Інформаційний аспект боротьби з логістикою набуває надзвичайно важливого значення. Дезінформацій ні кампанії, спрямовані на зрив логістичних ланцюгів, можуть виявитися не менш ефективними, ніж безпосередні фізичні атаки. Створення штучного інформаційного шуму, провокування внутрішніх конфліктів у логістичних підрозділах та маніпуляція даними систем управління – все це стає потужним інструментом стратегічного впливу.

Економічний напрямок боротьби з логістикою супротивника включає механізми санкцій, цілеспрямоване блокування постачання критично важливих ресурсів, а також маніпуляції на ринках енергоносіїв і сировини. Сучасні геополітичні конфлікти показують, що логістичне удушення може бути так само ефективним, як і традиційні військові дії. Руйнування економічних зв'язків, порушення транспортних коридорів і блокування фінансових потоків формують комплексну стратегію виснаження супротивника.

Військові методи впливу на логістику охоплюють різноманітні операції – від цілеспрямованих диверсій на критично важливих об'єктах інфраструктури до масштабних повітряних і ракетних атак на склади, транспортні вузли та комунікаційні мережі. Сучасні високоточні озброєння дозволяють максимально точно уражати логістичні цілі, зменшуючи при цьому побічні руйнування та супутні втрати.

Системний та інтегрований підхід до порушення логістики супротивника є принципово важливим. Найбільш ефективними виявляються комплексні операції, які об'єднують технологічні, інформаційні, економічні та військові інструменти впливу. Синергетичний ефект від такої взаємодії може призвести до повної деградації логістичної системи противника.

Одночасно боротьба з логістичними викликами вимагає безперервного технологічного оновлення та швидкої адаптації до змін у системах постачання і комунікації. Штучний інтелект, машинне навчання та аналітика великих даних стають невід'ємною частиною сучасних логістичних стратегій протидії.

Отже боротьба з логістикою супротивника стає окремим напрямком у забезпеченні національної безпеки. Комплексний та інтегрований підхід, що об'єднує технологічні, інформаційні, економічні та військові засоби впливу, дозволяє ефективно знижувати бойовий потенціал противника, порушуючи його здатність до стабільного функціонування та розвитку.

Рибачок Геннадій,
полковник,
адюнкт кафедри кіберборотьби
Інституту інформаційно-комунікаційних
технологій та кібероборони,
Національний університет оборони України

МЕТОДИЧНІ ОСНОВИ ВИБОРУ ПОКАЗНИКІВ І КРИТЕРІЇВ ДЛЯ ОЦІНЮВАННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ОРГАНАМИ ВІЙСЬКОВОГО УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність проблеми

Останні роки показали зростання кіберзагроз для військових структур України. Кібератаки на підрозділи ЗСУ у 2022–2023 рр. довели: навіть сучасні системи вразливі без гнучкої методики реагування. Нові типи атак — багатовекторні впливи, фішингові кампанії, спроби порушити зв'язок — засвідчили: відсутність критеріїв і системи показників веде до затримок у виявленні інцидентів, підвищує ризики й може впливати на боєздатність.

Коли атаки залишалися непоміченими через відсутність оцінки критичності, ставало очевидно: старих підходів недостатньо, потрібна методика, адаптована під військові потреби. Досвід командувань підтвердив — лише системний підхід дозволяє вчасно виявляти загрози, розставляти пріоритети й підвищувати стійкість інфраструктури.

Мета цієї роботи — сформулювати науково обґрунтовані методичні основи вибору показників та критеріїв для оцінки і реагування на кіберінциденти у військовому управлінні. Для досягнення цієї мети поставлені такі завдання:

– Проаналізувати сучасний міжнародний досвід (стандарти, рекомендації, кращі практики);

– Визначити класифікацію та систему показників, які доцільно застосовувати у ЗСУ;

– Описати принципи і алгоритм інтеграції цих критеріїв у діючу систему прийняття рішень;

Провідними світовими стандартами для реагування на кіберінциденти залишаються ISO/IEC 27035, NIST SP 800-61, рекомендації ENISA, а також практики, що застосовуються у ЗС НАТО. Згідно з ISO/IEC 27035, процес управління кіберінцидентами охоплює підготовку, ідентифікацію, реагування, відновлення та аналіз ефективності дій. Відповідно до NIST SP 800-61, особлива увага приділяється визначенню чітких метрик для оцінювання ефективності реагування, що дозволяє гнучко налаштовувати систему під конкретні потреби організації.

Міжнародний досвід показує: ключовими є поділ показників на кількісні (кількість інцидентів, середній час виявлення та реагування, відсоток вчасно ліквідованих загроз) та якісні (оцінка критичності впливу, готовність персоналу, захищеність інфраструктури). Автоматизація збору даних, впровадження SIEM-систем, регулярні тренування й навчання персоналу — обов'язкові елементи сучасних методик. Однак українська специфіка (швидка зміна обстановки, обмеження у ресурсах, гібридний характер загроз) вимагає адаптації підходів — механічне впровадження західних стандартів нерідко призводить до формалізації, яка не працює у реальних бойових умовах.

Запропоновано використовувати кількісні показники й якісні показники. Відмінність методики — інтеграція експертної оцінки: навіть якщо кількісні метрики не сигналізують про загрозу, персонал може запобігти критичним втратам.

На практиці це реалізується так:

– Постійний моніторинг і автоматизований збір даних через SIEM, аналіз журналів подій;

– Регулярна оцінка готовності персоналу (тестування, тренінги, симуляції);

– Введення експертної ради або чергової групи, що здійснює якісний аналіз отриманої інформації;

– Відстеження змін структури інцидентів і впровадження коригуючих заходів.

Алгоритм інтеграції критеріїв до системи прийняття рішень передбачає поетапний підхід:

1. Виявлення інциденту (автоматичний чи ручний збір інформації);
2. Класифікація й оцінка критичності (поєднання кількісних даних з експертною оцінкою);
3. Пріоритезація інцидентів та визначення порядку реагування;
4. Призначення відповідальних, запуск стандартних процедур реагування;
5. Локалізація й усунення наслідків, фіксація показників ефективності (KPI);
6. Постінцидентний аналіз і зворотний зв’язок — коригування алгоритмів, оновлення бази знань.

Особливо важливо забезпечити гнучкість підходу: у складних випадках командири мають змогу переглядати пріоритети у реальному часі, ґрунтуючись не лише на формальних показниках, а й на аналізі змін бойової обстановки. Також практика довела, що поєднання автоматичних засобів із людським фактором дає змогу уникати типових помилок й запобігати пропуску критичних подій.

Висновки

Запропонований у цій роботі підхід дозволяє не лише підвищити ефективність виявлення та ліквідації кіберінцидентів у Збройних Силах України, а й забезпечити стійкість інформаційних систем до нових, раніше невідомих загроз. Практика показала: саме поєднання формалізованих метрик, експертної оцінки та постійної роботи над помилками дає максимальний результат у підвищенні кіберстійкості та відповідності вимогам сучасних стандартів НАТО. Безперервний аналіз і гнучкість критеріїв є ключем до реального підвищення рівня кіберзахисту у військових структурах.

Сахневич Борис,
кандидат економічних наук,
Київський інститут Національної гвардії України

ТЕНДЕНЦІЇ СУЧАСНОГО РОЗВИТКУ ВІЙСЬКОВОЇ ЛОГІСТИКИ ТА ЛАНЦЮГІВ ПОСТАЧАННЯ

Ланцюги постачання розвиваються там, де є попит. Військова логістика визначає розміщення, переміщення, масштаби й обсяг дій військових сил. Ланцюги постачання — це постійний прояв військової потуги. Вони визначають, наскільки далеко можуть просунутись сили оборони, як організовано вони функціонують, і формують обмеження та можливості для командування.

Військова логістика сьогодення