УДК 351.865

О. Л. Назаренко, С. О. Годлевський, І. В. Скакалін

ОРГАНІЗАЦІЯ КОМПЛЕКСУ ЗАХОДІВ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДРОЗДІЛАМИ СИЛ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Розглянуто ключові підходи до маскування й обладнання інженерними та інженерно-технічними засобами важливих державних об'єктів та об'єктів критичної інфраструктури в умовах воєнного стану з огляду на досвід їх застосування підрозділами Сил безпеки і оборони України для забезпечення державної безпеки. Особливу увагу приділено принципам інтеграції природних і штучних елементів маскування з інженерно-технічними засобами охорони, а також організації охорони з урахуванням ведення противником розвідки різними способами і засобами для виявлення місць розташування важливих державних об'єктів та об'єктів критичної інфраструктури. У межах дослідження висвітлено проблематику взаємодії між різними складниками Сил безпеки і оборони України у процесі здійснення захисту важливих державних об'єктів та об'єктів критичної інфраструктури.

Ключові слова: *маскування, інженерні засоби, інженерно-технічні засоби, об'єкти критичної інфраструктури, важливі державні об'єкти, система забезпечення безпеки.*

Постановка проблеми. У сучасних умовах противником широко застосовується низка видів розвідки з метою виявлення важливих державних об'єктів (ВДО) та об'єктів критичної інфраструктури (ОКІ), а також визначення способів для їх ураження. Види розвідки тісно взаємопов'язані і взаємно доповнюють один одного, забезпечуючи комплексну картину для ухвалення рішень у різних сферах діяльності.

Наявна система забезпечення безпеки ВДО та ОКІ нерідко демонструє фрагментарність, недостатню координацію дій, відсутність єдиних стандартів планування та реагування на загрози. Це знижує загальну ефективність запобігання, виявлення та нейтралізації загроз на ранніх етапах їх реалізації. Отже, виникає потреба у формуванні і запровадженні цілісного комплексу заходів, спрямованих на забезпечення сталого функціонування ВДО та ОКІ, насамперед це застосування сучасних інженерних та ІТЗО, фізичного захисту, маскування, а також координація дій між підрозділами Сил безпеки і оборони України.

У зв'язку із цим особливого значення набуває вдосконалення комплексу заходів системи забезпечення безпеки об'єкта щодо організації фізичного, інженерного, інженерно-технічного та спеціального захисту. Комплекс цих заходів має забезпечувати виконання завдань із запобігання несанкціонованому проникненню, терактам, витоку конфіденційної інформації, а також гарантувати технічну надійність обладнання об'єкту та професійну підготовку персоналу. Однак ефективність цієї системи залежить від рівня узгодженості й інтеграції всіх складових елементів у єдину систему безпеки.

Для ефективного функціонування системи забезпечення безпеки ВДО та ОКІ необхідно комплексно використовувати інженерно-технічні засоби охорони (ІТЗО) з інженерними заходами посилення безпеки об'єктів, а також проведення додаткових заходів з підтримки маскувальної дисципліни. До таких засобів належать системи відеоспостереження і контролю доступу, різноманітні системи охоронної сигналізації, спостережні пости (позиції), укриття для особового складу, обладнання загороджень та маскування. Важливо розуміти, що їхня ефективність досягається лише у разі взаємодії всіх елементів системи як єдиного комплексу. Ігнорування окремих компонентів, зокрема маскувальних, або навпаки, зниження рівня інженерного обладнання під приводом підвищення прихованості призводить до послаблення загальної захищеності об'єкта. Тому технічне оснащення і матеріальне забезпечення заходів охорони мають базуватися на системному підході, який ураховує як вимоги щодо фізичної безпеки, так і необхідність мінімізації демаскуючих ознак в умовах сучасної гібридної війни.

Забезпечення безпеки ВДО та ОКІ потребує комплексного підходу і скоординованої взаємодії між усіма складниками сектору безпеки і оборони України.

Отже, є потреба у вдосконаленні підходів до вибору локації, маскування, інженерного обладнання ІТЗО, адаптованих до реалій сьогодення, з використанням досвіду, набутого під час російсько-

української війни, що триває. Такі підходи забезпечать вибір низки доцільних складників системи забезпечення безпеки ВДО та ОКІ з урахуванням їх особливостей.

Аналіз останніх досліджень і публікацій. Проведено огляд наукових публікацій стосовно організації комплексу заходів системи забезпечення безпеки важливих державних об'єктів та об'єктів критичної інфраструктури, зокрема в Україні. Авторами праці [1] доведено, що основними причинами, які негативно впливають на надійність цивільного захисту ОКІ, є такі: неповнота вихідних даних для розроблення технічного рішення; не у повному обсязі обґрунтування описів технічного рішення і в окремих випадках – невідповідність нормативних документів умовам будівництва ОКІ, зокрема умовам особливого періоду. У статті [2] здійснено наукову розвідку стосовно причин, які негативно впливають на надійність захисту ОКІ в умовах воєнного стану і прямого впливу бойових дій, а також недоліків, які виникають під час розроблення документації щодо інженерно-технічних засобів із захисту ОКІ. У науковій праці [3] висвітлено питання розподілу елементів ОКІ енергетичної галузі з інженерного захисту за пріоритетністю, запропоновано три типи інженерного захисту цих об'єктів та розглянуто організаційні й технічні аспекти побудови системи забезпечення безпеки об'єктів. Автор статті [4] запропонував методологічні підходи до визначення пріоритетності захисту ОКІ та напрямів подальшої розбудови в Україні системи захисту ОКІ. У статті [5] визначено рівень кібербезпеки підрозділу Міністерства оборони України, на основі отриманих результатів сформовано практичні рекомендації щодо забезпечення кібернетичної безпеки до необхідного рівня, а також запропоновано методику оцінювання захищеності кіберпростору ОКІ.

У зазначених публікаціях висвітлено низку недоліків в обґрунтуванні технічних рішень будівництва ОКІ відповідно до умов воєнного стану, у розробленні документації ІТЗО та їх пріоритетності; указано напрями подальшої розбудови ОКІ та розроблено рекомендації щодо забезпечення кібернетичної безпеки. Однак у чинних керівних документах і розглянутих працях [1–5] бракує уваги до питань організації та здійснення комплексу заходів для забезпечення безпеки ВДО та ОКІ частинами і підрозділами Сил безпеки і оборони України.

Метою статті є аналіз сучасних підходів до організації повного комплексу заходів для забезпечення безпеки об'єктів критичної інфраструктури, зокрема з питань інженерного обладнання, використання інженерно-технічних засобів охорони та маскування об'єктів критичної інфраструктури в Україні, з огляду на досвід виконання аналогічних завдань підрозділами Сил безпеки і оборони України, а також окреслення напрямів удосконалення системи забезпечення безпеки об'єкта із застосуванням новітніх технологій і засобів.

Виклад основного матеріалу. Проблема маскування об'єктів виходить за межі лише мінімізації демаскуючих ознак заборонених зон, тому вирішення її не є тільки прерогативою підрозділів Сил безпеки і оборони України. Ця проблема охоплює широке коло питань, як-то: захист від можливих загроз противника, отримання противником достовірних даних про належність об'єкта, його призначення та характер діяльності, мінімізація демаскуючих ознак його виробничого циклу в системі охорони. Усе це у кінцевому підсумку спрямовано на зберігання статусу об'єкта як такого, що не є пріоритетним для органів іноземної розвідки. Завдання маскування об'єктів вирішуються компетентними органами Сил безпеки і оборони України.

Метою маскування ВДО та ОКІ є введення в оману ймовірного противника стосовно місця розташування об'єктів з повним їх приховуванням або з приховуванням їх характеристики та діяльності. Повне приховування об'єкта означає позбавлення можливості розвідки противника виявляти його локацію, розташування та призначення. При цьому необхідно враховувати низку демаскуючих ознак, так само, як і можливість використання багатьох видів розвідувальних засобів противника, зокрема: оптичні, радіолокаційні, радіо- та радіотехнічні, пірометричні, інфрачервоні, акустичні, радіаційні та ін. Необхідно також враховувати можливості агентурної розвідки противника.

Саме тому пропонується доволі сумнівний підхід до рішення щодо маскування діючих об'єктів шляхом видалення (ліквідації) заборонених зон або щонайменше – основних їх елементів. З огляду на те, що багато з таких об'єктів уже зафіксовані розвідувальними органами противника, вони, скоріше, потребують посилення наявних заборонених зон новітніми, надійнішими технічними засобами охорони. Водночас треба вдосконалювати тактику дій Сил безпеки і оборони України щодо охорони та оборони важливих об'єктів.

Висновок стосовно того, що об'єкти, які приймаються під охорону, потребують маскування заборонених зон, уявляється спірним, якщо цю проблему розглядати з позиції маскування об'єкта в цілому [6, 7]. Якщо за характерними ознаками тих чи інших споруд об'єкта, що приймається під охорону, практично повністю розкривається характер його діяльності, то не доцільно вже під час

розроблення проєкту цього об'єкта знижувати надійність його охорони шляхом відмови від будівництва сучасного комплексу ІТЗО в його забороненій зоні.

Наприклад, окремі об'єкти визначаються характером споруд: випробувальні стенди, трубопроводи, блискавковідводи, залізничні комунікації, обвалування, лінії електромереж, великі трансформаторні підстанції, водосховища та ін. Тому на таких об'єктах наявність заборонених зон, а також обладнання комплексом ІТЗО небагато додає для розкриття їх призначення, характеру та виробництва. Крім зазначеного вище, є низка об'єктів, з руйнуванням яких буде завдано шкоди економіці країни або є ризик створення зони радіоактивного забруднення (АЕС). Один із імовірних варіантів завдання пошкоджень противником – це використання спеціальних підрозділів, тому необхідно заздалегідь вжити заходів щодо своєчасного виявлення і знешкодження диверсійних груп, що насамперед пов'язано з посиленням заборонених зон інженерними загородженнями та технічними засобами виявлення, зокрема й на шкоду маскуванню.

Окремі елементи інженерних та ІТЗО [8, 9] заборонених зон (контрольно-слідова смуга, охоронне освітлення, дороги, якими переміщуються сили і засоби охорони, інженерні загородження і перешкоди, лінії сигнальних систем та засоби виявлення тощо), військовослужбовці, що несуть службу в формі Сил безпеки і оборони України, також є демаскуючими ознаками. Однак не завжди доцільно з метою маскування об'єкта, що охороняється, не лише повністю відмовитися від них, але навіть зменшувати їхню кількість та склад. Відмова від деяких елементів ІТЗО знижує надійність охорони об'єкта, при цьому орієнтування на примітивне обладнання заборонених зон у разі збереження демаскуючих ознак об'єкта й особового складу не підвищить маскування об'єкта [10].

Інженерно-технічні засоби охорони створені цілеспрямованою працею спеціалізованих підприємств і державних установ, які відповідають за безпеку об'єктів протягом останніх років з урахуванням практичного досвіду, є важливим складником надійності охорони об'єктів. Застосовувані ІТЗО забезпечують [8]: складність візуального спостереження за специфікою робіт, спорудами тощо на території об'єктів; своєчасне сповіщення охорони про подолання лінії охорони і визначення напрямку дій порушника; сковування дій порушників під час подолання заборонених зон і просування їх у напрямку об'єктів (режимних приміщень), що охороняються; упізнання порушників і визначення замислу їхніх дій; створення умов для успішних тактичних дій Сил безпеки і оборони України.

Для зменшення демаскуючих чинників ІТЗО у забороненій зоні як важливого складника системи забезпечення безпеки об'єкта строго диференційовано, не шаблонно потрібно враховувати низку факторів, зокрема: надійність охорони об'єкта [11]; призначення об'єкта і можливі загрози його безпеці; вимоги до захисту і забезпечення безпеки об'єкта залежно від типу можливих загроз та ризиків [12]; наявність у об'єкта демаскуючих ознак; вартість комплексу ІТЗО й утримання охорони в цілому; запропоновані підходи до проблеми маскування об'єктів [13].

За статусом об'єкта у статті запропоновано таку класифікацію об'єктів: 1) з обмеженням допуску; 2) з посиленим контролем; 3) з комплексною охороною.

1. Об'єкт, який охороняється (приймається під охорону), не має інших демаскуючих ознак, що розкривають його призначення, крім тих, які властиві системі його охорони (з обмеженням допуску). У цьому випадку необхідно відмовитися від організації охорони об'єкта з використанням забороненої зони, обладнавши його лише основним загородженням; у режимних приміщеннях об'єкта службу з охорони підтримувати підрозділами у цивільному одязі. Охорону об'єкта здійснювати таким чином: режимні будівлі, цехи, приміщення обладнати двома-трьома рубежами ІТЗО, засобами відеоспостереження та інженерними засобами; охороняти чатовими на контрольно-пропускних пунктах (КПП) без здійснення ними патрулювання та інших дій, які можуть призвести до демаскування об'єктів, а у неробочий час – способом оперативного чергування; спостереження за територією здійснювати потай силами залучених до охорони і оборони об'єкта підрозділів та підрозділом режиму об'єкта.

2. На тлі інших демаскуючих ознак, які розкривають характер об'єкта, ознаки, характерні для системи охорони об'єкта по периметру, значно переважають, тобто вимагається їх зменшення (з посиленим контролем). Наслідком цього є зниження надійності охорони по периметру. Водночас необхідно підвищити надійність охорони будівель, цехів та приміщень на території об'єкта збільшенням кількості особового складу підрозділу, який охороняє об'єкт, або залученням до охорони і оборони об'єкта інших підрозділів Сил безпеки і оборони України. При цьому заборонену зону треба обладнати обмеженою кількістю ІТЗО із засобами, які першочергово виявлятимуть факти проникнення порушника, на окремих напрямках з установленням інженерних загороджень і перешкод з додержанням режиму маскування. Організацію охорони об'єкта пропонується

здійснювати так: режимні будівлі, цехи та приміщення мають бути обладнані двома-трьома рубежами ІТЗО, системами відеоспостереження та іншими інженерними засобами. Охорона на КПП повинна забезпечуватися чатовими без залучення їх до патрулювання чи інших дій, що можуть розкрити розташування об'єкта. У неробочий час охорона має здійснюватися шляхом оперативного чергування. Контроль за територією забезпечується потай підрозділами, залученими до охорони й оборони об'єкта, а також спеціальними режимними підрозділами об'єкта. Унаслідок використання систем автоматизованого пропуску співробітників (транспорту) на об'єктах вивільняються великі людські ресурси, які раніше залучалися до здійснення пропуску співробітників і транспорту під час несення служби на КПП.

3. Об'єкти, на яких система охорони значною мірою не впливає на розкриття характеру і призначення об'єкта і де не доцільно зменшувати демаскуючі ознаки системи охорони, необхідно обладнати певним комплексом ІТЗО (з комплексною охороною). Охорона на цих об'єктах може здійснюватися такими способами або їх поєднанням [11], як: несення служби чатовими на КПП, визначених ділянках периметра об'єкта та/або його режимних приміщень, реагування вартою на протиправні посягання стосовно об'єкта, а також на порушення пропускного чи внутрішньооб'єктового режимів; оперативне чергування варти, тобто забезпечення виявлення особовим складом варти людей або предметів по периметру об'єкта та/або в його режимних приміщеннях за допомогою засобів виявлення і відеоспостереження. Отже, умовна класифікація об'єктів за способами охорони, ступенем обладнання їх ІТЗО та за кількістю постів і особового складу, задіяних для охорони і оборони об'єктів, визначена наказом [11].

Оскільки маскування елементів системи охорони тісно пов'язане з надійністю охорони об'єкта і залежить передусім від режиму об'єкта в цілому або від його окремих підрозділів, до визначення системи забезпечення безпеки об'єкта необхідно підходити з позиції запропонованої у статті початкової класифікації об'єктів.

Наведемо визначені елементи ІТЗО за ступенем мінімізації їх демаскуючих чинників.

1. Контрольно-слідові смуги (КСС). Вони мають найбільш виражений демаскуючий характер, оскільки поверхня спеціально підготовлена і сформована, тому потребують заміни на природні КСС. Природна КСС зливається із тлом навколишнього середовища, демаскуючих ознак штучних КСС немає, а у випадку, якщо на території об'єкта облаштовані газони, то КСС буде природним продовженням цих газонів і забезпечуватиме виявлення слідів проникнення порушників за їх наявності. Є можливість і повністю відмовитися від КСС у разі забезпечення забороненої зони надійними сигнальними засобами, що дають змогу визначити напрямок проникнення порушників і засоби їх ідентифікації з використанням фото-, відеоапаратури та штучного інтелекту (ШІ).

2. Система освітлення у забороненій зоні як наступний за значущістю у демаскуванні елемент ІТЗО. Потребує модернізації та максимального наближення за зовнішніми ознаками до навколишнього середовища. Доцільно насамперед відмовитися від прожекторного освітлення, а також від усіх варіантів систем охоронного освітлення, поєднаних із засобами виявлення. Освітлення забороненої зони не повинне перевищувати освітлення інших територій, об'єктів, що знаходяться поблизу, щоб за їх конфігурацією було неможливо (складно) ідентифікувати периметр об'єкта. Для спостереження за станом КСС та інших елементів забороненої зони необхідно використовувати засоби нічного бачення, відеоспостереження, ШІ.

3. Шляхи руху охорони, а у деяких випадках – і стежки нарядів, особливо постійні, що мають штучне покриття і розташовані у забороненій зоні. Вони потребують мінімізації або взагалі відмови від них. Вирішення питання – це максимальне використання внутрішньооб'єктових доріг, а в окремих випадках – їх спеціальне (потайливе) будівництво насамперед на віддалених і вразливих місцях з розташуванням безпосередньо близько до забороненої зони. Це питання необхідно вирішувати на стадії розроблення актів міжвідомчої комісії та проєкту ІТЗО.

4. Інженерні споруди, загородження та перешкоди, які за їх традиційного розміщення у заборонених зонах є істотним демаскуючим елементом системи охорони. Відмова від застосування дротяних парканів, зокрема як основної огорожі та огорожі забороненої зони, підкреслює цивільну належність, оскільки звичайні державні об'єкти здебільшого таких огорож не мають, найпоширенішим варіантом основної огорожі є виготовлена із залізобетонних конструкцій. На цей час є чимало більш сучасних варіантів, таких, як декоративні паркани із композитів, електронні або сенсорні периметри та ін. Як внутрішню огорожу забороненої зони можна використовувати «живі огорожі», які у разі правильного розташування і догляду можуть слугувати перешкодою, будучи при цьому природним продовженням зелених насаджень у вигляді декоративних чагарників на території об'єкта. На віддалених і вразливих ділянках рекомендовано застосовувати інженерні перешкоди, а

саме: дротяні малопомітні завади, дротяну сітку на низьких кілках, дротяні гірлянди і спіралі та ін. Зазначені вище інженерні перешкоди розташовують на поверхні землі і маскують за допомогою спеціальних засобів, рослинного покриву властивостями під місцеві предмети. Для вирішення цього завдання ефективно використовувати мобільні комплекси технічних засобів охорони, а також розвідувальні локаційні комплекси.

5. Засоби виявлення і сигнально-загороджувальні системи у заборонених зонах об'єктів з посиленим контролем. Украй необхідно переглянути тактику використання засобів виявлення і сигнально-загороджувальних систем, виключивши засоби з великою і погано маскованою лінійною частиною сигнально-загороджувальних систем [8].

Оскільки для порушників головною завадою на об'єктах є основна огорожа, то сигнальний рубіж обов'язково має проходити по ній, а зона чутливості засобу виявлення розташовується так, щоб зафіксувати порушника у процесі подолання основної огорожі. Рекомендовано також використання двох рубежів сигналізації. Перший рубіж – по верху основної огорожі, а другий – у наземному виконанні або під землею. При цьому крім надійного визначення напрямку руху порушника можна зафіксувати підкоп під основну огорожу.

З огляду на зазначене вище сформуємо такі пропозиції.

1. Маскування об'єктів, що охороняються підрозділами НГУ та іншими військовими формуваннями, є важливим завданням, і виконувати його необхідно з урахуванням специфіки об'єкта і дотриманням вимог із забезпечення надійності їх охорони. Для виконання цього завдання потрібні наукові підходи і практичне застосування відповідно до досвіду і наукового прогресу.

2. Вирішення проблеми маскування об'єктів, і передусім їх системи охорони, потребує перегляду обладнання ІТЗО, що використовують під час охорони забороненої зони об'єкта, який охороняється.

3. Необхідно принципово переглянути відомі підходи до інженерно-технічного забезпечення охорони для досягнення якісного вдосконалення системи охорони об'єктів, що забезпечує її надійність у поєднанні з іншими важливими чинниками, зокрема високим рівнем маскування об'єкта. Відсутність в Україні централізованої структури, відповідальної за розроблення технічних засобів охорони та оцінювання їх експлуатаційних характеристик (зокрема й маскувальних властивостей) для потреб усіх зацікавлених міністерств і відомств, а також недостатньо розвинена промислова база, яка б забезпечила виробництво сучасних засобів і систем охорони, є одними з головних перешкод для вирішення цього завдання.

Назріла потреба в удосконаленні спеціалізованої галузі, здатної забезпечити розроблення, серійне виробництво та впровадження сучасних технічних засобів охорони, які відповідатимуть рівню найкращих світових аналогів.

Інвестування у розвиток цієї галузі промисловості є економічно доцільним, оскільки її продукція має стабільний і практично невичерпний ринок збуту (зокрема, системи автоматизованого контролю доступу можуть застосовуватися не лише на ВДО та ОКІ, а й у цивільному секторі), а також сприятиме оптимізації використання людських ресурсів шляхом зменшення потреби в охороні традиційними засобами.

4. На сьогодні доцільним є порушення питання розміщення у заборонених і режимних зонах промислових майданчиків (де вже реалізується система охорони периметру) не лише традиційних сигнальних засобів і систем, а й додаткових комплексних рішень, що активно застосовуються закордонними практиками [14, 15]: радіомовні, фотоелектронні та акустичні засоби психологічного впливу, автоматичні установки імітації стрільби, системи на основі LiDAR, радарні датчики, волоконно-оптичні детектори і тепловізійні камери для раннього виявлення порушників, керовані безпілотні комплекси та автономні роботизовані патрульні системи (UGV/дрони), а також лазерні засоби типу Dazzler для психологічного або сенсорного стримування.

Застосування таких систем є більш ефективним засобом для затримання порушника у межах забороненої зони і водночас значно економічнішим порівняно з розгортанням повноцінних інженерних рубежів механічного затримання.

Імовірність ураження порушника, який свідомо або випадково опинився у зоні дії таких засобів, не перевищує ризик ураження вогнепальною зброєю, що перебуває на озброєнні підрозділів охорони.

У процесі організації охорони та оборони об'єктів у мирний час і в умовах воєнного стану з метою протидії диверсійним загрозам доцільно розглядати можливість застосування для ширшого кола об'єктів сучасних високотехнологічних засобів. До таких належать: електронні бар'єри з інтегрованими сенсорами, автоматизовані бойові модулі з дистанційним керуванням або режимом автономного виявлення цілей, системи активного захисту на основі мікрохвильового або акустичного впливу, інтелектуальні протипроникні системи з використанням штучного інтелекту, а також

роботизовані патрульні платформи і дрони-розвідники, здатні виявляти і стримувати противника без залучення значного людського ресурсу.

Висновки

Отже, у сучасних умовах широкомасштабної збройної агресії, зростаючої активності диверсійно-розвідувальних груп та вогневого ураження повітряними засобами противника питання комплексного забезпечення безпеки об’єктів критичної інфраструктури та важливих державних об’єктів набуває пріоритетного значення. У статті обґрунтовано необхідність системного підходу до організації охорони таких об’єктів, який має базуватися на поєднанні традиційних і новітніх інженерних та інженерно-технічних засобів охорони, засобів маскування, систем відеоспостереження, радіолокаційного та сенсорного моніторингу тощо.

Маскування важливих державних об’єктів та об’єктів критичної інфраструктури є багатовимірною проблемою, що виходить за межі лише інженерних або організаційних рішень. Воно має враховувати всі чинники демаскування – від характерних елементів об’єктів до діяльності підрозділів охорони, з одночасним збереженням надійності системи безпеки.

Відмова від заборонених зон задля посилення маскування є спірним підходом, оскільки це призводить до зниження рівня захищеності. Натомість доцільним є їх модернізація шляхом інтеграції новітніх інженерно-технічних засобів охорони та систем виявлення для зменшення демаскуючих чинників.

Класифікація об’єктів (з обмеженням допуску, з посиленим контролем та з комплексною охороною) – дає змогу диференційовано підходити до організації маскування й охорони, оптимізуючи витрати ресурсів і рівень застосування інженерно-технічних засобів охорони.

Демаскуючі елементи інженерних та інженерно-технічних засобів охорони (контрольно-слідові смуги, освітлення, шляхи руху, інженерні загородження, системи виявлення) потребують цілеспрямованого вдосконалювання. Це можливо шляхом заміни штучних елементів природними (наприклад, «живими огорожами»), застосування прихованих сенсорних систем, використання природного ландшафту та високотехнологічних засобів (штучний інтелект, відеоаналітика, LiDAR, волоконно-оптичні сенсори).

Одним із важливих чинників ефективності є інтеграція технологій стримування і виявлення загроз, включно з акустичними, електронними, фотоелектронними, роботизованими та безпілотними платформами [14]. Підрозділи Сил безпеки і оборони України потребують єдиних стандартів, методичних рекомендацій та технічного забезпечення, адаптованого до умов воєнного стану. Не менш важливим є створення єдиного центру розроблення, випробування та впровадження інженерно-технічних засобів охорони, а також розвиток національної промислової бази, здатної задовольнити потреби у новітніх охоронних системах [15].

Застосування сучасних високотехнологічних рішень дає змогу зменшити залежність від людського ресурсу і підвищити надійність охорони за умови збереження високого рівня маскування об’єктів. У підсумку для ефективної охорони важливих державних об’єктів та об’єктів критичної інфраструктури вкрай необхідним є не лише технічне переоснащення, а й перегляд принципів організації охоронних заходів, їх адаптації до нових викликів і стандартів безпеки.

Перелік джерел посилання

1. Юрченко В. О., Соколовський І. П. (2023). Шляхи удосконалення інженерно-технічних заходів цивільного захисту об’єктів критичної інфраструктури в умовах особливого періоду. *Науковий вісник. Державне управління.* 2023. № 1 (13). С. 291–312. DOI: https://doi.org/10.33269/2618-0065-2023-1(13)-291-312.
2. Бубела Т. З., Мельник М. Я., Назаровець О. Б., Рудик Ю. І. (2024). Аналіз визначень та нормативних вимог системи захисту об’єкта критичної інфраструктури. *Вісник ЛДУБЖД. Цивільна безпека*. 2024. № 29. С. 119–127. DOI: https://doi.org/10.32447/20784643.29.2024.13.
3. Коваль М. В., Коваль В. В., Коцюруба В. І., Білик А. С. Організаційно-технічні засади побудови системи інженерного захисту об’єктів критичної інфраструктури енергетичної галузі України. *Наука і оборона. Актуальні питання національної безпеки та оборони.* 2022. № 3/4. С. 11–16. DOI: https://doi.org/10.33099/2618-1614-2022-20-3-4-11-16.
4. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Економіка.* 2015. № 4 (37). С. 83–93. URL: https://surl.li/szltgv (дата звернення: 29.07.2025).

5. Мурасов Р. К., Мельник Я. В. Оцінювання захищеності кіберпростору об’єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 1 (46). С. 41–44. DOI: https://doi.org/10.33099/2311-7249/2023-46-1-41-44.

6. Пугач В. В., Чепурний В. П., Куртов А. І. Маскування військ та об’єктів. Захист від високоточної зброї : навч. посіб. Харків : ВІОІ НЮУ ім. Ярослава Мудрого, 2022. 116 с.

7. Старух О. С., Овчаренко В. В., Пащенко В. В. Військово-інженерна підготовка : навч. посіб. Харків : НА НГУ, 2017. 262 с.

8. Власов К. В., Казіміров О. О., Глущенко Н. О. Комплексний інженерно-технічний захист об’єктів : підручник. Харків : НА НГУ, 2024. 554 с.

9. Про затвердження Інструкції з організації експлуатації інженерно-технічних засобів охорони на важливих державних об’єктах, які охороняються Національною гвардією України : наказ Міністерства внутрішніх справ України № 56 від 26.01.2017 р. URL: https://zakon.rada.gov.ua/laws/show/z0308-17#Text (дата звернення: 01.08.2025).

10. Назаренко О. Л., Головань О. Л., Рудинський В. В. Щодо питання оцінювання вразливості об’єктів критичної інфраструктури в умовах воєнного стану. *Безпека держави*. 2025. Вип. 1 (5). С. 73–82. DOI: https://doi.org/10.33405/2786-8613/2025/1/5/336731.

11. Про затвердження Положення про організацію та порядок несення служби з охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об’єктів, об’єктів критичної інфраструктури та спеціальних вантажів Національною гвардією України : наказ Міністерства внутрішніх справ України від 15.06.2023 р. № 497. URL: https://zakon.rada.gov.ua/laws/show/z1085-23#Text (дата звернення: 01.08.2025).

12. Назаренко О. Л. Особливості охорони об’єктів критичної інфраструктури підрозділами Національної гвардії України. *Актуальні проблеми діяльності складових сектору безпеки і оборони України в умовах особливих правових режимів: поточний стан та шляхи вирішення* : матеріали II Міжнар. наук.-практ. конф., м. Харків, 20 берез. 2025 р. Харків : НА НГУ, 2025. С. 370–371. URL: https://surl.li/atmtkg (дата звернення: 01.08.2025).

13. Запорожець Т. В. Державна політика у сфері захисту критичної інфраструктури : навч. посіб. Київ : ДКС-Центр, 2024. 186 с.

14. Nazarenko O. L., Hodlevskyi S. O., Danko V. V., Fedorenko V. O. Protecting Ukraine′s critical infrastructure from drone threats: the role of security and defence forces. *European Scientific e-Journal. Actual Issues of Modern Science.* 2025. Issue 37. P. 70–80. DOI: https://doi.org/10.47451/mil2025-04-01.

15. Назаренко О. Л., Онопрієнко О. С. Роль інформаційних технологій та штучного інтелекту в захисті об’єктів критичної інфраструктури. *Проблемні питання тактики дій та всебічного забезпечення військових формувань і правоохоронних органів держави в умовах воєнного стану :* зб. тез наук.-практ. конф., м. Харків, 26 черв. 2025 р. Харків : НА НГУ, 2025. С. 38–39. URL: https://surl.lu/xvqmha (дата звернення: 01.08.2025).

Стаття надійшла до редакції 12.08.2025 р.

UDC 351.865

O. Nazarenko, S. Hodlevskyi, I. Skakalin

ORGANIZATION OF COMPREHENSIVE SECURITY MEASURES FOR CRITICAL INFRASTRUCTURE FACILITIES BY THE SECURITY AND DEFENSE FORCES OF UKRAINE

The article analyzes the main approaches to camouflaging and equipping key critical infrastructure with engineering and technical means under martial law, in particular the experience of their use by units of the Security and Defense Forces of Ukraine to ensure state security. The emphasis is on the principles of combining natural and artificial means of camouflage with engineering and technical elements of protection, as well as on the organization of protection considering the enemy's reconnaissance activities aimed at identifying the location critical infrastructure. Separately, the issue of coordination and interaction between various structures of the Security and Defense Forces of Ukraine when ensuring the protection of these facilities is discussed.

The paper emphasizes that the fragmentation of the existing critical infrastructure protection system of necessitates the formation of the necessary holistic complex of measures that ensures their sustainability by combining physical protection, information security and coordinated interaction of the units of the Security and Defense Forces of Ukraine.

The need for a comprehensive approach to ensuring the security of critical infrastructure is substantiated by improving the choice of location, camouflage, engineering equipment and technical means, adapted to modern conditions and based on the experience of the russian-ukrainian war, which allows forming the optimal components of the critical infrastructure protection system, considering their specifics.

A classification of critical infrastructure by level of protection is proposed, such as with restricted access, with enhanced control and with comprehensive protection, which considers the features of the use of engineering and technical means of protection, the level of camouflage and the organization of interaction of security units.

The elements of the technical means are identified and listed according to the degree of reduction of their decamouflaging factors on critical infrastructure. Proposals are presented to solve the camouflaging issues and achieving a qualitative improvement in the system of ensuring the security of critical infrastructure. The feasibility of introducing a wider range of modern high-tech means of protection and defense for the elements is substantiated, electronic barriers with sensors, automated combat modules, active protection systems, intelligent anti-intrusion technologies, robotic patrol platforms and reconnaissance drones, capable of increasing the effectiveness of countering sabotage threats without significant involvement of human resources.

Therefore, effective protection of critical infrastructure requires the connection of traditional and modern high-tech means of protection and defense, engineering and technical means, camouflaging, video surveillance systems, radar and sensor monitoring. Instead of abandoning prohibited zones, they should be modernized using hidden sensor systems and the latest technologies adapted to martial law conditions, which allow reducing demasking factors and increasing the reliability of protection.

Keywords: *camouflage, engineering means, engineering and technical means of protection, critical infrastructure, facility security system.*

Назаренко Олег Леонідович – кандидат військових наук, доцент кафедри забезпечення державної безпеки навчально-наукового інституту забезпечення державної безпеки, Національна академія Національної гвардії України

https://orcid.org/0000-0001-7579-0658

Годлевський Сергій Олександрович – кандидат військових наук, начальник кафедри оперативної підготовки навчально-наукового інституту професійної освіти, Національна академія Національної гвардії України

https://orcid.org/0000-0002-0437-7847

Скакалін Ігор Володимирович – викладач кафедри тактики навчально-наукового інституту забезпечення державної безпеки, Національна академія Національної гвардії України

https://orcid.org/0009-0004-7568-5398