УДК 343.326

І. А. БІЛОУС,
курсант Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого;

Ю. Р. БУГАЙ,
курсант Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого

ДИВЕРСІЙНИЙ ВПЛИВ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВЕДЕННЯ «ГІБРИДНОЇ ВІЙНИ»

Характерною рисою для сучасних конфліктів є створення передумов для зростання соціального напруження, здійснення економічного та політичного тиску на країну, яка є об'єктом заінтересованості противника. З огляду війн та військових конфліктів останніх десятиліть зрозуміло, що ворогуючі сторони все частіше разом з традиційними, класичними способами ведення бойових дій застосовують політичні, економічні, інформаційні заходи, які є основою в концепції ведення бойових дій, яку називають також «гібридною війною».

Насамперед, домінують диверсійно-підривні дії, інформаційні спеціальні операції, щодо дестабілізації внутрішньої суспільно-політичної обстановки, загострення міжетнічних відносин в країні та атаки в кібернетичному просторі, які в свою чергу порушують роботу систем державного та воєнного управління, об'єктів критичної інфраструктури, мають відволікаючий характер від головних загроз. Саме тому посилення протидиверсійного захисту об'єктів критичної інфраструктури є досить актуальним завданням сьогодення.

Як визначено Законом України «Про основні засади забезпечення кібербезпеки України», до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Через свою важливість для обороноздатності країни дані об'єкти можуть бути обрані як об'єкт диверсійного впливу. При цьому успішно проведені диверсії можуть призвести до величезних збитків для економічної, політичної та соціальної сфери. Відповідно до статті 113 Кримінального кодексу України диверсія – це вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій.

Диверсійно-розвідувальна операція – одна із видів спеціальних операцій. Основна мета диверсій полягає у зниженні можливостей противника щодо ведення збройної боротьби та створення сприятливих умов для застосування сил своїх військ. Зазвичай, дані операції проводяться в тилу противника потайними засобами для порушення систем державного та військового управління ліній комунікацій забезпечення групувань збройних сил.

© Білоус І. А., Бугай Ю. Р., 2019

Як правило, диверсійно-розвідувальні операції здійснюють диверсійно-розвідувальні групи (ДРГ), кількісний та якісний склад яких, штатне озброєння, боєприпаси та спорядження залежать від класу задач, які на неї покладаються. В основному, ДРГ складається з таких суб'єктів: командир групи, снайпер, гранатометник (2 особи), кулеметник (2 особи), стрілець (радист), стрілець (санітар), стрілець (мінер).

Тактика диверсії, або ж підготовки та ведення диверсії є надзвичайним різноманіттям способів дій, які, як правило, здійснюються в момент найменшої здатності противника чинити опір. Великий вплив на неї здійснює характер війни, відношення до них народних мас, соціальний устрій ворогуючих сторін, політична та оперативна обстановка в тилу противника, стан охорони об'єктів. При плануванні таких операцій необхідно враховувати: можливість забезпечення виконавців диверсійними заходами, надійний зв'язок, плив географічних умов, характер обстановки, рівень підготовки та взаємодії особового складу групи, можливість використання місцевих сило опору.

Основою діяльності диверсійних груп є потайні (замасковані) дії, для яких характерна невелика чисельність підрозділу та легке озброєння. Потайне проникнення на територію об'єкта можливе за умов сприяння місцевості, часу доби, поганих погодних умов, за умови обходу засобів охоронної сигналізації та непомітного подолання інженерних та конструктивних перешкод. Також для проникнення на об'єкт диверсії може бути використано черговий транспорт служб термінового виклику (пожежні машини, машини швидкої допомоги). У зв'язку з метушнею в екстремальній ситуації та відволікання сил підрозділу охорони рівень ретельності перевірок такого транспорту на пропускних пунктах зменшується.

Також ДРГ застосовують відкриті, неприховані проникнення на територію, які розраховані на подолання охоронного рубежу найбільш зручним способом. При цьому чисельність диверсійного підрозділу повинна бути більша ніж при спробах потайного проникнення. Але при нападі ДРГ на об'єкт з використанням штурмової тактики факт нападу буде обов'язково виявлений, що викличе реакцію сил охорони, які будуть протидіяти нападникам. Тому, з огляду на складність об'єкта можливість швидкого виконання завдання диверсійною групою є малоймовірною.

Тактика диверсійних дій носить виключно творчий характер та не допускає ніякого шаблону, тому основна вимога – ніколи не повторюватись, а імпровізувати. Способи закидання ДРГ можуть бути такими, як: приховане проникнення суходолом чи морем через державний кордон (лінію розмежування), десантування (повітряне чи морське), відкритий в'їзд на територію країни під видом туристів, членів різноманітних делегацій, груп із наступним «розчиненням» серед місцевого населення і переміщення в райони очікування чи бойового застосування.

Способи скритого проникнення ДРГ на об'єкти критичної інфраструктури можуть бути наступними:

– маскування під цивільних осіб;

– проникнення та дії на території об'єкта за допомогою маскування під уповноважених осіб;

– висування, проникнення та дії на об'єкті під прикриттям несприятливих погодних умов;

– обходу засобів охоронної сигналізації та непомітне подолання інженерних та конструктивних перешкод;

– шляхом використання підроблених документів або при змові зі співробітниками охорони;

– проїзд чергового транспорту служб термінового виклику.

До протидиверсійного захисту об'єктів критичної інфраструктури долучається Служба безпеки України, Національна поліція, Національна гвардія України, Збройні Сили України.

В умовах ведення «гібридної війни» органи та підрозділи військового управління також можуть зазнати диверсійного впливу. Зокрема, можливе виведення з ладу чи взяття під контроль таких об'єктів, захоплення зброї, співробітників, матеріальних носіїв інформації з

обмеженим доступом, засобів конфіденційного зв'язку. Загрози стосовно об'єктів органів військового управління можуть бути як зовнішніми (особи, які не є співробітниками), так і внутрішніми (особи із числа працівників).

Так як виведення з нормального, сталого функціонування таких органів може призвести до масових безладів у суспільстві та зменшення авторитету складових сектору безпеки і оборони, тому розвиток та удосконалення системи протидиверсійного захисту об'єктів органів військового управління є актуальною науковою задачею. Вирішення цього питання має бути комплексним. Зокрема, потребує перегляду система наземної охорони та оборони в умовах міста, організації внутрішньооб'єктового режиму, посилення заходів власної безпеки. Саме вироблення дієвих механізмів протидії найбільш імовірним загрозам диверсійного характеру є запорукою недопущення (мінімізації наслідків) диверсій.

Загрозливі зміни безпекового середовища вимагають побудови в України надійної, інтегрованої та гнучкої системи протидиверсійного захисту об'єктів критичної інфраструктури. Складові такої системи повинні не допустити можливість вчинення диверсійно-підривних дій або мінімізувати їх наслідки в політичній, економічній, воєнних сферах та кібернетичному просторі. Підсумовуючи вищесказане, можна зробити висновок, що з метою дестабілізації обстановки, зростання соціального напруження, політичного й економічного тиску, противник застосовуватиме диверсії на мирних територіях, де не ведуться бойові дії та не оголошено воєнний стан. Саме за таких обставин на сектор безпеки і оборони України покладаються важливі завдання щодо забезпечення протидиверсійного захисту об'єктів критичної інфраструктури. Велике коло цих завдань вирішує Служба безпеки України.

Характерною рисою «гібридної» війни є те, що противник намагатиметься завдати поразки не тільки підрозділам регулярної армії, але й об'єктам критичної інфраструктури, які знаходяться в глибині території. Для реалізації такого сценарію розвитку подій постійно удосконалюються бойові можливості і способи застосування диверсійно-розвідувальних груп. Постійний розвиток форм та способів диверсійних дій в тилу противника, поліпшення тактико-технічних характеристик високоточної зброї та звичайних військових засобів ураження, загрози в кібернетичному просторі обумовлюють досить високі вимоги до національної системи проти диверсійного захисту об'єктів критичної інфраструктури.

Таким чином, в роботі показано важливість щонайшвидшого вирішення питання проти диверсійний захист об'єктів критичної інфраструктури України. Одним із позитивних зрушень в даному контексті стане прийняття проект Закону України «Про критичну інфраструктуру та її захист». Це надасть можливість унормувати сферу відповідальності за організацію проти диверсійного захисту між органами державної влади. Також доцільно визначити (утворити) державний орган, відповідальний за контроль та загальну координацію дій з питань захисту об'єктів критичної інфраструктури. Для прикладу можна використати досвід європейських країн, зокрема Словаччини, яка ще у 2007 році ухвалила «Концепцію критичної інфраструктури Словацької Республіки, її захисту та оборони», де визначено загальну стратегію захисту життєво важливих об'єктів країни.

Надійшла до редколегії 06.04.2019