DOI:**10.33099/2311-7249/2024-51-3-34-40**

УДК: 004.056

Мазулевський Олег Євгенович ***(кандидат технічних наук)***
Жолобович Назар Вікторович

Міністерство оборони України

ОЦІНКА ПОТОЧНОГО СТАНУ КІБЕРСТІЙКОСТІ З УРАХУВАННЯМ СИТУАЦІЇ У КІБЕРПРОСТОРІ

Метою статті є розроблення способу оцінки поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі, використовуючи статистичні дані кількості виявлених кіберінцидентів. Для проведення оцінки поточного стану кіберстійкості в статті використовуються методи лінійної алгебри та методи статистичного аналізу, за допомогою яких запропоновано виділити моменти критичних змін для подальшого аналізу та виявлення і прогнозування настання кризових ситуацій у кіберпросторі. У статті розроблено спосіб оцінки поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі, який визначається в числовому значенні та висвітлює ознаки можливості настання кризової ситуації у сфері кібербезпеки для оборонного відомства й може бути використаний для покращення ситуаційної обізнаності його керівництва. Стаття є першою в послідовності викладення підходу оцінки кіберстійкості оборонного відомства в межах окресленої законодавчими документами зони відповідальності. Розробка та впровадження оцінки кіберстійкості оборонного відомства та прогнозування виникнення кризових ситуацій і сфері кібербезпеки дає змогу швидко виявляти, а прогнозування запобігти, виникненню негативних наслідків впливу кризових ситуацій та постійної підтримки ситуаційної обізнаності керівного складу оборонного відомства.

Ключові слова*: кіберстійкість, кібербезпека, кризова ситуація в галузі кібербезпеки.*

Вступ

Постановка проблеми. В сучасному світі, де інформаційні технології стрімко розвиваються і проникають у всі сфери життя (включно з військовою сферою) кібербезпека стає критично важливим елементом діяльності будь-якої установи. Захист інформаційних ресурсів від загроз у кіберпросторі є одним із основних аспектів успішної функціональності, оскільки порушення кібербезпеки може призвести до суттєвих репутаційних та фінансових втрат і навіть зупинки діяльності, або втрати найціннішого – людського життя (у випадку воєнних організацій). Кількість і складність кібератак зростають із кожним роком, що вимагає від фахівців із кібербезпеки не лише вчасного реагування на загрози, а й прогнозування виникнення потенційних кризових ситуацій для зменшення їх наслідків. В цій статті розглянемо частину, розробленого вперше, процесу виявлення кризових ситуацій на основі аналізу статистичних даних кількості зафіксованих кіберінцидентів та визначення оцінки в числовому значенні поточного стану кіберстійкості оборонного відомства для підтримки ситуаційної обізнаності його керівництва.

Аналіз останніх досліджень та публікацій. Згідно з постановою №705 від 11 липня 2023 року, уряд передбачив створення ситуаційного центру Кабінету Міністрів і ситуаційних центрів центральних органів виконавчої влади, обласних, Київської міської державних адміністрацій, інших державних органів, органів сектору безпеки і оборони (зокрема і Міністерства оборони України). На даний час в українському інформаційному просторі відсутні публікації та висвітлення підходів із виявлення потенційно-можливих кризових ситуацій у кіберпросторі. Винятком є Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/ кібератаки затвердженого на засіданні Національного координаційного центру кібербезпеки 22 вересня 2022 року і який зазначає лише порядок взаємодії з усунення кризової ситуації, що вже сталася. Тому, автором розроблено, і в цій статті пропонується розглянути частину «Методу проведення прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних» вперше представленого в [1].

Запропонований підхід до оцінки та прогнозування, що розробляється, фокусується на трьох ключових етапах: оцінці забезпеченості кібербезпеки документами, їх змістом та технічними засобами кіберзахисту (результати планується опублікувати найближчим часом); аналізі поточної ситуації на основі статистичних даних про кількість і типи кіберінцидентів (саме цьому присвячена ця стаття); а також прогнозуванні можливих кризових ситуацій, що можуть виникнути в майбутньому (результати планується опублікувати найближчим часом).

Такий підхід дасть змогу посилити спроможність оборонного відомства до захисту від кіберзагроз, впровадивши заходи запобігання виникненню та ефективні стратегії реагування на кризові ситуації.

Отже, **метою статті є** розроблення способу оцінки поточного стану кіберстійкості з урахуванням поточної ситуації у кіберпросторі, із використанням статистичних даних кількості виявлених кіберінцидентів.

Виклад основного матеріалу дослідження

Однією з основних ознак розвитку сучасного суспільства в мирний час та воєнної організації під час війни є подальше та постійне зростання залежності від якості й надійності інформаційно-комунікаційних систем (далі – ІКС), що застосовуються в діяльності людини. Відповідне посилення стратегічної спрямованості інформаційних ресурсів зумовлює необхідність підвищення вимог до рівня їх інформаційної безпеки. Проблема ускладнюється тим, що особливості найбільшої глобальної мережі «Інтернет», з якою інтегровано більшість ІКС, і використання загальнодоступного програмного забезпечення призводять до нагромадження випадкових і непередбачених негативних впливів на вказані системи. Зазначимо, що ІКС, які мають підключення до інтернету, розглядається в ракурсі необхідності захисту ресурсів таких систем від кібератак у процесі реалізації базових технологічних процесів отримання, зберігання, транспортування, оброблення та відображення інформації [2].

Обумовимо, що деякі терміни будуть використовуватися відповідно до Наказу Міністерства оборони України (далі – МО України) від 18 квітня 2024 року №248 [3]:

інформаційна безпека та кібербезпека в інформаційно-комунікаційних системах (далі – інформаційна безпека в ІКС, ІБ в ІКС) − сукупність організаційних, правових, інженерно-технічних заходів, спрямованих на захист інформації та кіберзахист ІКС;

інцидент безпеки інформації – подія або низка несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці ІКС, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку інформації, що обробляється в таких ІКС.

Введемо термін: *кіберстійкість ІКС* – стан ІКС, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз.

Інші терміни вживаються в значеннях, які наведені в Законах України [4; 5], Державному Стандарті України [6].

Згідно статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII [4] МО України є одним із основних суб'єктів національної системи кібербезпеки і відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Тому слід мати можливість оцінити стан кіберстійкості ІКС оборонного відомства та державних органів (установ) для прийняття зважених управлінських рішень у мирний час та під час функціонування в особливий період.

Далі розглянемо отримання даних для проведення оцінки поточного стану з урахуванням ситуації у кіберпросторі. Для формування вірної картини стану кіберстійкості доречним буде проведення регулярного моніторингу результатів роботи засобів кіберзахисту в системі забезпечення інформаційної безпеки в ІКС. Моніторинг реалізується шляхом збору статистичних даних виявлених кіберінцидентів засобами кіберзахисту.

Для оцінки в МО України слід збирати дані за базові елементи національної системи кібербезпеки, а саме від державного сектору України (далі у формулах – DS), Збройних Сил України (далі у формулах – AFU) та МО України (далі у формулах – DOD), за можливості інших елементів.

Для проведення оцінки поточного стану, з урахуванням ситуації у кіберпросторі, стану кіберстійкості МО України використовуються наступні показники, що відображають рівень напруженості ситуації в кіберпросторі:

$Risk\_index_{\sum}$ – узагальнений індекс напруженості ситуації у кіберпросторі;

$Risk\_index_{DoD}$ – індекс напруженості ситуації у кіберпросторі для МО України;

$Risk\_index_{DS}$ – індекс напруженості ситуації у кіберпросторі для державного сектору України;

$Risk\_index_{AFU}$ – індекс напруженості ситуації у кіберпросторі для Збройних Сил України (далі – ЗС України);

$Incidents_{\sum}$ – узагальнений індекс змін кількості виявлених кіберінцидентів;

$divIncidents_{DoD}$ – індекс змін кількості виявлених кіберінцидентів у МО України;

$divIncidents_{DS}$ – індекс змін кількості виявлених кіберінцидентів у державному секторі України;

$divIncidents_{AFU}$ – індекс змін кількості виявлених кіберінцидентів у ЗС України;

CybeResilience – композитний показник кіберстійкості (розраховується у також з урахуванням оцінки забезпеченості ІБ в ІКС відомства, буде здійснено у подальших дослідженнях автора).

Розрахунок $Risk\_index_{\sum}$ та $Incidents_{\sum}$ проводиться на основі статистичних даних кількості виявлених інцидентів кібербезпеки в уповноважених підрозділах із ІБ в ІТС та відхилення кількості в поточний момент із врахування даних за певний період.

Індекс кількості виявлених інцидентів кібербезпеки розраховується для оцінки рівня змін виявлення активності дій проти ІКС зазначеної належності. Дані, що надходять, мають відповідати Переліку категорій кіберінцидентів розробленого на основі Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України [7]. Приклад таксономії переліку категорій та типів кіберінцидентів наведено на сайті CERT-UA [8]. Перелік призначений для впровадження таксономії як інструменту для обміну інформацією щодо кіберінцидентів. Дані зі звітів по 21 типу кіберінцидентів заносяться в таблицю. Для проведення статистичного аналізу необхідно мати вибірку даних не менше ніж 90 діб.

Надалі розмір вибірки може змінюватися з наданням обґрунтування. На основі вибірки розраховуються такі показники:

перцертранк поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі);

середнє геометричне перцертранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі);

кількість верхніх крайніх значень перцертранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів);

кількість нижніх крайніх значень перцертранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів).

Тепер розглянемо *розрахунок індексу напруженості ситуації у кіберпросторі*. Узагальнений індекс напруженості ситуації у кіберпросторі (3) розраховується на основі індексів напруженості ситуації у кіберпросторі для окремих елементів (2) – для ІКС МО України, ЗС України, Держсектору, які, в свою чергу, засновані на розрахунку перцертранків (1) кожного типу кіберінцидентів. Спочатку необхідно провести розрахунок індексу напруженості ситуації у кіберпросторі для елементів (2), які обчислюються однаково, проте на основі різних статистичних даних, отриманих зі звітів за напрямами та розрахованих за перцертранками (1).

Здійснимо *розрахунок перцертранку поточних значень кількості за типами кіберінцидентів.*

Перцертранк – процентильний ранг значення у масиві даних (зворотна функція процентиля). *Процентиль* – значення ознаки, яке відокремлює кожну соту частину впорядкованого ряду, вказує на відносне місце визначеного значення в загальному розподілі впорядкованої множини.

Функція розрахунку перцертраку (в MS Excell – PERCENTRANK.INC) обчислює процентильний ранг значення (x) у масиві даних *{A}*. Формула для обчислення виглядає так:

$$P(x)=(r-1)/(N-1), \quad (1)$$

де $P(x)$ – процентильний ранг значення x;

r – ранг значення x у впорядкованому масиві *{A}*;

N – загальна кількість елементів у масиві *{A}*.

Порядок розрахунку:

1. Впорядкування масиву: Спочатку впорядковується масив даних *{A}* у порядку зростання.

2. Визначення рангу: Знаходиться ранг r значення x у впорядкованому масиві. Ранг – це позиція значення x у масиві *{A}*, починаючи з першого найменшого значення.

3. Обчислення процентильного рангу: використовуючи формулу (1), де N – загальна кількість елементів у масиві, обчислюється процентильний ранг значення x.

Обчислення проводиться для кожного типу кіберінцидентів (КІ) за визначений період і буде визначати множину $\{_{date}Perc\}$ набору перцертранків кожного відліку (за датою).

Розглянемо розрахунок значень перцертранку для кожного типу КІ в MS Excel. Функція PERCENTRANK.INC – повертає ранг (відсоткову норму) значення як дольове значення величини елементів (0..1, включно з 0 і 1) сукупності даних. За допомогою цієї функції можна обчислити відносне положення значення в сукупності даних. Наприклад, значення кількості кіберінцидентів за добу міститься в діапазоні `OJ2:OJ22`, і для значення, яке знаходиться в клітинці `OJ2`, а попередні значення кількості кіберінцидентів за типами знаходяться у рядку 2, значення перцертранку розраховується формулою:

```
=IF(MAX(OFFSET(OI2,0,-6,1,7))>0,
IFERROR(PERCENTRANK.INC(OFFSET
(OI2,0,-90,1,91),OJ2)*100,ROUND
(IF(MAX(OFFSET(OI2,0,-6,1,7))>0,
    (OJ2/(MAX(OFFSET(OI2,0,-
  90,1,91))/100)),-1),2)),-1)
```

де перевіряється умова `MAX(OFFSET(OI2,0,-6,1,7))>0` визначення наявності даних, які відрізняються від нуля, за попередні 7 днів, якщо значення були менше або дорівнює 0 – то в чарунку заноситься значення (-1), а якщо є значення більші за нуль розраховується перецертранк із масиву даних (`OFFSET(OI2,0,-90,1,91)`) за попередні 90 днів, у відсотках (*100, за замовчуванням у частках із точністю 3 знаки після десяткової коми); за умови помилки в розрахунку перцертранку розраховується значення відсотку поточної кількості кіберінцидентів (в чарунці `OJ2`) від максимального значення кількості кіберінцидентів за попередні 90 днів, із точністю у 2 знаки після десяткової коми.

Помилки в розрахунку перцертранку виникають коли значення для якого розраховується більше за

максимальне значення за попередні 90 днів. За відсутності набору даних за 90 днів вбачається за доцільне, розраховувати відсоток від максимального значення за наявний період даних. Період у 90 значень показників кількості кіберінцидентів за типами (множина даних) було обрано з логіки того, що за 3 місяці проходять короткотермінові (спонтанні, неочікувані) кібератаки.

Наступним етапом розрахунків є знаходження середнього геометричного перцертранка поточних показників за всіма типами кіберінцидентів, що і буде значенням *індексу напруженості ситуації у кіберпросторі для елементу спостереження* (МО України, ЗС України, ДС). Для цього скористаємося класичною формулою розрахунку середнього геометричного: *Середнє геометричне* (середнє пропорційне) декількох додатних чисел дорівнює кореню, ступінь якого дорівнює кількості чисел, із добутку даних чисел. Значення узагальнюється на довільну кількість чисел більших нуля. Середнє геометричне E чисел a_1, $a_2 \ldots a_E$ дорівнює кореню E-го ступеня із добутку даних чисел. Середнє геометричне E чисел a_1, $a_2 \ldots a_E$ дорівнює

$$Risk\_index = \sqrt[E]{\prod_{e=1}^{E} a_e}\,, \qquad (2)$$

де E – кількість додатніх значень перцертранка за типами кіберінцдинтів; a_e – додатні значення перцертранка за типами кіберінцдинтів.

Розглянемо варіант розрахунку середнього геометричного перцертранків кількості кіберінцидентів за типами в програмі MS Excel для даних зібраних у стопчику (`OJ`). В прикладі, під час реалізації, розрахунку в MS Excel множина даних *{$_{date}$Perc}* буде визначена окремо в кожному стовпці в рядках від 28 до 48. Тобто, для прикладу дати 23 жовтня 2024 року, визначений стовпець `OJ2`, то *{$_{24.10.2024}$Perc}={*`OJ28:OJ48`*}*.

Приклад буде показано для розрахунку для 21 типу кіберінцидентів зазначених за таксономією CERT-UA. Напередодні було розраховано значення перцертранків для кількості кожного типу кіберінцидентів результати яких, наприклад, містяться в чарунках діапазону (`OJ28:OJ48`). Проведемо перенесення значень у новий діапазон чарунок (`OJ297:OJ317`) із відсівом значень рівним і меншим нуля, наприклад, використовуючи функцію перенесення в чарунку `OJ297`:

```
=IF(OJ28>0,OJ28,1).
```

Використовується функція привласнення із умовою: якщо значення більше нуля, то воно переноситься без змін, а якщо менше нуля то прирівнюється одиниці. Цей варіант використовується тому, що одиниця під час розрахунку добутку значень перцертранків не вносить змін (добуток числа та одиниці дорівнює цьому ж числу). В реальному розрахунку перцертранка значення ніколи не буде дорівнювати рівно одиниці тому, що використовується величина вибірки не кратна ста.

Для розрахунку середнього геометричного перцертранків кількості кіберінцидентів за типами в програмі MS Excel використовується функція:

```
=IF(COUNTIF(OJ297:OJ317,"<>1")>0,ROU
ND(POWER((OJ297*OJ298*OJ299*OJ300*OJ
301*OJ302*OJ303*OJ304*OJ305*OJ306*OJ
307*OJ308*OJ309*OJ310*OJ311*OJ312*OJ
313*OJ314*OJ315*OJ316*OJ317),1/COUNT
IF(OJ297:OJ317,"<>1")),2),0)
```

У функції проводиться перевірка наявності значень розрахованих перцертранків за типами кіберінцидентів (дані зі звіту наявні). У разі, коли кількість усіх значень буде не рівна 1 і більше 0, то проводиться розрахунок, якщо 0, то значення функції буде дорівнювати 0. Через відсутність у MS Excel функції вилучення кореню за визначеним ступенем, проведемо розрахунок середнього геометричного за допомогою функції піднесення в ступінь. Де значенням ступеня, згідно алгебраїчних властивостей ступеневих функцій, використано значення одиниці поділеної на кількість елементів не рівних 1. Значення середнього геометричного округлено до двох знаків після десяткової коми.

Індекс напруженості ситуації у кіберпросторі розраховується для кожного напряму спостереження, а саме для МО України ($Risk\_index_{DoD}$), ЗС України ($Risk\_index_{AFU}$), Державного сектору України ($Risk\_index_{DS}$).

Узагальнений індекс напруженості ситуації у кіберпросторі ($Risk\_index_{\sum}$) визначається як максимальне значення серед індексів напруженості кожного напряму спостереження:

$$Risk\_index_{\sum} = MAX(Risk\_index_{DoD}\,,\ Risk\_index_{AFU},\ Risk\_index_{DS})\,. \qquad (3)$$

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) КІ в одному із напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

Індекс змін кількості виявлених кіберінцидентів. Подальшим етапом обробки статистичних даних є *знаходження верхніх крайніх та нижніх крайніх значень перцертранку кількості кіберінцидентів за типами.* Порогові значення визначаються емпіричним шляхом (в подальшому можуть змінюватися для детального налаштування моделі прогнозування). На першому етапі прийнято рішення про фіксацію таких випадків:

для фіксації низького рівня кількості КІ виражених перцертранком за типами при зменшенні менше ніж порогове значення;

для фіксації високого рівня кількості КІ виражених перцертранком за типами при перебільшенні більше ніж порогове значення.

Використання декількох рівнів порогових значень може застосовуватися для визначення

ступеню впливу та побудови більш точних моделей виявлення та прогнозування різних типів кібератак (кібервпливів) та настання, на їх основі, кризових ситуацій. Для кожного окремого напряму розраховується значення кількості значень подолання порогових значень, в яких значення перераховані від більш суворих до більш м'яких. А також враховувати той чинник, щоб значення матриць порогових значень не перетиналися, а саме найм'якіший мінімальний поріг не був більший за найм'якіший максимальний поріг.

Для кожного напряму визначимо кількість спрацювань по кожному пороговому значенню у матриці кількості подолань порогів $[{}_{date}B]$ згідно виразу:

$$ {}_{date}B = \begin{bmatrix} |\forall \{{}_{date}Perc_{k=1..|{}_{date}Perc|}\} \le MinPor_{p=1..P}|; \\ |\forall \{{}_{date}Perc_{k=1..|{}_{date}Perc|}\} \ge MaxPor_{p=1..P}|; \end{bmatrix}, \quad (4) $$

де ${}_{date}Perc_{k=1..|{}_{date}Perc|}$ – усі елементи множини значень перцертранків кількості КІ за визначену дату; *MinPor* – матриця значень мінімальних порогових значень; *MaxPor* – матриця значень максимальних порогових значень.

Отже, в матриці кількості подолання порогів $[{}_{date}B]$ визначаються кількість зменшень відносно мінімальних порогів в першому рядку та кількість перебільшень максимальних порогів в другому рядку.

Подолання порогового значенням перцертранку кількості кіберінцидентів за типами дає змогу побачити аномальну активність/безактивність зловмисників. Перевищення покаже ймовірний початок нової атаки (етапу атаки), а заниження про завершення атаки (етапу атаки) і підготовку до нової атаки (етапу атаки). Як відомо, кібератака складається із декількох етапів, про що можливо дізнатися із різних підходів вивчення кібератак. Так, наприклад, Cyber Kill Chain від Lockheed Martin поділяє кібератаку на 7 етапів [9], а MITRE ATT&CK на 14 «тактик» із описом конкретних «технік» [10] для реалізації різних типів кібератак.

Не всі етапи кібератаки призводять до підвищення значень кількості КІ, не всі атаки використовують послідовність класичних моделей та можуть бути проведені в повному обсязі для досягнення поставлених цілей (у разі дії не фінансово вмотивованих зловмисників, а політично чи примусово…). Або кібератаки різного типу можуть бути етапами однієї більшої скоординованої кібератаки. Наприклад, останнім часом, ворогом (через використання APT-угрупувань, Advanced Persistent Threat) під час проведення атак на інфраструктуру державних структур для відволікання уваги фахівців кібербезпеки та/або переведення телекомунікаційного обладнання в критичні режими функціонування проводяться атаки на розподілену відмову в обслуговуванні з залученням контрольованих «хактивістів» (політично або ідеологічно вмотивованих кіберзлочинців здебільшого з низьким рівнем підготовки) країни агресора під різними вигаданими (надуманими) приводами. Отже, «хактивісти» вважають це проведенням окремого «акту впливу» (помсти, покарання), а насправді є інструментом на черговому етапі для більш скоординованої кібератаки.

Індекс змін кількості виявлених кіберінцидентів розраховується окремо за кожним напрямом МО України, ЗС України, державного сектору України тощо. Для його знаходження використаємо раніше визначену матрицю кількості подолання порогів $[{}_{date}B]$ відповідно для кожного напряму:

$$ divIncidents = ({}_{date}B_{1,1} + {}_{date}B_{2,1}) * q, \quad (5) $$

де ${}_{date}B_{1,1}$ – елемент матриці $[{}_{date}B]$, який показує кількість подолання найстрогішого мінімального порогу (1 строка 1 стовпець);

${}_{date}B_{2,1}$ – елемент матриці $[{}_{date}B]$, який показує кількість подолання найстрогішого максимального порогу (2 строка 1 стовпець);

q – рівнозважений коефіцієнт впливу подолання порогового значення.

Значення рівнозваженого коефіцієнту впливу спрацювання порогового значення визначається як: $q = 100\% / 21 \approx 4.76$, де 21 – кількість типів КІ в таксономії, який в подальшому можливо змінювати використовуючи наукові підходи, наприклад, методом парних порівнянь.

Узагальнений Індекс змін кількості виявлених кіберінцидентів ($Incidents_{\sum}$) визначається як максимальне значення серед індексів змін кількості виявлених кіберінцидентів кожного напряму спостереження:

$$ Incidents_{\sum} = MAX(divIncidentsDoD, divIncidentsAFU, divIncidentsDS). \quad (6) $$

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) КІ в одному з напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

Композитний показник кіберстійкості. Оцінивши документальне забезпечення кіберстійкості у оборонному відомстві, що є одним з напрямів подальшого дослідження автора, та поточний стан ситуації у кіберпросторі доцільним є звести усі оцінки в один Композитний показник кіберстійкості:

$$ CybeResilience = (CompDocImperf + Risk\_index_{\sum} + (Incidents_{\sum} - Risk\_index_{\sum} * Incidents_{\sum}/100))/2. \quad (7) $$

Для наочності, можливе відображення індикатора «Композитний показник кіберстійкості» – типу «спідометр» із наступними кольоровими розмежуваннями: «зелений» – менше 10; «жовтий» – більше 10 до 50; «червоний» – більше 50 (рис. 1).

Знаходження значення у вказаних проміжках значень може бути показником можливого виникнення кризової ситуації та сигналом для задіяння механізмів реагування з метою запобігання та/або пом'якшення наслідків виникнення кризової ситуації у галузі кібербезпеки.

Рисунок 1 – Приклад відображення інформаційної панелі «сфери кібербезпеки» в системі ситуаційної обізнаності Ситуаційного центру МО України (варіант)

Висновки й перспективи подальших досліджень

Використання наведеного в статті способу дасть змогу підвищити ступінь поінформованості про якісний характер впливу на Міністерство оборони України у кіберпросторі, та бути індикатором можливого виникнення кризової ситуації у сфері кібербезпеки. Спосіб «оцінки поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі», є елементом «*Методу проведення прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних*».

Розробка та впровадження Методу є подальшим напрямом досліджень. Його впровадження дасть змогу виявляти прогалини в організації/ забезпеченні кібербезпеки та виявляти ознаки настання кризових ситуацій в сфері кібербезпеки, підвищити рівень готовності Міністерства оборони України до можливих кризових ситуацій, зменшити втрати від кіберінцидентів і забезпечити стабільну роботу інформаційно-комунікаційних систем. Отже, розробка та використання такого Методу є важливим кроком до зміцнення кіберстійкості в умовах зростаючого тиску з боку кіберзлочинців, державно-вмотивованих APT-груп і нових загроз у кіберпросторі.

Список бібліографічних посилань

1. Мазулевський О., Денесюк Р. Прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних. *Інформаційно-аналітичне забезпечення органів військового управління: Проблемні питання та шляхи їх вирішення* : тези доповідей Науково-практичної конференції. НУОУ, 28.11.2024 р. С.74-75. **2. Терейковський І., Корченко А.** Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації : навчальний посібник. КПІ ім. Ігоря Сікорського, 2022. С. 175. **3. Основні засади забезпечення інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах** : затверджено Наказом Міністерства оборони України від 18.04.2024 № 248. **4. Про основні засади забезпечення кібербезпеки України** : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.11.2024). **5. Про захист інформації в інформаційно-комунікаційних системах**: Закон України (зі змінами) від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/ show/80/94-%D0%B2%D1%80#Text (дата звернення: 22.11.2024). **6. Державний Стандарт України ISO/IEC 27000:2023** Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Наказ ДП «УкрНДНЦ» від 17.08.2023 № 210 **7. Протокол** № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21). **8. Перелік категорій кіберінцидентів**: URL: https://cert.gov.ua/ recommendation/16904 (дата звернення: 22.11.2024). **9. The Cyber Kill Chain framework**. Lockheed Martin. 2024. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/ cyber-kill-chain.html (accessed 22 November 2024). **10. Globally-accessible knowledge base of adversary tactics and techniques MITRE ATT&CK**. 2024. URL: https://attack.mitre.org/ (accessed 22 November 2024).

ASSESSMENT OF THE CURRENT STATE OF CYBER RESILIENCE, TAKING INTO ACCOUNT THE SITUATION IN CYBERSPACE

Mazulevskyi Oleh (PhD)
Zholobovich Nazar

Ministry of defence of Ukraine

Formulation of the problem in general. *The article is published with the aim of highlighting a firstly developed method of assessing the current situation of cyber resilience of the defense department, taking into account the statistical data on the number of recorded cyber incidents.*

Research methods. *To assess the current state of cyber resilience, the article uses linear algebra and statistical analysis methods, with the help of which it is proposed to identify the moments of critical changes for further analysis and to identify and predict the onset of crisis situations in cyberspace. In the course of the article, the author uses the regulatory documents governing the cybersecurity industry.*

Analysis of recent researches and publications. *The analyzed sources do not contain any approaches to detecting crisis situations at the strategic level, taking into account the processing of statistical data.*

Presenting the main material. *The article develops a method for assessing the current state of cyber resilience, taking into account the situation in cyberspace, which is defined in numerical terms and highlights the signs of the possibility of a cybersecurity crisis for the defence department and can be used to improve the situational awareness of its leadership.*

Elements of scientific novelty. *Therefore, the article proposes for the first time to develop a method for detecting abnormal activity of malicious influence on the resources of the defense department. Abnormal are cases of extreme increases or decreases in the values of cyber incidents, which is evidence of a targeted impact on resources and may indicate the next stage of a cyberattack.*

Theoretical and practical significance of the article. *Processing data on the occurrence of extreme changes in the time perspective can be used to identify potential cybersecurity crises.*

Conclusion and the perspectives of future researches. *A further direction of research is to expand the parameters for assessing cyber resilience and predicting the occurrence of crisis situations. The use of situational awareness and decision support systems will significantly reduce the response time and the consequences of crisis situations.*

Keywords*: cyber resilience, cybersecurity, cybersecurity crisis.*

References

1. Mazulevs′kyy, O., Denesyuk, R., (2024). Forecasting and detection of crisis situations in cyberspace based on statistical data processing. Informatsiyno-analitychne zabezpechennya orhaniv viys′kovoho upravlinnya: Problemni pytannya ta shlyakhy yikh vyrishennya : tezy dopovidey Naukovo-praktychnoyi konferentsiyi. NUOU, 28 lystopada 2024 r., 74-75. **2. Tereykovsky, I., Korchenko, A.,** (2022). Intellectualized methods of information security: neural networks in information security: textbook. Igor Sikorsky Kyiv Polytechnic Institute, **3. Basic principles of information security and cybersecurity in information and communication systems,** (2024). Order of the Ministry of Defence of Ukraine №248, 18 April. **4. On the Basic Principles of Ensuring Cybersecurity of Ukraine** [online], (2017). Law of Ukraine № 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Accessed: 22 November 2024]. **5. On the Protection of Information in Information and Communication Systems**. Law of Ukraine (as amended) of 16.12.2020 No. 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2 %D1%80#Text [Accessed: 22 November 2024]. **6. State Standard of Ukraine ISO/IEC 27000:2023** Information technology. Methods of protection. Information security management systems. Overview and glossary of terms. Order of the State Enterprise "UkrSIRC" dated 17.08.2023 No. 210. **7. Protocol** No. 18 of the meeting of the National Coordination Center for Cybersecurity under the National Security and Defense Council of Ukraine of 25.10.2021 (No. 16/320/21 of 28.10.2021). **8. List of categories of cyber incidents**: Available at: https://cert.gov.ua/recommendation/16904 [Accessed: 22 November 2024]. **9. The Cyber Kill Chain® framework** [online], (2024). *Lockheed Martin.* Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed: 22 November 2024]. **10. Globally-accessible knowledge base of adversary tactics and techniques** [online], (2024). *MITRE ATT&CK®* Available at: https://attack.mitre.org [Accessed: 22 November 2024].