УДК 004.056
DOI https://doi.org/10.32844/2618-1258.2025.5.31

ГАЄВСЬКА В.О.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ: ЗАСТОСУВАННЯ ТЕОРІЇ ЙМОВІРНОСТЕЙ І МАТЕМАТИЧНОЇ СТАТИСТИКИ ДЛЯ ОЦІНКИ ЗАГРОЗ

CYBERSECURITY AND INFORMATION PROTECTION: APPLYING PROBABILITY THEORY AND MATHEMATICAL STATISTICS TO THREAT ASSESSMENT

У статті обґрунтовано, що сучасна кібербезпека як сфера публічного та приватного управління ризиками потребує переходу від описових переліків загроз до доказової, вимірюваної ймовірнісно-статистичної оцінки загроз і наслідків. Наголошено, що загрози кіберпростору мають стохастичну природу: частота інцидентів, їх інтенсивність у часі, імовірність успішної реалізації атаки, затримка виявлення, масштаби втрат та ефективність контрзаходів не є детермінованими величинами, а формують розподіли випадкових змінних. Показано, як інструменти теорії ймовірностей (моделі подій, умовні ймовірності, теорія надійності та виживання) і математичної статистики (оцінювання параметрів, перевірка гіпотез, послідовні критерії, аналіз дисбалансу класів, ROC/PR-метрики, теорія екстремальних значень) можуть бути інтегровані у практику оцінки загроз, узгоджену зі стандартами управління ризиками (NIST, ISO) та вимогами ризик-орієнтованого регулювання (GDPR, NIS2, національне законодавство України). Окрему увагу приділено проблемі хибнопозитивів у детекції та так званій пастці базової частоти, коли навіть високоточні алгоритми можуть генерувати статистично невиправданий обсяг помилкових тривог за низької апріорної частоти реальних атак. Запропоновано концептуально-методологічну основу ймовірнісно-статистичного профілю загрози з довірчими інтервалами як управлінський продукт для кіберзахисту та захисту інформації загалом.

Ключові слова: *кібербезпека, захист інформації, оцінка загроз, теорія ймовірностей, математична статистика, послідовне виявлення, аномалії, ризик-менеджмент, національна безпека.*

The article substantiates that modern cyber security as a field of public and private risk management requires a transition from descriptive lists of threats to an evidence-based, measurable probabilistic-statistical assessment of threats and consequences. It is emphasized that cyberspace threats are stochastic in nature: the frequency of incidents, their intensity over time, the probability of successful implementation of an attack, detection delay, the scale of losses and the effectiveness of countermeasures are not deterministic quantities, but form distributions of random variables.

It is shown how the tools of probability theory (event models, conditional probabilities, reliability and survival theory) and mathematical statistics (parameter estimation, hypothesis testing, sequential criteria, class imbalance analysis, ROC/PR metrics, extreme value theory) can be integrated into the practice of threat assessment, consistent with risk management standards (NIST, ISO) and the requirements of risk-based regulation (GDPR, NIS2, national legislation of Ukraine).

Special attention is paid to the problem of false positives in detection and the so-called base frequency trap, when even highly accurate algorithms can generate a statistically unjustified amount of false alarms at a low a priori frequency of real attacks. The conceptual and methodological basis of the probabilistic-statistical threat profile

© ГАЄВСЬКА В.О. – кандидат математичних наук, доцент, доцент кафедри фізики та математики (Державний біотехнологічний університет) https://orcid.org/0000-0002-1562-8656
Стаття поширюється на умовах ліцензії CC BY 4.0

with confidence intervals is proposed as a management product for cybersecurity and information security in general.

Key words: *cybersecurity, informationsecurity, threatassessment, probabilitytheory, mathematicalstatistics, sequentialdetection, anomalies, riskmanagement, nationalsecurity.*

Постановка проблеми.Кібербезпека в сучасній державі та економіці перестала бути суто технічною дисципліною і стала елементом національної безпеки, критичної інфраструктури, корпоративного управління, захисту прав і свобод людини, а також сфери юридичної відповідальності організацій за недбалість у забезпеченні належного рівня захисту даних та стійкості сервісів. Водночас у практиці й досі домінує парадокс, оскільки попри декларовану «ризик-орієнтованість» стандартів і регулювання, значна частина рішень ухвалюється на підставі якісних суджень, рейтингових шкал, експертних інтуїцій або популярних метрик, які не відображають невизначеність і не дають змоги перевіряти ефективність заходів на конкретних даних. Організація може мати сотні політик, процедур і засобів захисту, але при цьому не мати відповіді на базові питання управління, наприклад, яка реальна інтенсивність інцидентів у нашій екосистемі, як змінюється ризик після впровадження контролю, наскільки ймовірно, що конкретний тип атаки буде успішним саме в нашому контексті, а також що ми знаємо достовірно, а де лише припускаємо.

Цей розрив між нормою належного рівня безпеки та операційною можливістю її обґрунтувати загострюється двома факторами: 1) кіберзагрози є динамічними й адаптивними – супротивник змінює тактики, атаки стають більш автоматизованими та масштабованими, а вразливості з'являються системно через складність ланцюгів постачання, хмарну трансформацію, інтеграцію API та людський фактор; 2) дані про інциденти мають фундаментальні обмеження – не все виявляється, не все класифікується однаково, не всі втрати спостережувані, а телеметрія є похідною від налаштувань систем моніторингу. У підсумку кіберризик за своєю природою є стохастичним, а не детермінованим об'єктом, і будь-яке управління ним без інструментів теорії ймовірностей та статистики перетворюється на управління видимістю безпеки, а не її реальним рівнем. Саме тому в центрі сучасної методології кіберзахисту має стояти формалізація загрози як випадкового процесу і побудова оцінок, які не приховують невизначеність, а роблять її керованою.

Мета статті полягає у системному аналізі та викладенні підходу до оцінки загроз кібербезпеки та захисту інформації на основі теорії ймовірностей і математичної статистики.

Стан дослідження. Проблематика застосування теорії ймовірностей і математичної статистики для оцінки загроз кібербезпеки та захисту інформації тією чи іншою мірою була предметом дослідження невеликої кількості вчених, серед яких, перш за все, доцільно назвати наступних: В. Л. Бурячок, Н. В. Галайко, С. О. Гнатюк, Л. Ф. Дзюба, О. Г. Корченко, О. І. Огірко, В.Б. Толубко, С.В. Толюпа, В. П. Харченко, В. О. Хорошко, О. Ю. Чмир та інші. Попри наявність наведеного кола науковців і відповідного масиву праць, у сучасній доктрині та прикладній літературі досі відсутнє комплексне, цілісне й методологічно узгоджене дослідження, яке б системно поєднувало теорію ймовірностей і математичну статистику з практикою оцінювання кіберзагроз і наслідків із формалізацією невизначеності, інтервальними оцінками та процедурою валідації у єдиній моделі, придатній одночасно для операційного кіберзахисту, ризик-менеджменту та правового обґрунтування достатності заходів захисту інформації.

Виклад основного матеріалу.Теорія ймовірностей дає мову для опису подій і умовності для моделювання потоків інцидентів, переходів у сценаріях атак, а також для байєсівського перегляду переконань у міру надходження нових даних [1, с. 9–20]. Математична статистика, у свою чергу, надає інструменти, щоб із реальних, часто неповних, даних отримувати параметри моделей, оцінювати похибки, контролювати помилки рішень, перевіряти гіпотези про ефективність контролів і будувати обґрунтовані висновки щодо зміни ризику в часі [1, с. 115–132]. У сфері кібердетекції це проявляється у формальному виборі порогів та метрик, здатних працювати за дисбалансу класів. У ризик-менеджменті – у переході від одного числа до розподілу втрат і подальших характеристик. У комплаєнсі – в можливості пояснювати, чому обрані заходи є пропорційними, достатніми і заснованими на доказах.

Сучасна правова та організаційна структура кібербезпеки дедалі жорсткіше прив'язує вимоги до захисту інформації до оцінки ризиків і загроз, а не до формального переліку обов'язкових заходів. У праві ЄС цей зсув чітко проявляється в ризик-орієнтованих приписах щодо належного рівня безпеки та необхідності врахування ризиків для прав і свобод (зокрема, у GDPR), а також у комплексних вимогах до управління кіберризиками та звітування про інциденти (NIS2) [2]. Для України подібна логіка закладена у визначенні правових та організаційних основ забезпечення

кібербезпеки, спрямованих на захист життєво важливих інтересів у кіберпросторі, та у стратегічних документах держави, які відображають пріоритетність системності, координації і керованості кіберзахисту [3]. Паралельно діє спеціальне законодавство про захист інформації в інформаційно-комунікаційних системах, яке вимагає організаційно-технічних заходів, але практично завжди ставить питання на кшталт який рівень захисту є достатнім у конкретних умовах загроз і вразливостей [4]. Саме тут проявляється методологічний розрив між юридичною нормою, яка апелює до належного рівня безпеки та управлінською реальністю, де цей рівень необхідно обґрунтовувати: чому один контрзахід пріоритетніший за інший; чому певний клас інцидентів критичніший; як змінюється ризик після впровадження контролю; наскільки достовірними є оцінки. Відповіддю може бути лише кількісна модель загроз, яка перетворює загрозу з риторичного терміна на вимірюваний об'єкт із імовірністю реалізації, розподілом наслідків і метрикою довіри до оцінки. Такий підхід узгоджується зі стандартами управління ризиками: NIST прямо визначає оцінювання ризиків як структурований процес аналізу загроз, вразливостей, схильних умов і наслідків, орієнтований на підтримку управлінських рішень [5, p. 1–4].

Загроза у кібербезпеці як об'єкт оцінювання завжди має мінімум три складові – частоту (як часто відбуваються події певного класу), ймовірність успіху за умов наявних вразливостей чи контролів та тяжкість наслідків у разі успішної реалізації. У спрощених моделях ризик подають як добуток «ймовірності × шкоди», однак для кіберпростору такий детермінізм методологічно небезпечний: і «ймовірність», і «шкода» є розподілами, причому часто з «важкими хвостами» (rare-but-catastrophic), а доступні дані – неповні, зашумлені та зміщені (бо не всі інциденти виявляються і не всі втрати вимірюються). Саме тому NIST у керівництві з оцінювання ризиків акцентує, що оцінка – це процес формування судження з урахуванням невизначеності, а не одноразове присвоєння числа.

Почнемо з імовірнісного опису частоти інцидентів. Нехай $N(t)$ – кількість інцидентів певного типу за період довжини t. У найпростішій моделі $N(t)$ розглядають як пуассонівський процес з інтенсивністю λ: $N(t) \sim Poisson(\lambda t)$. Ця модель описує статистику подій у системі спостереження (SOC/SIEM) і дає змогу оцінити очікувану кількість інцидентів, довірчі інтервали для λ, а також статистично відстежувати зміни інтенсивності (сплески сканувань, фішингових кампаній, атак на доступність). Якщо події не є незалежними або інтенсивність змінюється, застосовують нестаціонарні або самозбуджувальні процеси, але навіть базова пуассонівська модель створює формальний «нульовий рівень» (baseline), від якого відштовхуються статистичні критерії змін. У кібербезпеці практична цінність такого підходу полягає в тому, що аномальність інцидентного потоку можна визначати як статистично значуще відхилення від очікуваного рівня з контрольованим рівнем хибних тривог. У методологічному сенсі це є реалізацією ідеї Деннінг про виявлення вторгнень як аналіз відхилень поведінки системи [6, с. 39-46].

Окремо постає питання ймовірності успіху атаки за наявності вразливостей і контролів. Тут природною є логіка умовних імовірностей: $P(S|V,C,E)$, де S – подія успіху атаки, V – вектор вразливостей, C – набір контролів, E – середовищні умови (експозиція сервісів, зрілість процесів, поведінка користувачів тощо). На практиці V часто кодують через метрики вразливостей, і найпоширенішим стандартом комунікації «технічної тяжкості» є CVSS, який формує бали на основі експлуатованості та впливу. Важливо підкреслити принципову тезу FIRST та NVD: CVSS – це міра severity, а не прямий вимір ризику; він не замінює імовірнісної оцінки загрози, а є одним із предикторів чи факторів [7]. Відповідно, коректний науково-практичний підхід полягає в тому, щоб розглядати CVSS як частину моделі умовної ймовірності успіху та/або умовного розподілу збитків.

Третя складова – розподіл наслідків (втрат). Економічно та управлінськи суттєво не лише очікуване значення, а і хвостові характеристики: квантилі (VaR), умовні хвости (CVaR/ ExpectedShortfall), імовірність перевищення порогів. Загальна модель річних (або квартальних) втрат часто має вигляд складеної суми: $L=\sum_{i=1}^{N} X_i$, де N – кількість інцидентів за період, X_i – випадкова величина втрат від і-го інциденту. У термінах кількісного ризик-менеджменту така постановка безпосередньо сумісна з логікою FAIR, де ризик розкладається на частоту подій загрози та ймовірну величину втрат; сучасні матеріали FAIR-спільноти прямо описують інтеграцію кількісної оцінки з ISO-орієнтованими процесами ризик-менеджменту [8, с. 2–5]. Звідси випливає ключовий методологічний наслідок: коректним результатом оцінки загроз є не одне число ризику, а розподіл L (або принаймні його параметри та інтервали невизначеності), який потім використовується для оптимізації контролів і обґрунтування належної обачності.

Однак будь-яка модель у кібербезпеці стикається з проблемою неповноти спостереження: ми не бачимо «всіх атак», ми бачимо телеметрію та алерти. Тому критичною стає байєсівська

постановка, яка дозволяє поєднувати апріорні знання (threatintelligence, галузеві ландшафти, історичні дані) з новими спостереженнями. В найпростішому випадку інтенсивність λ для пуассонівського потоку може мати гамма-розподіл як апріорі: λ~Gamma(α,β); після спостереження N(t)=k posterior залишається гамма-розподілом із оновленими параметрами. Практичний сенс: SOC отримує не лише «оцінку λ^», а й кредитивний інтервал (наприклад, 95%) для частоти інцидентів – що прямо підтримує управлінську відповідальність: рішення базуються на інтервалі невизначеності, а не на ілюзії точності.

Щоб пов'язати «мову атак» із «мовою ймовірностей», доцільно використати таксономії тактик і технік. MITRE ATT&CK описує тактики й техніки супротивника у вигляді матриці, що може слугувати системою координат для агрегації даних: ми не просто рахуємо інциденти «взагалі», а оцінюємо частоти ймовірнісних подій для класів технік (наприклад, за сегментами інфраструктури) [9].

У такій постановці моделі типу марковських ланцюгів природно описують переходи між станами «ланцюга атаки» (наприклад, від первинного доступу до закріплення і руху всередині мережі): P(Xt+1=j|Xt=i). На відміну від простого чекліста, марковська модель дає змогу оцінювати, які переходи статистично найімовірніші у конкретній організації та де контрзаходи максимізують зменшення ймовірності досягнення критичних станів (екфільтрація, шифрування, зупинка сервісів). Це створює місток між технічними патернами та економіко-правовим питанням пріоритезації контролів: пріоритет отримує той, що статистично найбільше знижує ймовірність критичного сценарію або хвостовий ризик втрат.

У реальному часі значна частина кіберзагроз проявляється не «однією подією», а зміною статистичних властивостей потоків даних і поведінкових показників: зростанням частоти невдалих входів, зсувом профілю мережевих потоків, нетиповими обсягами звернень до файлів чи доменних запитів тощо. Тому оцінка загроз природно формулюється як виявлення змін (changepointdetection) та статистичне виявлення аномалій: будується модель нормального режиму, а відхилення трактується як подія з контрольованою ймовірністю хибної тривоги, що забезпечує не лише раннє попередження, а й формалізовану відповідь «чому це підозріло» (важливо для аудиту, розслідувань і комплаєнсу). Водночас практична пастка кібердетекції полягає в дисбалансі класів (атаки рідкісні, нормальні події масові), через що «висока точність» може вводити в оману; отже, ключовими стають статистично коректні процедури налаштування порогів і оцінювання якості (зокрема підходи, чутливі до рідкісних подій), аби мінімізувати шум і не перетворити захист на фабрику хибних спрацювань [10].

Окрема, принципово важлива роль математичної статистики – доказове оцінювання ефективності контрзаходів (EDR, MFA, сегментація, резервне копіювання, DLP тощо) та причинно-наслідковий аналіз: чи справді після впровадження контролю зменшились імовірність успішної атаки, інтенсивність інцидентів або «хвіст» часу виявлення/реагування. Статистично це вирішується через порівняння розподілів «до/після» та квазіекспериментальні схеми (перервані часові ряди, невизначеності, моделі виживання для показників time-to-detect/time-to-respond із цензуруванням), що дозволяє замінити «віру в контроль» на вимірювану зміну параметрів ризику з інтервалами невизначеності. Юридично це перетворює кіберзахист на підкріплену даними конструкцію належної обачності: організація може обґрунтовувати пропорційність і адекватність заходів не декларативно, а через відтворювані статистичні докази їх результативності в конкретному середовищі загроз.

Таким чином, для задач оцінювання загроз кібербезпеки та захисту інформації обґрунтовано і системно сформульовано інтегрований «ймовірнісно-статистичний профіль загрози» (ЙСПЗ) як результат оцінки, який: 1) задає загрозу трійкою стохастичних компонентів (частота подій, умовна ймовірність успіху, розподіл наслідків) з явною невизначеністю (довірчими/кредитивними інтервалами); 2) поєднує байєсівське оновлення параметрів ризику на основі телеметрії SOC/SIEM із галузевими таксономіями загроз (MITRE ATT&CK) для сценарного агрегування та пріоритезації контролів; 3) вводить статистично процедуру калібрування детекторів загроз, що враховує «пастку базової частоти» (base-ratefallacy) та використовує ROC/PR-метрики для вибору порогів з контрольованими помилками першого/другого роду; 4) обґрунтовує застосування теорії екстремальних значень для хвостового аналізу кіберінцидентів як підстави для економічного та правового обґрунтування резервів і пропорційності заходів; 5) забезпечує методологічну сумісність із міжнародними стандартами оцінки та управління ризиками (NIST SP 800-30, ISO 31000/27005) і ризик-орієнтованим регулюванням (GDPR, NIS2), що дозволяє використовувати результати оцінки як доказову базу належної обачності.

У підсумку, запропонований нами підхід дозволяє по-новому відповісти на класичні питання кіберзахисту щодо того, які загрози для нас найкритичніші, що зміниться після впровадження контролю, наскільки ми впевнені в оцінці і де межа достатності заходів. Перевага теорії ймовірностей полягає у формалізації невизначеності й умовності, а перевага математичної статистики – у можливості оцінювати параметри за даними, перевіряти гіпотези та контролювати помилки. Саме в синергії цих двох дисциплін кібербезпека набуває статусу зрілої, інженерної та юридично обґрунтованої практики.

Висновки. Отже, наведена логіка кількісної оцінки загроз доводить, що ефективна кібербезпека є насамперед дисципліною керування невизначеністю. Організація не може знати напевно, коли саме й у який спосіб відбудеться атака, але може системно оцінювати ймовірності, інтенсивності, сценарні переходи та розподіли втрат, перетворюючи невизначеність на вимірюваний фактор управління. Вирішальним є відхід до інтервальних оцінок і розподілів, оскільки саме вони відображають реальний стан даних у кіберпросторі та дозволяють ухвалювати рішення з контролем ризику помилки. Практично значущим результатом стає перетворення детекції на статистичний процес, за якого алерт не трактують як факт інциденту, а інтерпретують через імовірність із урахуванням базової частоти, що підвищує точність пріоритезації реагування. Водночас, стратегічне управління кіберризиком набуває економічної і юридичної зрілості тоді, коли наслідки моделюються як розподіли з урахуванням всіх ризиків, адже саме рідкісні, але масштабні події визначають потреби в резервуванні, відмовостійкості та пропорційності інвестицій у захист.

Концепція ймовірнісно-статистичного профілю загрози створює узгоджений формат, у якому технічні дані SOC, сценарні таксономії загроз і ризик-орієнтовані вимоги стандартів зводяться до єдиного управлінського продукту, де організація отримує структуровану картину загроз із пояснюваною невизначеністю та можливістю порівняння альтернативних контролів за їхнім реальним ефектом на критичні сценарії та втрати. У цьому полягає ключова прикладна користь: пріоритезація захисту перестає бути реактивною під впливом гучних інцидентів або модних показників і стає оптимізаційною – з орієнтацією на найбільше зниження ймовірності досягнення критичних станів і на мінімізацію втрат. Таким чином, синергія теорії ймовірностей і математичної статистики переводить кібербезпеку з площини декларативних вимог і суб'єктивних оцінок у площину відтворюваних, прозорих і юридично релевантних процедур оцінювання загроз, що є необхідною умовою стійкості цифрових систем у сучасному середовищі ризиків.

Список використаних джерел:

1. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика : навч. посіб. Львів : ЛьвДУВС, 2017. 292 с.

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *EUR-Lex.europa.eu.* URL https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата звернення: 20.06.2024).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

4. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

5. Ross R. Guide for Conducting Risk Assessments : NIST Special Publication 800-30 Rev. 1. Gaithersburg, MD : National Institute of Standards and Technology, 2012. 95 p. DOI: 10.6028/NIST.SP.800-30r1.URL:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.(дата звернення: 13.02.2024).

6. Chandola V., Banerjee A., Kumar V. Anomaly detection: a survey. *ACM Computing Surveys.* 2009. Vol. 41, Issue 3. Article No. 15. P. 1–58. DOI: 10.1145/1541880.1541882. URL: https://www.researchgate.net/publication/220565847_Anomaly_Detection_A_Survey(дата звернення: 13.04.2024).

7. FIRST.Org, Inc. Common Vulnerability Scoring System version 3.1: Specification Document. Revision 1. 2019. 24 с. URL: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (дата звернення: 16.05.2024).

8. Goyal P., Sanna N., Tucker T. A FAIR Framework for Effective Cyber Risk Management: Leveragingthe FAIR Model, FAIR-CAM, and FAIR-MAM to Align Cybersecurity Efforts with Business Priorities and Regulatory Compliance. FAIR Institute, 2025. URL: https://1616664.fs1.hubspotusercontent-na1.net/hubfs/1616664/FAIR%20Institute%20--%20Integrating%20FAIR%20

Models%20for%20Cyber%20Risk%20Management%20%28December%202024%29.pdf (дата звернення : 16.02.2025).

9. The MITRE Corporation. Enterprise Matrix. *MITRE ATT&CK®*. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення : 19.01.2025).

10. Basseville M., Nikiforov I. V. Detection of Abrupt Changes: Theory and Application. Prentice Hall, 1993. 527 p. URL: https://www.researchgate.net/publication/2406812_Detection_of_Abrupt_Change_Theory_and_Application (дата звернення : 01.03.2025).

Дата першого надходження рукопису до видання: 21.08.2025
Дата прийнятого до друку рукопису після рецензування: 10.09.2025
Дата публікації: 25.09.2025