DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-03
УДК [004.02/.032/.421] + 621.391 +004.031.42+007.2
**Козубцова Леся Михайлівна**, к.т.н.
https://orcid.org/0000-0002-7866-8575
**Рудоміно-Дусятська Ірина Анатоліївна,** к.фіз.-мат.н., доцент
https://orcid.org/0000-0003-3006-3320
**Сновида Вікторія Євгеніївна**
https://orcid.org/0000-0002-5539-2588
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут

# ОБЧИСЛЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І КІБЕРБЕЗПЕКИ

**Козубцова Л.М., Рудоміно-Дусятська І.А., Сновида В.Є. Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки.** У статті подано часткове рішення науково-технічної проблеми з розроблення методики оцінювання ефективності функціонування системи захисту інформації і кібербезпеки. Часткове рішення полягає у виборі підходів, показників, критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки. Наукова новизна одержаного результату полягає в тому, що вперше комплексно і систематично проаналізовано підходи до вибору критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки, які забезпечують цілісну картину. Практичне значення роботи полягає в подальшій можливості, на основі обраних показників, критеріїв розробити методику оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.
**Ключові слова:** кіберзахищеність, кібербезпека, підходи, показники, критерії, оцінювання, ефективність, функціонування, система захисту інформації і кібербезпеки.

**Козубцова Л.М. Рудомино-Дусятская И.А., Сновида В.Е. Вычисление характеристик эффективности функционирования системы защиты информации и кибербезопасности.** В статье представлено частичное решение научно-технической проблемы по разработке методики оценки эффективности функционирования системы защиты информации и кибербезопасности. Частичное решение состоит в выборе подходов, характеристик, критериев оценки эффективности функционирования системы защиты информации и кибербезопасности. Научная новизна полученного результата состоит в том, что впервые комплексно и систематически проанализированы подходы к выбору критериев оценки эффективности функционирования системы защиты информации и кибербезопасности, обеспечивающей целостную картину. Практическое значение работы состоит в дальнейшем возможности на основе выбранных показателей, критериев разработать методику оценки эффективности функционирования системы защиты информации и кибербезопасности.
**Ключевые слова:** кибербезопасность, кибербезопасность, подходы, показатели, критерии, оценка, эффективность, функционирование, система защиты информации и кибербезопасности.

**Kozubtsova L.M. Rudomino-Dusyatska I.A., Snovida V.E. Calculation of performance indicators of the information protection and cybersecurity system.** The article presents a partial solution to the scientific and technical problem of developing a methodology for evaluating the effectiveness of the information security and cybersecurity system. A partial solution consists in choosing approaches, characteristics, criteria for evaluating the effectiveness of the information security and cybersecurity system. The scientific novelty of the obtained result consists in the fact that for the first time approaches to the selection of criteria for evaluating the effectiveness of the information security and cybersecurity system that provides a holistic picture have been comprehensively and systematically analyzed. The practical significance of the work consists in the further possibility, based on the selected indicators, criteria, to develop a methodology for evaluating the effectiveness of the information security and cybersecurity system.
**Key words:** cybersecurity, cybersecurity, approaches, indicators, criteria, evaluation, efficiency, functioning, information protection system and cybersecurity.

**Постановка завдання і зв'язок її з важливими науковими завданнями.** Згідно Закону України "Про основні засади забезпечення кібербезпеки України" [1]; Стратегії кібербезпеки України [2]; Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [3] кібербезпеку визначено як пріоритетний напрямком. Безумовно в Україні для реалізації вимог представлених в документах [1 – 4], як і усьому цивілізованому світі ведуться постійні роботи з удосконалення системи захисту інформації і кібербезпеки щодо забезпечення безперервності її функціонування.

Система захисту інформації і кібербезпеки (СЗІКБ) – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки. Слід визнавати що СЗІКБ є відносно новою системою. Тому доцільно вивчити питання ефективного її функціонування, а саме розробити математичний апарат її оцінки. Показники оцінки ефективності СЗІКБ носять ймовірнісний характер

Під «ефективністю системи захисту інформації і кібербезпеки» ($E_{СЗІКБ}$) будемо розуміти ступінь відповідності досягнутих результатів поставленим цілям щодо захисту інформації.

Оцінка ефективності може здійснюватися в процесі створення, приймання та експлуатації СЗІКБ. Ключовим поняттям є критерій оцінки – ознака, підстава прийняття рішення щодо оцінки ефективності на відповідність висунутим вимогам.

Для перевірки та оцінки функціональної спроможності СЗІКБ, за аналогією, як до будь-якої системи, необхідна методика такої оцінки, яка наразі відсутня. Виходячи з розглянутого та вище сказаного виникає наукове завдання з розроблення методики оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.

**Аналіз останніх досліджень і публікацій.** З аналізу останніх досліджень і публікацій за обраним напрямком досліджень можна зробити висновок, що поставлене завдання дослідження є новим.

У роботі [4] для оцінки ефективності системи захисту інформаційної системи, автор застосовував наступну розрахункову формулу (1):

$$E = \frac{E_ф}{B}, \quad (1)$$

де Е– під ефективністю розуміють ступінь досягнення мети цієї системою;

Еф – ефект, який досягається при впровадженні СЗІКБ;

В – витрати, сукупні витрати на придбання, установку і конфігурування, супровід і підтримку, а також витрати пов'язані з простоєм устаткування вчасно технічне обслуговування або усунення несправностей.

Слід зазначити, що через специфіку функціонування СЗІКБ визначити прямий ефект від їх впровадження важко.

В роботах [5; 6] автори дотримуються єдиної думки та використовують математичну модель оцінювання ефективності функціонування системи за критерієм запобігання втрат. Витрати на забезпечення інформаційної безпеки слід вважати ефективними, якщо вони забезпечують виконання вимог нормативних документів і стандартів, прийнятих державою, а також концепції інформаційної безпеки організації.

Кінцевим результатом впровадження та проведення заходів щодо забезпечення інформаційної та кібербезпеки є значення попередження втрат (ПВ), яке розраховують за формулою (2):

$$ПВ = В1 – В2, \quad (2)$$

де В1 – втрати від реалізації загроз до впровадження заходів, що підвищують рівень інформаційної або кібербезпеки.

В2 – втрати від реалізації загроз після впровадження заходів, що підвищують рівень інформаційної або кібербезпеки СЗІКБ.

По суті, ЗВ є різницею втрат до і після реалізації заходів, спрямованих на підвищення рівня інформаційної або кібербезпеки, і в цілому відображає ту частину прибутку, яка могла бути втрачена.

Застосування даного підходу ускладнено внаслідок відсутності підходів до розрахунку В1 та В2. В зв'язку з цим актуалізується сформульована нова наукова задача.

Запропонована в роботі [7] методика вирішує лише питання оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій.

**Мета статті**. Оскільки необхідність оцінювання ефективності функціонування системи захисту інформації і кібербезпеки виникла вперше, то необхідно обрати підходи, показники та критеріїв такого оцінювання.

**Виклад основного матеріалу.**

Оцінка ефективності – це процедура, спрямована на визначення якісних і кількісних показників ефективності, виявлення критичних елементів системи, а також визначення інтегрального показника ефективності системи в цілому.

Підходи до оцінювання ефективності функціонування СЗІКБ.

Під «імовірнісним підходом до оцінки ефективності» розуміється використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності можна отримати шляхом моделювання або визначити за характеристиками реальної системи. Однак можливості імовірнісних методів ефективності стосовно СЗІКБ обмежені в силу ряду причин: високий ступінь невизначеності вихідних даних, складність формалізації процесів функціонування, відсутність загальновизнаних методик розрахунку показників ефективності і вибору критеріїв оптимальності.

Показник ефективності – це величина, що характеризує ступінь досягнення системою будь-якого з поставлених перед нею завдань.

Вимоги до показника ефективності: мати певний фізичний зміст; бути придатним для кількісного аналізу; мати просту і зручну форму; відображати одну із значущих сторін функціонування системи; забезпечувати необхідну чутливість. Поодинокі (часткові) показники ефективності, відображають якусь із значущих сторін функціонування системи (ймовірність виявлення порушника або ймовірність його нейтралізації силами охорони і т.п.).

Відповідно до цього означення запропонуємо наступні часткові показники ефективності, як числові величини, що характеризуватимуть ступінь досягнення системою захисту інформації і кібербезпеки поставлених перед нею завдань:

кіберзахищеність ($P_{КЗ}$). Кіберзахищеність – здатність системи зв'язку виконувати завдання за призначенням в умовах програмно-математичних впливів противника, тобто ймовірність того, що ця система буде захищеною від кібернетичного втручання;

коефіцієнт укомплектованості засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту ($K_{УЗ}$);

коефіцієнт технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту ($K_{ТГЗ}$);

коефіцієнт укомплектованості справними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту ($K_{УСЗ}$);

коефіцієнт укомплектованості штатних посад системними адміністраторами ($K_{СА}$);

коефіцієнт укомплектованості штатних посад обслуговуючим персоналом ($K_{ОП}$);

кіберзахищеність за результатами penetration testing ($P_{КЗ}^{РТ}(S)$).

Під «засобом криптографічного захисту інформації» будемо розуміти програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації.

Під «засобом технічного захисту інформації» будемо розуміти програмний, апаратно-програмний та апаратний засіб, призначений для технічного захисту інформації та має відповідний експертний висновок.

Під «засобом кібернетичного захисту інформації» будемо розуміти програмний, апаратно-програмний та апаратний засіб, призначений для кібернетичного захисту інформації.

Комплексні (узагальнені) показники ефективності являють собою комбінацію часткових показників. Оскільки конкретній вплив часткових показників у загальну ефективність ще не відомо, то пропонується узагальнений показник ефективності функціонування системи захисту інформації і кібербезпеки обчислювати за формулою (3):

$$E_{СЗІКБ} = \frac{P_{КЗ} + K_{УЗ} + K_{УСЗ} + K_{СА} + K_{ОП} + P_{КЗ}^{РТ}(S)}{N_{Р}}, \quad (3)$$

де $N_{Р}$ – кількість задіяних в розрахунку часткових показників ефективності функціонування системи захисту інформації і кібербезпеки.

Якщо за окремим показником не здійснювалось обчислення, то в розрахункову формулу (3) не підставляються відповідні значення і у висновках дається коротке і лаконічне обґрунтування чому саме не застосовувався окремий показник.

Критеріїв ефективності СЗІКБ може бути багато, проте вибір конкретних залежить від специфіки проведеної оцінки. Критерії оцінки ефективності функціонування системи захисту інформації і кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України за узагальненим показником подані в (табл. 1).

Таблиця 1. Критерії оцінки ефективності функціонування системи захисту інформації і кібербезпеки за узагальненим показником

| Критерій $E_{СЗІКБ}$ | Рівень | Лінгвістичний опис | |
|---|---|---|---|
| $0 \le E_{СЗІКБ} \le 0{,}25$ | незадовільний (НЗ) | незадовільний рівень ефективності. Система не працездатна, підлягає повному відновленню. | Можливий витік інформації |
| $0{,}25 < E_{СЗІКБ} \le 0{,}5$ | низький (Н) | низький рівень ефективності. Система підлягає відновленню | Створення умов для витоку інформації |
| $0{,}5 < E_{СЗІКБ} \le 0{,}75$ | середній (С) | середній рівень ефективності. Система правильно функціонує | Забезпечення гарантованого захисту інформації та кібербезпеки |
| $0{,}75 < E_{СЗІКБ} \le 0{,}9$ | високий (В) | в цілому високий рівень ефективності. Система працездатна | |
| $0{,}9 < E_{СЗІКБ} \le 1$ | найвищий (НВ) | найвищий рівень ефективності. Система справна | |

Орієнтовний (критичний) вклад окремих (часткових) показників ефективності на узагальнений показник ефективності функціонування СЗІКБ подано в табл. 2.

Таблиця 2. Критерії оцінки окремих (часткових) показників ефективності на узагальнений показник ефективності функціонування СЗІКБ

| Критерії оцінки ефективності | окремий (частковий) показник ефективності ($E_{ч(СЗІКБ)}$) | | | | |
|---|---|---|---|---|---|
| | $0 \le E_{ч(СЗІКБ)} \le 0{,}25$ | $0{,}25 < E_{ч(СЗІКБ)} \le 0{,}5$ | $0{,}5 < E_{ч(СЗІКБ)} \le 0{,}75$ | $0{,}75 < E_{ч(СЗІКБ)} \le 0{,}9$ | $0{,}9 < E_{ч(СЗІКБ)} \le 1$ |
| | незадовільний (НЗ) | низький (Н) | середній (С) | високий (В) | найвищий (НВ) |
| $0 \le E_{СЗІКБ} \le 0{,}25$ | НЗ | НЗ | НЗ | НЗ | НЗ |
| $0{,}25 < E_{СЗІКБ} \le 0{,}5$ | Н | Н | Н | Н | Н |
| $0{,}5 < E_{СЗІКБ} \le 0{,}75$ | С | С | С | С | С |
| $0{,}75 < E_{СЗІКБ} \le 0{,}9$ | С | С | С | В | В |
| $0{,}9 < E_{СЗІКБ} \le 1$ | В | В | В | В | НВ |

Клітинки табл. 2, розташовані на перетині відповідних рядків і стовпців, вказують рівень спроможності обчисленого часткового показника щодо впливу на забезпеченні відповідної ефективності $E_{СЗІКБ}$.

Математичну модель оцінювання ефективності функціонування СЗІКБ за показником кіберзахищеності ($P_{КЗ}$) можна представити як наближене співвідношення (4):

$$E_{СЗІКБ} \approx P_{КЗ} \tag{4}$$

Повну викладку методики розрахунку кіберзахищеності опускаємо, оскільки детально описано в роботі [8].

Критерії оцінки кіберзахищеності, що забезпечує СЗІКБ за результатами внутрішнього (пасивного) аудиту подано в табл. 3.

Таблиця 3. Критерії оцінки кіберзахищеності, що забезпечує СЗІКБ за результатами внутрішнього (пасивного) аудиту

| $P_{КЗ}$ | $P_{КЗ}^{РТ}(S)$ | Рівень | Рівень кіберзахищеності |
|---|---|---|---|
| $0{,}9 < P_{КЗ} \le 1$ | $0{,}9 < P_{КЗ}^{РТ}(S) \le 1$ | найвищий | Високий рівень кіберзахищеності, ДІВ практично ніколи не буде проведено |
| $0{,}75 < P_{КЗ} \le 0{,}9$ | $0{,}75 < P_{КЗ}^{РТ}(S) \le 0{,}9$ | високий | Середній рівень кіберзахищеності, ймовірність проведення ДІВ досить низька |
| $0{,}5 < P_{КЗ} \le 0{,}75$ | $0{,}5 < P_{КЗ}^{РТ}(S) \le 0{,}75$ | середній | Низький рівень кіберзахищеності, ймовірність проведення ДІВ середня |
| $0{,}25 < P_{КЗ} \le 0{,}5$ | $0{,}25 < P_{КЗ}^{РТ}(S) \le 0{,}5$ | низький | Дуже низький рівень кіберзахищеності, ймовірність проведення ДІВ висока . |
| $0 \le P_{КЗ} \le 0{,}25$ | $0 \le P_{КЗ}^{РТ}(S) \le 0{,}25$ | незадовільний | Не задовільний рівень кіберзахищеності, ймовірність проведення ДІВ дуже висока |

Наступним етапом розглянемо оцінювання ефективності функціонування СЗІКБ за частковим показником (кіберзахищеності) виявлених активних загроз за результатами penetration testing.

Даний підхід вбачає за мету контроль кіберзахищеності засобів та їх компонентів ІТС станом на момент часу $t_{ДІВ1}$ за умов дій тестових деструктивних інформаційних впливів (ДІВ), $F_{ДІВ}$ =1. Якщо в СЗІКБ є засоби (компоненти) активної протидії кібервпливам (ДІВ), то в такому випадку обчислення $P_{КЗ}(S)$ здійснюється з використанням показників вдалих і невдалих спроб порушення нормального функціонування зазначеного засобу. Розрахунок кіберзахищеності $P_{КЗ}(S)$ системи $S$ здійснюється за формулою (5):

$$P_{КЗ}^{РТ}(S) = 1 - \frac{N_{ДІВ}^{Вдалих}(S)}{N_{ДІВ}^{Заг}(S)}, \tag{5}$$

де $N_{ДІВ}^{Заг}(S)$ – загальна кількість проведених ДІВ на всю систему $S$;

$N_{ДІВ}^{Вдалих}(S)$ – кількість вдалих спроб реалізації ДІВ на всю систему $S$ за результатами сповіщення системою фіксування інцидентів.

Висновок про стан кіберзахищеності за результатами penetration testing робимо на основі отриманих даних та відповідності їх табл. 3.

Оцінювання ефективності функціонування СЗІКБ за частковим показником укомплектованості засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту наступним чином. Для цього розрахуємо коефіцієнт укомплектованості засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту за формулою (6):

$$K_{УЗ} = \frac{Ф_З}{Ш_З}, \tag{6}$$

де $K_{УЗ}$ – коефіцієнт укомплектованості засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ш_З$ – штатна чисельність засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ф_З$ – фактично наявна чисельність засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту.

Критерії оцінки спроможності укомплектованої засобами СЗІКБ можуть критично впливати на узагальнений показник ефективності функціонування СЗІКБ, який подано в табл. 2.

Для оцінювання ефективності функціонування СЗІКБ за частковим показником технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту розрахуємо коефіцієнт технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту за формулою (7):

$$K_{ТГЗ} = \frac{Ф_{СЗ}}{Ф_З}, \tag{7}$$

де $K_{ТГЗ}$ – коефіцієнт технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ф_{СЗ}$ – кількість справних засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ф_З$ – фактично наявна чисельність засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

Критерії оцінки спроможності технічної готовності засобами СЗІКБ можуть критично впливати на узагальнений показник ефективності функціонування СЗІКБ, який подано в табл. 2.

Оцінювання ефективності функціонування СЗІКБ за частковим показником укомплектованості справними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту здійснимо за допомогою коефіцієнта укомплектованості справними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту, який розрахуємо за формулою (8):

$$K_{УСЗ} = K_{УЗ} \times K_{ТГЗ} = \frac{Ф_{СЗ}}{Ш_З}, \tag{8}$$

де $K_{УСЗ}$ – коефіцієнт укомплектованості справними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$K_{УЗ}$ – коефіцієнт укомплектованості засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$K_{ТГЗ}$ – коефіцієнт технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ф_{СЗ}$ – кількість справних засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту;

$Ш_З$ – штатна чисельність засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту.

Критерії оцінки спроможності укомплектованими справними засобами СЗІКБ можуть критично впливати на узагальнений показник ефективності функціонування СЗІКБ, який подано в табл. 2.

Розглянемо оцінювання ефективності функціонування СЗІКБ за частковим показником укомплектованості штатних посад системними адміністраторами. Даний підхід вбачає за мету оцінити ефективність функціонування СЗІКБ за показником укомплектованості штатних посад системними адміністраторами та обслуговуючим персоналом та одержаним при цьому рівнем кіберзахищеності. Для цього скористаємось наступною формулою (9):

$$K_{СА} = \frac{Ф_{СА}}{Ш_{СА}}, \tag{9}$$

де $K_{СА}$ – коефіцієнт укомплектованості штатних посад системними адміністраторами СЗІКБ;

$Ш_{СА}$ – штатна чисельність посад системних адміністраторів СЗІКБ;

$Ф_{СА}$ – фактично наявна чисельність системних адміністраторів СЗІКБ.

Критерії оцінки спроможності укомплектованості штатних посад системними адміністраторами СЗІКБ можуть критично впливати на узагальнений показник ефективності системи подано в табл. 2.

Оцінювання ефективності функціонування СЗІКБ за частковим показником укомплектованості штатних посад обслуговуючим персоналом розрахуємо допомогою коефіцієнта укомплектованості штатних посад обслуговуючим персоналом, а саме за формулою (10):

$$K_{ОП} = \frac{Ф_{ОП}}{Ш_{ОП}}, \tag{10}$$

де $K_{ОП}$ – коефіцієнт укомплектованості штатних посад обслуговуючим персоналом СЗІКБ;

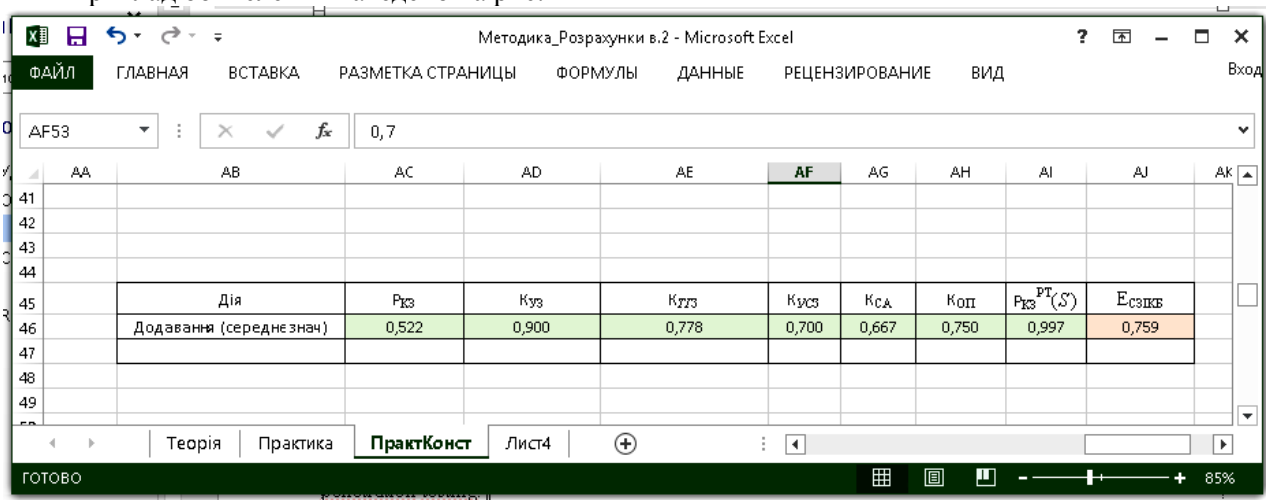
$Ш_{ОП}$ – штатна чисельність посад обслуговуючого персоналу СЗІКБ;

$Ф_{ОП}$ – фактично наявна чисельність обслуговуючого персоналу СЗІКБ.

Критерії оцінки спроможності укомплектованості штатних посад обслуговуючим персоналом СЗІКБ критично впливати на узагальнений показник ефективності функціонування СЗІКБ подано в табл. 2.

Тоді узагальнений показник ефективності функціонування СЗІКБ обчислимо за формулою (3).

Приклад обчислення наведено на рис. 1




| Дія | $Р_{КЗ}$ | $К_{УЗ}$ | $К_{УГЗ}$ | $К_{УСЗ}$ | $К_{СА}$ | $К_{ОП}$ | $Р_{КЗ}^{РТ}(S)$ | $Е_{СЗІКБ}$ |
|---|---|---|---|---|---|---|---|---|
| Додавання (середнє знач) | 0,522 | 0,900 | 0,778 | 0,700 | 0,667 | 0,750 | 0,997 | 0,759 |

Рис. 1. Фрагмент обчислення ефективності із застосуванням Microsoft Excel

Відповідно до значення $Е_{СЗІКБ}$, оцінювання ефективності здійснимо за критеріями наведених в табл. 1. Для значення $Е_{СЗІКБ}$,=0,759 – в цілому високий рівень ефективності, система захисту інформації і кібербезпеки працездатна.

**Висновки.** На сучасному етапі науки вбачається раціональним застосовувати не всі, а найбільш показові підходи, показники та критерії, що дозволяють наочно продемонструвати та оцінити ефективність функціонування системи захисту інформації і кібербезпеки.

Для оцінювання ефективності функціонування системи захисту інформації і кібербезпеки запропоновано застосовувати наступні показники: кіберзахищеність; коефіцієнт укомплектованості засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту; коефіцієнт технічної готовності засобів криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту; коефіцієнт укомплектованості справними засобами криптографічного захисту інформації, технічного захисту інформації та кібернетичного захисту; коефіцієнт укомплектованості штатних посад системними адміністраторами; коефіцієнт укомплектованості штатних посад обслуговуючим персоналом; кіберзахищеність за результатами penetration testing.

**Наукова новизна одержаного результату** полягає в тому, що вперше комплексно і систематично проаналізовано підходи до вибору показників та критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.

**Перспективи подальших досліджень у даному напрямку.** Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування методики оцінювання ефективності функціонування системи захисту інформації і кібербезпеки.

**Список бібліографічного опису**

1. Закон України "Про основні засади забезпечення кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 28.05.21).
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", затверджена Указом Президента України від 15.03.16 №96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення 28.05.21).
3. Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13.02.17 №254/2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17 (дата звернення 28.05.21).
4. Маслова Н.А. Методы оценки эффективности систем защиты информационны систем. *Искусственный интеллект*. 2008. № 4.С. 253 – 264.
5. Андреев К. Метод оценки экономической эффективности подразделения по защите информации. *Информационная безопасность*. 2010. № 5. URL: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 27.11.2021).
6. Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности. *Бизнес-информатика*. 2015. №1(31). С. 51 – 57.
7. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. №2 (41). С. 17 – 22.
8. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. *Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво».* Луцьк, 2020. Випуск № 39. С. 127 – 135. URL: https://doi.org/10.36910/6775-2524-0560-2020-39-22.

**References**

1. Law of Ukraine"on basic principles of ensuring cybersecurity of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed 28.05.21).
2. On the decision of the national security and Defense Council of Ukraine of January 27, 2016 "on the cybersecurity strategy of Ukraine", approved by Presidential Decree No. 96/2016 of 15.03.16. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (accessed 28.05.21).
3. Decision of the national security and Defense Council of Ukraine of 10.07.17 "on the status of implementation of the decision of the national security and Defense Council of Ukraine of December 29, 2016" "on threats to state cybersecurity and urgent measures to neutralize them", put into effect by Presidential Decree No. 254/2017 of 13.02.17. URL: https://zakon.rada.gov.ua/
laws/show/n0006525-17 (accessed 28.05.21).
4. Maslova N.A. Methods of evaluating the effectiveness of information systems protection systems. Artificial Intelligence. 2008. No. 4.Pp. 253-264.
5. Andreev K. Method of assessing the economic efficiency of the information protection unit. Information security. 2010. No. 5. URL: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (accessed 27.11.2021).
6. Efimov E.N., Lapitskaya G.M. Evaluation of the effectiveness of information security measures under uncertainty. Business informatics. 2015. No.1(31). Pp. 51 – 57.
7.Kozubtsova L.M., Khlaponin Yu.I., Kozubtsov I.M. Methodology for evaluating the effectiveness of measures to ensure cybersecurity of critical information infrastructure objects of organizations. Modern information technologies in the field of security and defense. 2021. №2 (41). Pp. 17 – 22.
8.Kozubtsova L.M. Improved methodology for diagnosing cybernetic security of an information system taking into account destructive cybernetic influences. Scientific journal "Computer-Integrated Technologies: Education, Science, production". Lutsk, 2020. Issue # 39. Pp. 127-135. URL: https://doi.org/10.36910/6775-2524-0560-2020-39-22.