кількість спрацювань антивірусного захисту	Сумарна кількість спрацювань системи антивірусного захисту на файли які містили в собі віруси або трояни та були видалені з системи — контроль кінцевих точок.
Кількість СПАМ листів заблокованих на почтовому шлюзі безпеки	Сумарна кількість СПАМ листів заблокованих на почтовому шлюзі безпеки
Заблоковано WAF	Сумарна кількість запитів заблокованих Web Application Firewall за сигнатурами виробника та власно створеними правилам

Практика спостережень за параметрами кібербезпеки дозволяє по відношенню до деякий з них визначити умовно нормальну поведінку.

За рядом параметрів, наприклад заблоковано WAF, в наслідок відсутності пов'язаного з цим параметром критерія або фактору, визначити умовно нормальну поведінку неможливо.

Значення параметру кібербезпеки яке можна розглядати як умовно нормальну поведінку представлено в табл. 2.

Таблиця 2

Параметр кібербезпеки	**Умовно нормальна поведінка**
Кількості отримання шкідливих файлів на поштову скриньку співробітників	до 0,5% загальної кількості поштових скриньок
Кількість брутфорс атак (підбор паролю) на облікові записи користувачів (в тому числі і за рахунок помилок користувачів)	до 2% від загальної кількості користувачів
Кількість брутфорс атак (підбор паролю) на VPN мережу (в тому числі і за рахунок помилок користувачів)	до 10% від кількості користувачів які мають доступ до сервісу
Кількість спам листів які мають в своєму тілі посилання на шкідливі ресурси	0,6% від загальної кількості поштових скриньок
Кількість унікальних спрацювань на віруси, трояни і т. д.	0,17% від загальної кількості користувачів
Кількість спрацювань антивірусного захисту	0,08% від загальної кількості користувачів
Кількість СПАМ листів заблокованих на почтовому шлюзі безпеки	14% від загальної кількості поштових скриньок

Як показує практика спостережень за параметрами кібербезпеки оцінювання та можливість прогнозування ситуації залежить від періоду спостережень. Чим він більший, тим точніші оцінювання та прогнозування можна зробити. Не інформативними є статистичні данні в форматі вчора/сьогодні. Всю зібрану статистику за параметрами доцільно представляти в вигляді точкової діаграми.

Під час спостережень доцільно оцінювати максимальне значення певного параметру кібербезпеки за весь період спостережень та його середнє значення. Це дозволить оцінити поточний стан та напрямок можливого нападу в разі зростання певного параметру (візуально за діаграмою або по абсолютному значенню).

Так в разі отримання значень параметру яке представлене на малюнку нижче можна зробити висновок що в поточний момент за ним відбувається підвищений інтерес який перевищує середнє значення, але цей інтерес не перевищує зафіксовані до цього випадки.

ISSN 2663 - 4023

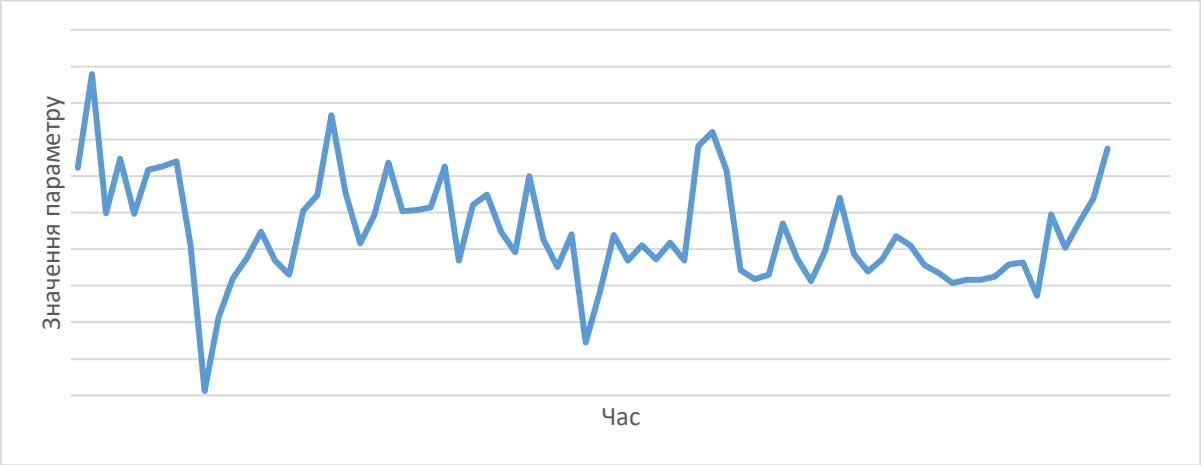

Рис. 1 Статистика змін значень параметру протягом певного часу

Також доцільно розглядати максимальне та середнє значення параметру кібербезпеки в межах певного досліджуваного періоду. При цьому в разі кібератаки, особливо значної за своїм обсягом, спостерігається суттєвий вплив на максимальне значення в рамках всього періоду спостереження що призводить до погіршення візуальної можливості поточної оцінки за діаграмою. Ілюстрацію зазначеного наведено нижче.

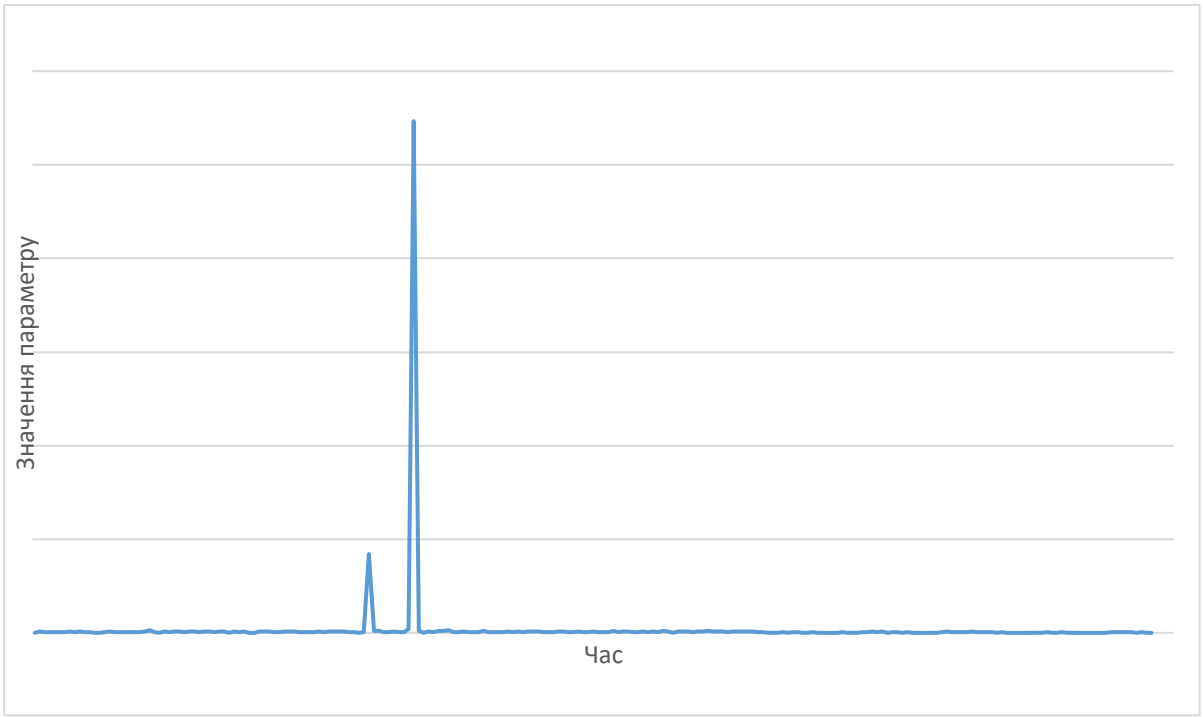

Рис. 2 Статистика змін значень параметру в разі кібератаки

Тому в ряді випадків значення параметрів під час кібератак при візуалізації потребують певної обробки — приведення до вигляду який дозволяє проводити спостереження шляхом виключення з спостереження пікових значень або зміни періоду спостереження. Так, в цьому випадку, для візуального спостереження доцільно

використовувати період після атаки, або інше часове обмеження — наприклад попередній до атаки поточний.

Як показує практика, рішення щодо ефективності захисту може бути прийнято на основі поточних значень параметрів кібербезпеки та відслідковування їх значень з впливом часу. Тобто до уваги треба брати не лише поточне значення параметру, а і попереднє його значення. Таким чином можна сформувати індикативне значення параметру.

Таблиця 3

Параметр кібербезпеки	Індикативне значення параметру
Кількості спрацювань по блокуванню мережевих атак на периметрі	Значення змінюється з впливом часу, не дорівнює нулю
Кількості отримання шкідливих файлів на поштову скриньку співробітників	Значення змінюється з впливом часу, не дорівнює нулю
Кількість брутфорс атак (підбор паролю) на облікові записи користувачів (в тому числі і за рахунок помилок користувачів)	Значення змінюється з впливом часу але можливі інтервали часу (до декількох днів) коли значення дорівнює нулю
Кількість брутфорс атак (підбор паролю) на VPN мережу (в тому числі і за рахунок помилок користувачів)	Значення змінюється з впливом часу але можливі інтервали часу (до декількох днів) коли значення дорівнює нулю
Кількість спам листів які мають в своєму тілі посилання на шкідливі ресурси	Значення змінюється з впливом часу але можливі інтервали часу (до тижня) коли значення дорівнює нулю
Спроб сканувань периметру підприємства (розвідки)	Значення змінюється з впливом часу, не дорівнює нулю
Кількість унікальних спрацювань на віруси, трояни і т. д.	Значення змінюється з впливом часу але можливі інтервали часу (до декількох днів) коли значення дорівнює нулю
Кількість спрацювань антивірусного захисту	Значення змінюється з впливом часу але можливі інтервали часу (до декількох днів) коли значення дорівнює нулю
Кількість СПАМ листів заблокованих на почтовому шлюзі безпеки	Значення змінюється з впливом часу, не дорівнює нулю
Заблоковано WAF	Значення змінюється з впливом часу, не дорівнює нулю

Відхилення від індикативного значення параметру може свідчити що система захисту не працює або по відношенню до неї спостерігаються проблеми які потребують дослідження та усунення. Практика спостережень показує що повтор одного й того ж значення параметру кібербезпеки майже виключений, особливо для випадків коли реєструється суттєві (сотня та більше) значення за параметром.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином запропонований контроль параметрів кібербезпеки може дозволити фахівцям які займаються цим напрямком оцінювати ефективність захисту та визначити її непрацездатність або тимчасовий збій якщо параметри з впливом часу не змінюються або дорівнюють нулю. На основі статистики яка збирається фахівці можуть будувати прогнозування безпекової ситуації, оцінювати свій поточний стан, шукати певні маркери та взаємозв’язки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0.* https://www.nist.gov/cyberframework
2. National Institute of Standards and Technology. (2012). *NIST SP 800-61: Computer Security Incident Handling Guide.*
3. National Institute of Standards and Technology. (2008). *NIST SP 800-55 Rev. 1: Performance Measurement Guide for Information Security.*
4. The Australian Signals Directorate. (2017). *Strategies to mitigate cyber security incidents.*
5. Адміністрація Держспецзв'язку. (2021). *Про затвердження методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури* (Наказ № 601, зі змінами). https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
6. Адміністрація Держспецзв'язку. (2023). *Про затвердження методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі* (Наказ № 570). https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori
7. Державна служба спеціального зв'язку та захисту інформації України. (2024). *Статистичний звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році.*
8. ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT).
9. Кабінет Міністрів України. (2023). *Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі* (Постанова № 299). https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text
10. Міністерство енергетики України. (2022). *Про вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури* (Наказ № 417). https://zakon.rada.gov.ua/laws/show/z0249-23#Text

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Valerii Yermoshyn
Head of the Information Security Department
NEC Ukrenergo, Kyiv, Ukraine
ORCID ID: 0000-0003-3747-0471
yermoshyn.vv@ua.energy

CONTROL OF CYBER SECURITY PARAMETERS AS A MECHANISM FOR EVALUATING THE EFFECTIVENESS OF PROTECTION AND FORECASTING THE SITUATION

Abstract. The current legal framework in Ukraine defines a set of cybersecurity measures and the need to plan their further development, which allows us to formulate and describe a general approach to cybersecurity in the form of a systematic process. At the same time, there is a need to form specific cybersecurity parameters that allow quantifying cybersecurity not only as a management process, but also as a real protection system with its own peculiarities and disadvantages. Based on the author's experience, an approach to the formation of cybersecurity parameters as a mechanism for assessing the effectiveness of protection by quantifying each of the parameters under consideration and their further use as a tool for forecasting the cybersecurity situation is proposed. The parameters proposed by the author are related to the external information and communication perimeter of the organization, user authentication systems, ensuring their remote work, the usage of e-mail, as well as endpoint protection and web technology protection implemented in the organization. The cybersecurity parameters proposed by the author are technically oriented and contain a description that allows determining their number and conditionally normal behavior. Based on statistical data and taking into account conditionally normal behavior according to the parameters defined by the author, it is proposed to assess cyber risks. The author proposes optimal periods of observation in relation to certain parameters of cyber defense and notes the dependence of their informativeness and objectivity of observation on the accumulation of data by the time parameter. The author also proposes to consider indicative values that allow assessing the effectiveness, which allows to perform certain forecasting of cyber defense situations in general.

Keywords: cyber security; assessment of protection effectiveness.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0.* https://www.nist.gov/cyberframework
2. National Institute of Standards and Technology. (2012). *NIST SP 800-61: Computer Security Incident Handling Guide.*
3. National Institute of Standards and Technology. (2008). *NIST SP 800-55 Rev. 1: Performance Measurement Guide for Information Security*.
4. The Australian Signals Directorate. (2017). *Strategies to mitigate cyber security incidents*.
5. Administratsiia Derzhspetszviazku. (2021). *Pro zatverdzhennia metodychnykh rekomendatsii shchodo pidvyshchennia rivnia kiberzakhystu krytychnoi informatsiinoi infrastruktury* (Nakaz № 601, zi zminamy). https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
6. Administratsiia Derzhspetszviazku. (2023). *Pro zatverdzhennia metodychnykh rekomendatsii shchodo reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori* (Nakaz № 570). https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori
7. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2024). *Statystychnyi zvit za rezultatamy roboty systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky v 2023 rotsi.*
8. DSTU ISO/IEC 27002:2023 Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Zasoby kontroliuvannia informatsiinoi bezpeky (ISO/IEC 27002:2022, IDT).

9. Kabinet Ministriv Ukrainy. (2023). *Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori* (Postanova № 299). https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text
10. Ministerstvo enerhetyky Ukrainy. (2022). *Pro vymohy z kiberbezpeky palyvno-enerhetychnoho sektoru krytychnoi infrastruktury* (Nakaz № 417). https://zakon.rada.gov.ua/laws/show/z0249-23#Text