КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ/ CYBER-SECURITY & CRITICAL INFORMATION INFRA-STRUCTURE PROTECTION

DOI: 10.18372/2225-5036.29.17868

КІБЕРСТАТИСТИКА В УКРАЇНІ. СУЧАСНИЙ СТАН

Андрій Давидюк[1], Віталій Зубок[2], Юлія Хохлачова[3], Микола Худинцев[4], Максим Комаров[5]

[2, 3] Національний авіаційний університет
[1,4, 5] Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

ДАВИДЮК Андрій Вікторович, молодший науковий співробітник.
Рік та місце народження: 1994 рік, м. Звягель, Житомирська область, Україна.
Освіта: Інститут спеціального зв'язку та захисту інформації України Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», 2018 рік.
Посада: молодший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України.
Наукові інтереси: кібербезпека, аудит систем управління інформаційної безпеки, кіберзахист критичної інфраструктури, управління ризиками, кіберстійкість.
Публікації: понад 60 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях, патент на корисну модель.
E-mail: andrey19941904@gmail.com.
Orcid ID: 0000-0003-1238-2598.

ЗУБОК Віталій Юрійович, д.т.н., старший дослідник.
Рік та місце народження: 1971 рік, м. Київ, Україна.
Освіта: Київський політехнічний інститут, 1994 рік.
Посада: професор кафедри Комп'ютеризованих систем управління НАУ.
Наукові інтереси: глобальні комп'ютерні мережі, топологія складних мереж, кібербезпека, управління ризиками, кіберстійкісь, цифрова стійкість.
Публікації: понад 80 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: vit@visti.net.
Orcid ID: 0000-0002-6315-5259.

ХОХЛАЧОВА Юлія Євгеніївна, к.т.н., доц.
Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, оцінювання уразливостей, оцінювання стану кібербезпеки інформаційних систем, захищеність кіберфізичних систем.
Публікації: понад 150 друкованих наукових праць, серед яких підручники, навчальні посібники, монографії, наукові статті у вітчизняних та міжнародних фахових виданнях, матеріали і тези доповідей на конференціях, свідоцтва про реєстрацію авторського права на твір (комп'ютерну програму).
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

ХУДИНЦЕВ Микола Миколайович, к.ф.-м.н., доц., лауреат Державної премії України в галузі науки і техніки.
Рік та місце народження: 1969 рік, м. Новокузнецьк, Кемеровська обл., СРСР
Освіта: Одеський національний університет ім. І.І. Мечнікова, 1991 рік.
Посада: докторант ІПМЕ ім. Г.Є. Пухова НАН України.
Наукові інтереси: інформаційна безпека, оцінювання стану кібербезпеки інформаційних систем, захищеність кіберфізичних систем, синхронізація в телекомунікаціях, квантова теорія розсіяння, фізика гранульованих матеріалів.
Публікації: понад 90 друкованих наукових праць, серед яких монографії, наукові статті у вітчизняних та міжнародних фахових виданнях, матеріали і тези доповідей на конференціях, свідоцтва про реєстрацію авторського права на твір.
E-mail: nh@te.net.ua.
Orcid ID: 0000-0002-9324-6901.

КОМАРОВ Максим Юрійович, к.т.н.
Рік та місце народження: 1980 рік, м. Москва, СРСР.
Освіта: Спеціальний факультет Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», 2002 рік.
Посада: старший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України.
Наукові інтереси: кібербезпека, аудит систем управління інформаційної безпеки, кіберзахист критичної інфраструктури, управління ризиками, кіберстійкість, технічний захист інформації.
Публікації: понад 20 наукових публікацій, серед яких наукові статті, монографії, тези та матеріали доповідей на конференціях, патент на корисну модель, свідоцтво про реєстрацію авторського права на твір.
E-mail: maxkom32@gmail.com.
Orcid ID: 0000-0002-5739-8959.

Анотація. *З розвитком кіберзахисту в Україні збільшуються і технічні спроможності для забезпечення безпеки інформації. Новітнє обладнання здатне збирати великі масиви даних для аналізування потенційних загроз кібербезпеці. Інтеграція аналізу цих даних в процеси кіберзахисту дасть змогу попередити виникнення ряду кіберінцидентів. Водночас існує імовірність того, що суб'єкти забезпечення кібербезпеки під час виконання власних функцій збирають одні і ті ж самі набори даних інформацію, що значно зменшує ефективність їх інформаційного обміну та пов'язаних процесів. З огляду на зазначене, доцільним є впровадження процесів кіберстатистики, що має на меті диференціювати функції суб'єктів забезпечення кібербезпеки за наборами даних, які вони використовують у власній діяльності. Така диференціація допоможе визначити існуючі проблеми в процесах цих суб'єктів та сприятиме впровадженню уніфікованих підходів до збору та аналізування даних в сфері кібербезпеки. Таким чином розробка та впровадження методики збору та оброблення даних кіберстатистики дасть змогу оптимізувати процеси забезпечення кібербезпеки.*

Ключові слова: *кіберстатистика, данні, кібербезпека, кіберінцидент, кіберзахист, збір інформації.*

Аналіз останніх досліджень і публікацій

В умовах ведення проти України військових дій значно зросли загрози критичній інфраструктурі взагалі та критичній інформаційній інфраструктурі зокрема, підтвердженням чому стали випадки пошкодження об'єктів і здійснені кібератаки на енергетичну інфраструктуру, що засвідчили вразливість об'єктів критичної інфраструктури держави до нових типів загроз. Актуальність дослідження проблем кіберживучості об'єктів критичної інформаційної інфраструктури та забезпечення кіберстійкості об'єктів енергетики було розглянуто роботах [1, 2].

Процеси забезпечення кібербезпеки нерозривно пов'язані з постійним моніторингом систем і мереж передачі даних. На даний час розроблено ряд програмних та програмно-апаратних рішень для збору та оброблення цих даних. Додатково побудовані ІТ інфраструктури для агрегації цих даних з різних джерел. Розроблені бази вразливостей та загроз кібербезпеці, наприклад національна база даних уразливостей (NVD), яку підтримує NIST, і база даних Common Vulnerabilities and Exposures (CVE) [3, 4].

В Україні законодавством визначено суб'єктів забезпечення кібербезпеки (далі - СКБ) їх обов'язки, функції та повноваження. Процеси, пов'язані з виконанням цих функцій, залежать від наявних у СКБ даних, що слугують для оцінювання ризиків та підтримки прийняття рішень в сфері кібербезпеки тощо. Розуміння залежності розвитку сфери кібербезпеки від наявних технологій та методик збору та аналізу великих даних робить задачу формування кіберстатистики актуальною. Враховуючи відсутність в українсь-

кому законодавстві терміну «кіберстатистика», з метою уникнення невизначеностей при подальшому викладенні матеріалу дослідження, під кіберстатистикою будемо розуміти результат збору, аналізування та інтерпретації даних, пов'язаних із інцидентами кібербезпеки (кіберінцидентами), кіберзагрозами, вразливостями та тенденціями (трендами) кібербезпеки. Вона охоплює кількісне вимірювання та дослідження інцидентів кібербезпеки, загроз, вразливостей, тенденцій та інших відповідних факторів. Це передбачає використання статистичних методів і методологій, щоб отримати уявлення про ландшафт кібербезпеки, що постійно змінюється.

Завданням Стратегії кібербезпеки України [5] С. 3-19 передбачено розроблення методики збору кіберстатистики то щорічне оприлюднення статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах. Завданням Плану реалізації цієї стратегії [6] передбачено розроблення та затвердження методики збору кіберстатистики нормативно-правовим актом Адміністрації Державної служби спеціального зв'язку та захисту інформації України, а такою збирання та оприлюднення у відповідності до розробленої методики відповідних статистичних даних.

Станом на 01.05.2023 р. термін «кіберстатистика» є предметом гострих дискусій з нормативної та наукової точки зору. Ряд досліджень, зокрема [7], до кіберстатистики відносять:

- тенденції кібербезпеки;
- найбільші витоки даних і статистика зламів;
- статистику кіберзлочинності за типом атак;
- статистику відповідності та управління кібербезпекою;
- галузеву кіберстатистику;
- статистику витрат на кібербезпеку;
- статистику зайнятості в сфері кібербезпеки;
- популярні загрози та тенденції загроз;
- вартість кіберзлочинності;
- моделі та засоби захисту;
- поширені типи кібератак;
- щоденну та щорічну кількість атак, частоту атак.

У теорії статистики [8] під статистикою розуміють:

- кількісні дані, які характеризують визначену сторону суспільного життя;
- практичну діяльність державних установ, спрямовану на збір, обробку і аналіз даних про масові явища та процеси суспільного життя;
- науку, яка розробляє і впроваджує принципи і методи дослідження кількісних характеристик масових суспільних явищ.

Постановка проблеми

Предметом статистичного вивчення (дослідження) є розміри і кількісні співвідношення масових суспільних явищ та закономірностей їх формування і розвитку в конкретних умовах простору та часу. Статистичні дослідження здійснюються за допомогою методів масового статистичного спостереження, статистичного зведення і групування, узагальнених статистичних показників, а також їх аналізу, викладення та інтерпретації.

До показників (індикаторів, параметрів, характеристик) масових суспільних явищ можуть буди віднесені, з певними обумовленнями, показники метаданих, індикатори безпеки, компрометації, загроз, заходів з протидії шкідливому впливу, інші показники, пов'язані з даними технічного характеру.

Загальна картина, яка характеризує порушників та зловмисників, в сфері кібербезпеки, змінюється з часом, але загальні категорії загроз та небезпек лишаються незмінними. Для того, щоб зірвати плани зловмисників проводяться відповідні дослідження, тому точна та актуальна класифікація кіберзагроз відіграє важливу роль в цьому процесі. Загальні вимоги до таксономії кіберзагроз об'єктів критичної інформаційної інфраструктури наведені у роботі «Requirements for a Taxonomy of Cyber Threats of Critical Infrastructure Facilities and an Analysis of Existing Approaches» [9].

Мета та постановка завдання

Кіберстатистика відіграє значну роль у розумінні характеру та масштабів кіберзагроз, виявленні моделей і тенденцій атак і формулюванні ефективних стратегій для зменшення ризиків. Аналізуючи відповідні дані, фахівці з кібербезпеки можуть оцінити ефективність заходів кібербезпеки, визначити напрями для покращення та прийняти обґрунтовані рішення для поліпшення загального стану кібербезпеки. Кіберстатистика використовується для аналізування кіберінцидентів, зокрема вивчення даних про минулі кіберінциденти, для визначення векторів кібератак, їх методів і тенденцій, а також розуміння впливу різних типів кібератак. Ця статистика також є необхідною для розвідки загроз, збору і аналізування даних про нові кіберзагрози, включаючи шкідливе програмне забезпечення, фішингові кампанії, методи злому та вразливості, для завчасного виявлення потенційних ризиків. Водночас є корисною для оцінювання ризиків, зокрема використання статистичних моделей для оцінювання ймовірності та впливу кіберзагроз і вразливостей, допомоги організаціям у визначенні пріоритетів їхніх заходів кібербезпеки та ефективного розподілу ресурсів. Вимірювання продуктивності, в тому числі моніторинг і вимірювання ефективності засобів контролю безпеки, таких як системи виявлення вторгнень, брандмауери та антивірусне програмне забезпечення, щоб визначити області для вдосконалення та оптимізувати механізми захисту також використовують кіберстатистику. Аналіз відповідності та нормативних вимог також потребує аналізу даних для оцінки відповідності нормам кібербезпеки, галузевим стандартам і

найкращим практикам, а також виявлення областей невідповідності або вразливостей, що не можливо без кіберстатистики. Використовуючи кіберстатистику, організації можуть отримати глибше розуміння кіберзагроз, з якими вони стикаються, приймати рішення на основі даних для підвищення рівня безпеки та ефективно реагувати на інциденти. Ця галузь продовжує розвиватися в міру появи нових джерел даних, статистичних методів і аналітичних підходів, що дозволяє створювати більш ефективні та проактивні стратегії кібербезпеки.

Нормативно-правову базу в Україні статистики в цілому та кіберстатистики зокрема становлять наступні нормативно-правові акти:

- Закон України «Про офіційну статистику» [10];

- Закон України «Про основні засади забезпечення кібербезпеки України» [11];

- Наказ Державної служби статистики України від 26.07.2022 № 212 «Про затвердження форми державного статистичного спостереження №1-ІКТ (річна) "Використання інформаційно-комунікаційних технологій на підприємстві у 2023 році"» [12];

- Указ Президента України від 26.08.2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» [5];

- Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [13];

- Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені Наказом Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 [14].

Виклад основного матеріалу дослідження

Аналіз наявних наборів даних кіберстатистики

Основою підготовки даних в рамках статистичного підходу є визначення базисних параметрів, призначених для зіставлення незіставних статистичних показників. Базисні параметри статистичної сукупності формують систему базисних параметрів та є системоутворюючими для такої системи. Формування системи базисних параметрів вважається основним завданням системного аналізу статистичних систем.

До базовий параметрів наборів даних кіберстатистики або статистичної системи індексів про кіберінциденти, кібератаки, кіберзагрози та заходи протидії можуть належати:

- індикатори кіберінцидентів;
- індикатори кібератак;
- індикатори кіберзагроз;
- індикатори кіберризиків;
- заходи (показники заходів) кіберзахисту.

Набори даних кіберстатистики мають враховувати положення нормативних документів:

- Національна система оцінки кіберінцидентів CISA / CISA National Cyber Incident Scoring System (NCISS);

- Класифікація кіберінцидентів (Звіт про нові практики в регіоні ОБСЄ) / Cyber Incident Classification (A Report on Emerging Practices within the OSCE Region);

- NIST: Оцінка кіберризиків / NIST Cyber Risk Scoring (CRS);

- MITRE: показники кібервідмовостійкості, показники ефективності та оцінка / MITRE: Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring;

- ETSI GS ISI 00X Індикатори інформаційної безпеки / ETSI GS ISI 00X Information Security Indicators (ISI);

- ISO/IEC 27004:2016(E) Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимірювання, аналіз та оцінка;

- Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 р. № 601.

Відповідні базисні параметри широко використовуються для формування глобальних індексів кібербезпеки [15].

Станом на сьогодні найбільш розповсюдженими процесами кібербезпеки, пов'язаними зі статистикою статистичний аналіз витоків даних, кібератак та інцидентів кібербезпеки, що дає можливість оцінити їх частоту, вплив і характеристики, розвідка загроз (Threat Intelligence) – для аналізу потенційних викликів кібербезпеки, пошук і розповсюдження відомостей про вразливості, зокрема кількісна оцінка вразливостей програмного забезпечення та їх використання для визначення пріоритетів у процесах управління вразливостями, оцінювання ризиків, зокрема застосування статистичних методів для оцінки ймовірності та потенційного впливу різних ризиків кібербезпеки на інформаційні активи та IT інфраструктуру організації, аудит інформаційної безпеки, зокрема в частині відповідності вимогам для оцінки дотримання правил і стандартів кібербезпеки, формування шаблонів атак для їх статистичного аналізу, зокрема таких як розповсюдження зловмисного програмного забезпечення, фішингові кампанії або вторгнення в мережу, для виявлення повторюваних методів і шаблонів, контроль стану кібербезпеки для оцінки ефективності заходів безпеки шляхом статистичного аналізу інцидентів і результатів їх оброблення, поведінковий аналіз дій користувача, як-от використання пароля, оцінювання чутливості до методів соціальної інженерії для підвищення обізнаності щодо кібербезпеки та навчання персоналу.

Вищезазначені процеси включають перелік основних наборів даних, таких як дані про кіберінциденти (тип атаки, уражені системи, вплив і методи,

використані зловмисниками); дані розвідки загроз (індикатори компрометації (IOC), сигнатури шкідливих програм, шкідливі IP-адреси, домени та URL-адреси), бази даних вразливостей (оцінка критичності, уражені системи та доступні виправлення), дані мережевого трафіку (дані на рівні пакетів, записи мережевого потоку або мережеві журнали), дані про зразки шкідливого програмного забезпечення (далі – ШПЗ) (зразки ШПЗ), дані з журналів поведінки користувача та автентифікації (дії користувача, події автентифікації та шаблони доступу в системі чи мережі), дані з відкритих джерел та дані Dark Web (інформація про дискусії, тенденції та події, пов'язані з кіберзагрозами та хакерськими спільнотами), дані з аудиту інформаційної безпеки (далі - ІБ) (інформація, пов'язана з дотриманням стандартів і правил кібербезпеки).

Вищезазначені процеси в тому чи іншому вигляді представлені у функціях СКБ, а отже і присутні вищевказані набори даних та, можливо, і інші відомості. Таким чином стає можливим створити умовну матрицю розподілу наборів даних між СКБ (табл. 1) відповідно до їх функцій.

Таблиця 1.

Зразок структури бази даних з кібербезпеки СКБ

СКБ	**Набори даних**							
	Дані про кіберінциденти	Дані розвідки загроз	Бази даних вразливостей	Дані мережевого трафіку	Дані про ШПЗ	Дані з журналів	Дані з відкритих джерел та дані Dark Web	Дані з аудиту ІБ
Державна служба спеціального зв'язку та захисту інформації України								
Національна поліція України								
Служба безпеки України								
Міністерство оборони України та Генеральний штаб Збройних Сил України								
Розвідувальні органи								
Національний банк України								

Абстрагуючись від конкретних завдань кожного СКБ, стає зрозуміло, що СКБ можна розділити на дві категорії – надавачі та користувачі на наборів даних. Водночас варто розуміти, що кожен СКБ може бути одночасно надавачем і користувачем одного і того ж самого набору даних. Однак після заповнення такої матриці стане зрозумілою необхідність створення (або достатність) спільних ресурсів (баз даних) для наповнення даними кіберстатистики та надання доступу для користування.

У випадку коли надавачами даних з одного набору є декілька СКБ доцільним є створення додаткової класифікації відомостей з набору даних для більш швидкої адресної роботи з ними. Розробка такої класифікації потребує детального аналізу функцій кожного СКБ, так як критеріями для класифікації даних кіберстатистики, повинні стати вимоги до оцінювання (вимірювання) результатів виконання функцій СКБ в часі. Оцінювання результатів виконання функцій СКБ на основі кіберстатистики дасть змогу об'єктивно сформувати потреби СКБ у кадровому та матеріальному забезпеченні.

Формування кіберстатистики

Очевидно, що джерелами та агрегаторами кіберстатистики є не тільки СКБ. Таким чином є доцільним визначити окремо основних суб'єктів забезпечення кіберстатистики. До них можна віднести команди реагування на комп'ютерні надзвичайні події (наприклад CERT-UA) [16], Національний координаційний центр кібербезпеки при РНБО України [17], Державна служба статистики України [18], Кіберполіція [19], органи оцінки відповідності [20], галузеві регуляторні органи з повноваженням в сфері кібербезпеки (наприклад Державна інспекція в сфері ядерного регулювання в сфері енергетики [21]), науково-дослідні установи та аналітичні центри, галузеві асоціації та громадські об'єднання, міжнародні організації, такі як Організація Об'єднаних Націй (ООН) [22], Міжнародний союз електрозв'язку (ITU) [23] або Агентство Європейського Союзу з кібербезпеки (ENISA)

[24], центри компетенцій можуть сприяти обміну кіберстатистикою між країнами-членами та сприяти гармонізації статистичних методологій.

Отже, кіберстатистика спирається на збір відповідних даних із різних джерел, таких як звіти про інциденти, канали розвідки про загрози, бази даних уразливостей, мережеві журнали, журнали поведінки користувачів і дані відповідності. Ці джерела даних можна отримати від державних установ, приватних організацій, науково-дослідних установ або галузевих асоціацій. Потім зібрані дані агрегуються та стандартизуються для забезпечення їх послідовності та порівнянності. Для забезпечення послідовності та порівнюваності (кореляцій) цих даних доцільно визначити базові методи збору та оброблення кіберстатистики.

Опитування та анкети використовуються для збору даних безпосередньо від окремих осіб, організацій або секторів промисловості. Ці інструменти можуть містити запитання про методи кіберзахисту, звітування про інциденти, засоби контролю безпеки та обізнаність користувачів. Опитування допомагають збирати суб'єктивну інформацію та отримувати думки від широкого кола зацікавлених сторін.

Методи статистичного аналізу застосовуються до зібраних даних, щоб отримати вибірку найважливішої інформації та кількісно визначити різні аспекти кібербезпеки. Описова статистика, наприклад підрахунок частоти, середні значення та відсотки, допомагає узагальнити й описати дані. Перевірку гіпотез, регресійний аналіз або аналіз часових рядів, можна використовувати, щоб зробити висновки, виявити кореляції та оцінити тенденції.

Методи машинного навчання [25] та інтелектуального аналізу [26] даних використовуються для виявлення закономірностей, аномалій і зв'язків (залежностей) у наборах даних кібербезпеки. Ці методи можуть допомогти у визначенні нових шаблонів атак, прогнозуванні майбутніх загроз або виявленні шкідливих дій. Алгоритми машинного навчання, такі як кластеризація, класифікація або виявлення аномалій, застосовуються до даних кібербезпеки, щоб отримати цінну інформацію.

В загальному сенсі машинне навчання – це процес використання хронологічних («історичних») даних для створення алгоритму прогнозування за майбутніми даними [27].

Методи моделювання використовуються для повторення сценаріїв кіберінцидентів і оцінки потенційного впливу різних факторів. Використовуючи дані ретроспективного аналізу, статистичні розподіли та інструменти моделювання, аналітики можуть оцінити ймовірність подій в кіберпросторі, оцінити ефективність заходів кібербезпеки або спрогнозувати потенційні наслідки політичних рішень в сфері кібербезпеки.

Кіберстатистиці часто допомагають міждисциплінарні дослідницькі підходи, які поєднують методології з таких галузей, як економіка, соціологія, психологія чи наука про дані. Ці міждисциплінарні підходи забезпечують повне розуміння економічних, соціальних і поведінкових аспектів кібербезпеки, роблячи аналіз кіберстатистики більш цілісним та повним.

Звісно, варто також визначити загальні критерії до даних кіберстатистики для отримання об'єктивних результатів, зокрема під час вибору наборів даних для кіберстатистики слід враховувати якість, релевантність і придатність даних. До основних критеріїв для оцінки наборів даних для кіберстатистики можна віднести довіру до джерела даних і його авторитет. Набори даних з авторитетних джерел, таких як урядові установи, визнані дослідницькі установи або галузеві асоціації, як правило, більш надійні та заслуговують довіри. Необхідно також оцінити масштаб і охоплення набору даних, зокрема визначити, чи охоплює він конкретні аспекти кібербезпеки, які цікавлять, наприклад інциденти, загрози, уразливості або поведінку користувачів. Також треба оцініть якість даних і надійність набору даних, в тому числі повноту, точність, узгодженість і цілісність даних з урахуванням методології збору даних, процесів перевірки даних і будь-які відомі конфлікти інтересів чи обмеження. Кібербезпека — це сфера, яка швидко розвивається, тому вкрай важливо враховувати своєчасність і актуальність набору даних. Доцільно працювати з наборами даних, які регулярно оновлюються, щоб відобразити останні найновіші тенденції, загрози та технології. Застарілі дані можуть не точно відображати поточний ландшафт кібербезпеки. Залежно від потреб СКБ до формування кіберстатистики можуть знадобитися конкретні атрибути, як-от вектори атак, уражені системи або характеристики ШПЗ. Набір даних має забезпечувати необхідний рівень деталізації для досягнення конкретних цілей. Варто враховувати конфіденційність і етичні норми, пов'язані з наборами даних, зокрема відповідність. процесів збору та обміну даними чинним законам і нормам. Для захисту конфіденційної інформації та конфіденційності осіб або організацій, представлених у наборі даних, мають бути вжиті заходи анонімізації та захисту даних. З огляду на зазначене доцільно визначити, чи є набір даних загальнодоступним чи для доступу потрібні певні дозволи, угоди.

Таким чином кіберстатистика є важливим елементом кібербезпеки країни, однак потребує багато зусиль та ресурсів для її коректного формування.

Висновки. Використовуючи кіберстатистику, дослідники та практики можуть отримати уявлення про мінливий характер кіберзагроз, розробляти стратегії управління ризиками, оцінювати ефективність заходів кібербезпеки та розробляти підходи до кібербезпеки.

Доступ до цих наборів даних і їх аналіз часто потребують належної авторизації, дотримання правил

конфіденційності та дотримання етичних міркувань. Багато дослідницьких організацій з кібербезпеки, наукових установ і державних установ зберігають і надають доступ до підібраних наборів даних для дослідницьких цілей, забезпечуючи при цьому конфіденційність і безпеку даних.

Співпраця та обмін інформацією між цими зацікавленими сторонами мають вирішальне значення для забезпечення повної та точної кіберстатистики, яка може підтримувати ефективне прийняття рішень щодо кібербезпеки.

Важливо зазначити, що розробка кіберстатистики вимагає ретельного розгляду якості даних, репрезентативності та етичних міркувань, зокрема захисту конфіденційності. Перевірка джерел даних, забезпечення статистичної достовірності аналізу та збереження цілісності даних є важливими аспектами розробки надійної кіберстатистики.

Варто зазначити, що сама по собі кіберстатистика не надає комплексних рішень безпеки, але є цінним інструментом для розуміння ландшафту кібербезпеки та інформування процесів прийняття рішень.

Список літератури

[1]. Комаров М.Ю., Гончар С.Ф., Дмітрієва Д.О. Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 2021. С. 59-66.

[2]. Комаров М.Ю., Гончар С.Ф. Актуальність забезпечення кіберстійкості об'єктів енергетики. III Наук-практ. конф. «Безпека енергетики в епоху цифрової трансформації», 22.12.2021. 79 с.

[3]. NVD – Home [Electronic resource] // NVD - Home. Mode of access: https://nvd.nist.gov/ (date of access: 12.06.2023).

[4]. CVE -CVE [Electronic resource] // CVE -CVE. Mode of access: https://cve.mitre.org/ (date of access: 12.06.2023).

[5]. Стратегія кібербезпеки України, Указ Президента України від 26.08.2021 № 447/2021, «Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України».

[6]. Указ Президента України від 01.02.2022 № 37/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України».

[7]. 50 найпопулярніших статистичних даних, цифр і фактів з кібербезпеки, Е.Воттерс, Computing Technology Industry Association (CompTIA). 27 Jan. 2023. URL: https://connect.comptia.org/blog/cyber-security-stats-facts (дата звернення: 10.05.2023).

[8]. Мармоза А.Т. Теорія статистики. 2-е вид. переоб. і доп. К.: Центр учбової літератури, 2013. 592 с.

[9]. Komarov M., Davydiuk A., Onyskova A., Tkachenko V., Honchar S. (2021) Requirements for a Taxonomy of Cyber Threats of Critical Infrastructure Facilities and an Analysis of Existing Approaches. In: Zaporozhets A., Artemchuk V. (eds) Systems, Decision and Control in Energy II. Studies in Systems, Decision and Control, vol 346. Springer, Cham. 22 March 2021.

[10]. Про офіційну статистику: Закон України від 16.08.2022 р. № 2524-IX. URL: https://zakon.rada. gov. ua / laws / show / 2524-20#Text (дата звернення: 13.06.2023).

[11]. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https: //zakon. rada. gov. ua / laws / show / 2163-19#Text (дата звернення: 13.06.2023).

[12]. Про затвердження форми державного статистичного спостереження N 1-приватизація, додатка до форми державного статистичного спостереження N 1-приватизація та Інструкції щодо їх заповнення : Наказ Держ. ком. статистики України від 24.10.2005 р. № 326 : станом на 11 січ. 2007 р. URL: https://zakon. rada. gov. ua / laws / show / z1358-05#Text (дата звернення: 13.06.2023).

[13]. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 р. № 518 : станом на 7 верес. 2022 р. URL: https: // zakon. rada. gov.ua/laws/ show / 518-2019-п#Text (дата звернення: 13.06.2023).

[14]. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (зі змінами). URL: https://cip.gov.ua/ua/ news / nakaz-ad-2021-10-06-601 (дата звернення: 13.06.2023).

[15]. Худинцев М.М. (заг. ред.), Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. К.: 2021. 240 с.

[16]. CERT-UA [Electronic resource] // cert.gov.ua. Mode of access: https://cert.gov.ua/ (date of access: 12. 06.2023).

[17]. Про Національний координаційний центр кібербезпеки [Електронний ресурс] : Указ Президента України від 07.06.2016 р. № 242/2016 : станом на 17 лип. 2021 р. Режим доступу: https://zakon.rada.gov. ua/laws/show/242/2016#Text (дата звернення: 12.06. 2023).

[18]. Державна служба статистики України [Електронний ресурс] // ukrstat.gov.ua. Режим доступу: https://www.ukrstat.gov.ua/ (дата звернення: 12.06. 2023).

[19]. Кіберполіція [Електронний ресурс] // cyberpolice.gov.ua. Режим доступу: https://cyberpolice.gov.ua/ (дата звернення: 12.06.2023).

[20]. Що таке орган з оцінки відповідності? - Державна служба України з питань праці [Електронний ресурс] // Державна служба України з питань праці - Державна служба України з питань праці. Режим доступу: https://dsp.gov.ua (дата звернення: 12.06.2023).

[21]. Державна інспекція ядерного регулювання України [Електронний ресурс] // snriu.gov.ua/. Режим доступу: https://snriu.gov.ua/ (дата звернення: 12.06.2023).

[22]. Організація Об'єднаних Націй в Україні [Електронний ресурс] // Організація Об'єднаних Націй в Україні. Режим доступу: https://ukraine.un.org/uk (дата звернення: 12.06.2023).

[23]. ITU [Electronic resource] // itu.int. Mode of access: https://www.itu.int/ru/Pages/default.aspx (date of access: 12.06.2023).

[24]. ENISA [Electronic resource] // ENISA. Mode of access: https://www.enisa.europa.eu/ (date of access: 12.06.2023).

[25]. Machine Learning, ML [Electronic resource] // IT-Enterprise – your one-stop ecosystem for reengineering | it.ua. Mode of access: https://www.it.ua/knowledge-base / technology-innovation / machine-learning (date of access: 12.06.2023).

[26]. Basic Data Mining Concepts [Electronic resource] // Microsoft Learn: Build skills that open doors in your career. Mode of access: https: // learn.microsoft.com/ru-ru/analysis-services/data-mining/data-mining-concepts?view=asallproducts-allversions (date of access: 12.06.2023).

[27]. Clarence Chio and David Freeman "Machine Learning and Security", O'Reilly, 2020, 388 p.

УДК 004.622

Davydiuk A., Zubok V., Khokhlachova Yu., Khudyntsev M., Komarov M. The cyber statistics in Ukraine. Current state

Abstract. *With the development of cybersecurity in Ukraine, the technical capabilities for ensuring information security are increasing. Modern equipment can collect large amounts of data for analyzing potential cybersecurity threats. Integrating the analysis of this data into cybersecurity processes will enable the prevention of various cyber incidents. However, it is possible that cybersecurity entities may collect the same sets of data during their functions, which significantly reduces the effectiveness of their information exchange and related processes. Considering this, it is advisable to implement cyber statistics processes aimed at differentiating the functions of cybersecurity entities based on the datasets they use in their activities. Such differentiation will help identify existing problems in the operations of these entities and contribute to the implementation of unified approaches to data collection and analysis in the field of cybersecurity. Thus, the development and implementation of a methodology for collecting and processing cyber statistics data will optimize cybersecurity processes.*

Keywords*: cyber statistics, data, cybersecurity, cyber incident, cyber defense, information gathering.*

Давидюк Андрій Вікторович, аспірант кафедри Безпеки інформаційних технологій НАУ, молодший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України, Technical researcher NATO CCDCOE.
Andrii Davydiuk, Phd student of the Department of information technology security of NAU, junior scientific researcher G.E. Pukhov IMEE NAS of Ukraine, Technical researcher NATO CCDCOE.

Зубок Віталій Юрійович, доктор технічних наук, старший дослідник, професор кафедри Комп'ютеризованих систем управління НАУ.
Vitalii Zubok, Doctor of Technical Sciences, senior researcher, professor of the Department of Computerized Management Systems of NAU.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри Безпеки інформаційних технологій НАУ.
Yuliia Khokhlachova, candidate of technical sciences, associate professor, associate professor of the Department of information technology security of NAU.

Худинцев Микола Миколайович, кандидат фізико-математичних наук, доцент, докторант ІПМЕ ім. Г.Є. Пухова НАН України, лауреат Державної премії України в галузі науки і техніки.
Mykola Khudyntsev, candidate of physical and mathematical sciences, associate professor, doctoral student of the G.E. Pukhov IPME NAS of Ukraine, laureate of the State Prize of Ukraine in the field of science and technology.

Комаров Максим Юрійович, кандидат технічних наук, старший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України.
Maksym Komarov, candidate of technical sciences, associate professor, senior scientific researcher G.E. Pukhov IPME NAS of Ukraine.

Отримано *3 червня 2023 року*, затверджено редколегією *28 серпня 2023 року*