Юлія СИНИЦІНА
доцент кафедри
інформаційних технологій
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
кандидат технічних наук
https://orcid.org/0000-0002-6447-821X

КІБЕРЗАГРОЗИ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасному світі кіберзагрози стали одним із ключових викликів національній безпеці. Зростання цифрових технологій супроводжується кібератаками на державні установи, критичну інфраструктуру, фінансовий сектор та особисті дані громадян. Гібридні війни, кібершпигунство, дезінформація та шкідливе програмне забезпечення використовуються як засоби впливу на політичні та економічні процеси.

Кіберзагрози є однією з головних проблем національної безпеки в цифрову епоху. Державні установи, критична інфраструктура, підприємства та громадяни стикаються з ризиками атак на інформаційні системи, що можуть призвести до масштабних наслідків, включаючи збої в енергосистемах, фінансових установах, оборонному секторі та органах державного управління.

Кіберзагрози це небезпеки, пов'язані з використанням інформаційно-комунікаційних технологій для здійснення зловмисних дій, що спричиняють шкоду або потенційну загрозу безпеці інформаційних систем, мереж, даних або фізичних об'єктів. Кіберзагрози можуть включати кібератаки, несанкціонований доступ до даних, зловмисне програмне забезпечення (віруси, трояни, шпигунські програми), а також інші форми кібер-діяльності, які ставлять під загрозу конфіденційність, цілісність та доступність інформації або інфраструктури.

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кіберзагроза визначається як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів [1-2].

До основних видів кіберзагроз потрібно віднести: кіберзлочинність, кібершпигунство, кібертероризм, та кібервійни та гібридні загрози (рис. 1).

Рис. 1. Основні види кіберзагроз

Україна регулярно зазнає кібератак, що підривають стабільність держави. В умовах військового конфлікту особливо актуальними є ефективні методи кіберзахисту: правове регулювання, технологічні інновації, міжнародна співпраця та підготовка фахівців. Вивчення загроз та механізмів їхньої нейтралізації є необхідним для зміцнення національної безпеки та кіберстійкості держави.

Стрімкий розвиток обчислювальних технологій, поява сучасних кіберзагроз з ознаками гібридності та синергізму висуває жорсткі вимоги до економічної складової національної безпеки держави та особливо процесам забезпечення кібербезпеки функціонування економіки.

Індустрія кібербезпеки намагається відповідати вимогам сьогодення, впроваджуючи нові і більш досконалі технології і методи гарантування безпеки, однак вважається, що такий універсальний підхід недостатній [3-4]. Тому потрібно провести порівняльний аналіз основних методів аналізу кіберзагроз з визначенням переваг та недоліків кожного. До основних методів аналізу кіберзагроз потрібно віднести: метод експертних оцінок; метод аналізу загроз (Threat Analysis); метод моделювання загроз (Threat Modeling); метод аналізу ризиків; метод моніторингу та виявлення аномалій.

Метод експертних оцінок. Оцінка кіберзагроз здійснюється експертами на основі їхнього досвіду, знань та інтуїції. Цей метод включає оцінку ймовірності та потенційного впливу різних загроз на інформаційну безпеку.

Переваги: швидка оцінка загроз на основі досвіду; може бути корисним для виявлення нових, неочікуваних загроз; застосовується навіть за обмеженості даних.

Недоліки: підвищена суб'єктивність через залежність від досвіду експертів; може бути обмеженим для оцінки складних або технічно специфічних загроз; не завжди дозволяє отримати точні і кількісні результати.

Метод аналізу загроз (Threat Analysis). Цей метод передбачає систематичний підхід до ідентифікації, оцінки й аналізу загроз, що можуть впливати на інформаційні системи. Включає інструменти, такі як STRIDE або P.A.S.T.A.

Переваги: визначення потенційних загроз на всіх етапах життєвого циклу інформаційної системи; щцінка ризиків дозволяє приймати обґрунтовані заходи для зниження вразливостей; може бути інтегровано в процеси проектування та управління безпекою.

Недоліки: потрібні значні ресурси для детального та комплексного аналізу; вимагає участі кваліфікованих фахівців і спеціальних інструментів; витратний процес, особливо в масштабах великих організацій.

Метод моделювання загроз (Threat Modeling). Моделювання загроз дозволяє візуалізувати можливі атаки та вразливості в системах, щоб оцінити ймовірність їх виникнення та потенційні наслідки. Це метод, який активно використовує графічні моделі для виявлення слабких місць.

Переваги: дає змогу систематизувати та візуалізувати всі аспекти кіберзагроз; може використовуватись на ранніх етапах розробки інформаційних систем для попередження вразливостей; підвищує ефективність виявлення ризиків у складних середовищах.

Недоліки: може бути складним і дорогим у використанні для деяких організацій; не завжди може точно передбачити нові чи невідомі загрози; вимагає регулярного оновлення для відображення нових загроз.

Метод аналізу ризиків. Аналіз ризиків дозволяє оцінити ймовірність виникнення загрози та її вплив на систему. Це допомагає визначити критичні уразливості й відповідні заходи безпеки.

Переваги: дозволяє визначити пріоритети в забезпеченні безпеки; забезпечує науковий підхід до аналізу та керування ризиками; допомагає зрозуміти реальні загрози, а не лише теоретичні можливості.

Недоліки: вимагає великих обсягів даних для оцінки; складний процес, особливо в разі великої кількості факторів; залежить від точності отриманих даних та інтерпретації результатів.

Метод моніторингу та виявлення аномалій. Постійний моніторинг та виявлення аномалій дозволяє відслідковувати підозрілі дії в мережах та інформаційних системах. Використовуються методи на основі штучного інтелекту та машинного навчання для

виявлення невідомих загроз.

Переваги: забезпечує швидке реагування на нові або змінені загрози; може виявляти приховані або нові загрози в реальному часі; динамічно адаптується до нових умов.

Недоліки: високі вимоги до обчислювальних ресурсів; може викликати помилкові спрацювання, що потребує додаткової перевірки; не завжди здатне виявити складні, добре замасковані загрози.

Кожен з методів аналізу кіберзагроз має свої переваги й недоліки, і ефективність їх використання залежить від конкретних умов та цілей дослідження. Поєднання кількох методів дозволяє забезпечити комплексний підхід до оцінки та нейтралізації кіберзагроз.

Перспективні напрями дослідження кіберзагроз та методів їх виявлення в контексті національної безпеки можуть включати наступні ключові шляхи вдосконалення, а саме:

Розвиток методів прогнозування кіберзагроз: використання технологій штучного інтелекту (ШІ) та машинного навчання для прогнозування можливих кіберзагроз на основі великих даних (Big Data). Це дозволяє створювати адаптивні системи, які можуть передбачити нові загрози до того, як вони проявляться. Розробка моделей для виявлення аномалій в мережах та системах на ранніх етапах їхнього розвитку, що дозволить вчасно приймати заходи щодо нейтралізації загроз.

Інтеграція кібербезпеки з національною безпекою: створення єдиного інформаційного простору для обміну даними між державними структурами, правоохоронними органами та іншими важливими установами. Це дозволить більш ефективно відслідковувати, виявляти та нейтралізувати кіберзагрози. Розробка інтегрованих інструментів для швидкої взаємодії між органами безпеки в умовах кіберконфліктів або гібридних війн.

Створення систем автоматичного виявлення та нейтралізації кіберзагроз: використання інструментів на основі ШІ для автоматичного виявлення та блокування кібератак в реальному часі. Це дозволить зменшити час реагування на інциденти та підвищити ефективність реагування. Вдосконалення технологій глибокого навчання для виявлення нових та невідомих загроз без людського втручання [5].

Розвиток технологій блокчейн для забезпечення безпеки: використання блокчейн-технології для захисту важливої інформації та запобігання несанкціонованому доступу. Блокчейн може стати основою для розробки безпечних комунікаційних каналів та захисту даних від маніпуляцій. Створення децентралізованих систем для зберігання та передачі чутливої інформації.

Удосконалення механізмів забезпечення кібербезпеки в умовах гібридних війн: розробка нових методів протидії гібридним атакам, що включають як кіберзагрози, так і традиційні військові методи. Це передбачає інтеграцію кібербезпеки в національні стратегії безпеки. Проведення тренувань для військових та правоохоронних органів щодо кібербезпеки та розробка сценаріїв для захисту від кібератак в умовах військових конфліктів.

Покращення правового забезпечення кібербезпеки на національному рівні: розробка нових законодавчих ініціатив, які визначають правовий статус кіберзагроз, відповідальність за кіберзлочинність та критерії для виявлення кіберзагроз. Зміцнення міжнародного співробітництва щодо боротьби з кіберзагрозами та створення єдиних міжнародних стандартів кібербезпеки.

Розвиток технологій захисту критичної інфраструктури: забезпечення кібербезпеки для об'єктів критичної інфраструктури, таких як енергетичні системи, транспорт, фінансові інститути, де кіберзагрози можуть мати серйозні наслідки для національної безпеки. Впровадження систем моніторингу та виявлення вторгнень у реальному часі для забезпечення захисту критичних об’єктів інфраструктури від кіберзагроз.

Розвиток кіберспільноти для боротьби з кіберзагрозами: створення міжнародних груп для спільного аналізу та боротьби з кіберзагрозами, що дозволяє обмінюватися досвідом та кооперувати зусилля в боротьбі з кіберзлочинністю та тероризмом. Стимулювання розвитку стартапів та інновацій у сфері кібербезпеки через фінансування та створення сприятливих умов для розвитку таких ініціатив.

Ці напрямки забезпечують комплексний підхід до вирішення проблем кібербезпеки

в контексті національної безпеки, зважаючи на швидкий розвиток технологій та нові виклики, що постають у сфері кіберзагроз.

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII, Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.02.2025).

2. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2023, IDT) [Чинний від 29.11.2024] Вид. офіц. Київ : Держспоживстандарт України, 2024. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112376 (дата звернення: 10.02.2025).

3. Milov O., Hrebeniuk A., Nalyvaiko A., Pasko I., Rzayev Kh., Salii A., Soloviova O. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. *Eastern-European Journal of Enterprise Technologies*, № 6/2 (108), ISSN ISSN 1729-3774 Scopus, DOI: 10.15587/1729-4061.2020.218660, 2020 р., с. 30-52

4. Синиціна Ю. П. Інформаційна безпека в процесах виробництва та обробки даних. *Проблеми якості оборонної продукції: організаційні, технічні та фінансово-економічні аспекти. Всеукр. наук.-практ. конф. (м. Київ, 20 червня 2024 р.).* Київ: Національний університет оборони України,навчально-науковий центр оборонного менеджменту, 2024. С. 205 – 208.

5. Синиціна Ю. П. Роль штучного інтелекту у питаннях вдосконалення систем захисту від кіберзагроз. *Кібербезпека в Україні: правові та організаційні питання: матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 17 листопада 2023 р.).* Одеса: Одеськ. держ. ун-т внутр. справ, 2023. С. 74-75.

Валентина ХОДЗИЦЬКА
доцент кафедри бухгалтерського обліку та консалтингу
Київського національного економічного університету імені Вадима Гетьмана
(м. Київ, Україна)
кандидат економічних наук, доцент
https://orcid.org/0000-0002-7722-5350

ОБЛІК ЕКОЛОГІЧНИХ ВИТРАТ: АСПЕКТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Світова спільнота крок за кроком здійснює важливі кроки до міжнародної безпеки. Економіки, які завдають шкоду планеті та ресурсам, є факторами кризи. Економіки світу мають забезпечити соціальну, екологічну та економічну сталість. Фінансовий та управлінський облік залишаються основними інструментами для прийняття ефективних рішень, але продовжують адаптуватися до нових реалій. Врахування екологічних та соціальних аспектів стає першочерговим в сьогоденні, хоча практики бухгалтерського обліку та підзвітності потребують часу для повної ефективності в сталому світі.

На сьогодні корпоративні системи розрахунку витрат і надалі не надають повної інформації про екологічні витрати. Наразі не існує жодної системи обліку, що дозволяє повністю включити усі зовнішні та внутрішні екологічні витрати в склад собівартості продукції. Вимірювання таких екологічних витрат, як забруднення повітря, залишається одним зі складних рівнянь без розв'язку. На етапі впровадження систем обліку екологічних витрат господарюючі суб'єкти включають до свого аналізу різноманітні види екологічних витрат. Одним з таких підходів є всеосяжний облік екологічних витрат, який охоплює як поточні, так і очікувані витрати, акцентуючи зовнішні фактори. Важливим є аналіз прогнозованих екологічних витрат, що розраховує майбутні витрати на продукт [3].

Метод всеосяжного екологічного обліку дозволяє інтегрувати екологічні аспекти в процес менеджменту, об'єднуючи внутрішній та зовнішній впливи, пов'язані з діяльністю суб'єкта господарювання на довкілля та ментальне здоров'я. Для ідентифікації зовнішніх впливів господарюючі суб'єкти використовують підходи з використанням функції шкоди для монетизації впливів на довкілля, досліджуючи дані та використовуючи екологічні моделі для перетворення впливів на довкілля у фінансові збитки.