Розділ 4

ЗОВНІШНЯ ПОЛІТИКА ТА НАЦІОНАЛЬНА БЕЗПЕКА

http://doi.org/10.26565/1727-6667-2024-1-10
УДК 351/354(007.5)

Лукін Сергій Юрійович,
доктор наук з державного управління, доцент,
директор Регіонального центру підвищення кваліфікації Київської області,
площа Лесі Українки, 1, м. Київ, Україна
ORCID ID: https://orcid.org/0000-0001-6516-5605
e-mail: serge.lukin77@gmail.com

Тихоненко Олександр Олександрович,
кандидат наук з державного управління,
викладач Регіонального центру підвищення кваліфікації Київської області,
площа Лесі Українки, 1, м. Київ, Україна
ORCID ID: https://orcid.org/0000-0002-5140-3737
e-mail: tikhonenko4mail@gmail.com

ЗАСТОСУВАННЯ ПРОФАЙЛІНГУ В СИСТЕМАХ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. В статті пропонується авторське бачення щодо можливостей та ефективності використання сучасних наукових методів в системах забезпечення фізичної безпеки об'єктів різних форм власності, в тому числі й об'єктів критичної інфраструктури. Метою даної статті є продовження дослідження механізмів профайлінгу у сфері виявлення загроз в державній безпеці, що особливо актуально в умовах глобальних геополітичних змін, які стали передумовами підвищення військових, кримінальних, терористичних та інших ризиків та загроз. Все це комплексно спливає на систему публічного управління, тому авторами крізь призму безпеки як стану та процесу висвітлено актуальну потребу щодо пошуку та розробки ефективних практичних методів їх досягнення. Профайлінг як метод прогностичного аналізу поведінки антропогенного виду загроз – порушника та пов'язаних з ним подій – є важливим практичним інструментом в арсеналі кінцевого виконавця – фахівця в сфері охорони (захисту). У статті досліджується теоретичний та практичний базис впровадження в практичні процеси забезпечення безпеки об'єкту критичної інфраструктури в умовах підвищених військових ризиків. Розглянуто способи інтеграції профайлінгу з іншими технологіями забезпечення фізичної безпеки, включа-

ючи сучасні системи відеоспостереження, контролю та управління доступом, штучного інтелекту та інших. Показано, що ефективне забезпечення фізичної безпеки вимагає не тільки сучасного оснащення систем безпеки та високої кваліфікації кінцевих виконавців – співробітників, здатних оперативно реагувати на загрози, – а й у створенні певного середовища, при якому використання такого оснащення та співробітників буде мати максимально продуктивний рівень із залученням мінімально необхідних ресурсів. Для підвищення ефективності державного управління в відповідній сфері на основі проведених досліджень зроблено висновок про необхідність розробки єдиної методології, стандартів та протоколів для застосування профайлінгу в процесі побудови системи фізичної безпеки об'єктів критичної інфраструктури, що дозволить підвищити ефективність виявлення та запобігання загрозам, мінімізувати рівень ризиків для цивільного населення та забезпечити стабільне функціонування критично важливих об'єктів, навіть в умовах військової нестабільності, раціонально використовувати ресурси, сили та засоби. Авторами розглядаються перспективи подальших досліджень у галузі профайлінгу та його інтеграції з перспективними технологіями, спрямованими на підвищення рівня державної безпеки.

Ключові слова: *профайлінг, національна безпека, державне управління, критична інфраструктура.*

Як цитувати: Лукін С. Ю., Тихоненко О. О. Застосування профайлінгу в системах безпеки об'єктів критичної інфраструктури. *Теорія та практика державного управління*. 2024. Вип. 1 (78). С. 168–182. https://doi.org/10.26565/1727-6667-2024-1-10

Вступ. В сучасних умовах державні об'єкти – підприємства, установи, організації, органи місцевого самоврядування та державної влади, об'єкти критичної інфраструктури тощо (далі – важливі об'єкти) перебувають у стані високої ймовірності реалізації великого спектру загроз їхнього сталого функціонування. У зв'язку з високим рівнем динамічності подій в країні, достатньо важко з високим рівнем точності визначити всі можливі негативні наслідки. Вся система державного управління перебуває в стані невизначеності та постійних зовнішніх ризиків. Окремо хочемо зауважити, що це контрастує з тим, що у разі настання небезпеки на важливому об'єкті може утворитися ланцюгова реакція, що зачепить всі важливі державні сектори, починаючи від забезпечення базових потреб людини до основних життєво важливих функцій держави – здібностей, можливостей державних сил та засобів забезпечувати власну безпеку, що особливо актуально під час військового стану в умовах повномасштабної агресії ворога.

Загалом, важливі об'єкти мають широкий спектр впливу та вагоме значення для сталого функціонування держави, а порушення їхнього функціонування може призвести до виникнення кризової, небезпечної ситуації державного, регіонального, місцевого чи локального значення. У зв'язку з цим актуальними постають питання, які охоплюють коло завдань із забезпечення фізичної безпеки всіх важливих об'єктів.

Мета. Метою статті є дослідження ролі та місця застосування профайлінгу в безпекових заходах, що спрямовані на забезпечення фізичної безпеки (охорони захисту) об'єктів, зокрема, теоретичної та практичної оцінки і визначення

ефективності профілювання порушника, розробки ефективного механізму організації безпекового середовища щодо об'єкту забезпечення фізичної безпеки, в тому числі й об'єктів критичної інфраструктури в умовах воєнного стану.

Огляд літератури. У спеціалізованій літературі безпека об'єкта як термін трактується у широкому сенсі – від стану об'єкта при якому відсутня будь-яка небезпека, до процесу щодо спроможності досягнення такого стану. Наприклад, згідно Закону України «Про критичну інфраструктуру та її захист» термін, який нас цікавить трактується як: «стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість критичної інфраструктури», а процес щодо досягнення такого стану захисту як – «всі види діяльності, спрямовані на своєчасне виявлення, запобігання й нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків їх реалізації». В той же час Закон України «Про національну безпеку України» трактує поняття безпеки як стан: а) «захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних та потенційних загроз невоєнного характеру»; б) «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [8, 9].

Вивчаючи сутність трактування терміну безпеки від філософського до таких, що викладені в діючому чинному законодавстві, ми можемо зробити припущення про те, що для забезпечення безпеки як процесу необхідні ефективні механізми з попередження, виявлення та локалізації (припинення) реалізації небезпеки (загрози) важливих об'єктів, а у разі їх настання – мінімізації чи компенсації збитків. Також зазначимо, що досягнення визначеного стану захищеності неможливе без забезпечення фізичних заходів, що необхідні для збереження цілісності важливих об'єктів, попередження, реагування та локалізації небезпек (загроз) шляхом здійснення охорони (захисту) визначеного об'єкта чи окремого його елементу. Ефективні заходи з охорони об'єкта повинні здійснюватися комплексно з використанням необхідних інженерних, технічних, адміністративних, фізичних та інших заходів та засобів, в тому числі фахівців, персоналу охорони (захисту), які здійснюють захист об'єкту та\або його складових – майна, устаткування, інформації, природних та інших ресурсів, життя та здоров'я персоналу тощо.

Багатьма вітчизняними науковцями (Д. Бобро, В. Франчук, П. Пригунов, С. Мельник, М. Шутий, А. Сосин, Ю. Оніщенко, К. Чукалов, А. Синжерян, В. Ємельянов, Г. Бондар, С. Кондратов, О. Суходоля та ін.) проводилась робота в напрямку аналізу науково-аналітичних, нормативно-правових та інших джерел, за результатами якої багато з них визначають, що з різних причин в Україні відсутня усталена система безпеки важливих об'єктів, а питання організації фізичної безпеки часто розглядаються частково, не повно, фрагментарно [1, 2, 4, 5, 10, 13, 17, 18, 21]. Особливо це контрастує в ході порівняння безпекових засад, впроваджених в країнах НАТО та Європейського союзу. Таку особливість пояснюють тим, що вищевказані країни були піонерами в створенні початкових безпекових концепцій, визначення важливих об'єктів як критичної інф-

раструктури та неопосередковане поєднання їхнього сталого функціонування безпосередньо з національною безпекою країни [6].

Наприклад, вважається, що вперше термін «критична інфраструктура» з'явився у 1996 році в Сполучених Штатах Америки. В 2001 році в США вже було прийнято перший закон, у якому чітко було заявлено про тісний зв'язок між державною безпекою та станом захищеності важливих державних об'єктів. Проте, незважаючи на значно вищий рівень теоретичного та практичного забезпечення в частині, що стосується питань захисту важливих об'єктів, країни ЄС та НАТО все одно визначають досить актуальними питання безпеки та наголошують на подальшому вдосконаленні систем та процедур захисту, про що неодноразово заявлялось та оприлюднювалось в засобах масової інформації президентом Єврокомісії Урсулою фон дер Ляйен та генеральним секретарем НАТО Єнсом Столтенбергом [3,7].

Вивчаючи джерела виникнення небезпеки як явища, що здатне за певних умов завдати негативного впливу на цілісність чи стале функціонування важливих об'єктів, нами було виділено та умовно поділено їх на дві групи: за явної участі людини як джерела (антропогенні небезпеки) та без такої участі (природні небезпеки) [17 С. 148-149].

Забезпечення безпеки важливих об'єктів може складатись із значної кількості заходів, що направлені на забезпечення мінімізації економічних, екологічних, кримінальних, терористичних, інформаційних, правових та інших небезпек. Так, одним із першочергових, базових заходів є створення безпекового середовища шляхом визначення меж об'єкта та забезпечення їх фізичного захисту (охорони), контрольованого потрапляння осіб на територію, переміщення майна, першочергового реагування на надзвичайні події тощо.

Здійснення фізичної охорони є складовим механізмом забезпечення безпеки об'єктів, що містить (повинно містити) фізичні, технічні, інженерні та інші заходи, що охоплюють широку сферу можливих (потенційних) загроз важливим державним та приватним об'єктам [4]. У той же час, персонал охорони (людина) своєю діяльністю чи бездіяльністю може становити небезпеку (загрозу) таким об'єктам, у зв'язку з чим набуває актуальності безпосередня оцінка діяльності та розробка ефективних алгоритмів їхніх дій, створення належних умов для безпосереднього виконання завдань за призначенням, особливо в умовах впровадження у державі правового режиму воєнного стану.

Методологія дослідження. Для вивчення застосування профайлінгу в системах безпеки об'єктів критичної інфраструктури в умовах воєнного стану було розроблено багатоетапну методологію, яка включала в себе теоретичний аналіз, емпіричне дослідження та метод синтезу отриманих даних.

Першим етапом дослідження стало вивчення наукових джерел та останніх вітчизняних та міжнародних досліджень з теми профайлінгу та безпеки об'єктів критичної інфраструктури. Було проведено аналіз напрацювань, статей, тез наукових конференцій, а також міжнародних стандартів та протоколів безпеки. Особлива увага приділялась матеріалам, що описують застосування профайлінгу в умовах підвищених рівнів загроз, таких як терористичні акти та військові

конфлікти. Було виокремлено ключові концепції, методи та інструменти профайлінгу, що застосовуються в безпековій сфері.

На другому етапі проводили емпіричне дослідження, що охоплювало збирання даних шляхом опитування та проведення інтерв'ю як з експертами, так і з кінцевими виконавцями заходів в галузі безпеки, в ході чого було опитано представників державних структур, приватних охоронних компаній та академічної спільноти. Для збору даних використовувались анкети з попереднього наукового дослідження, що дало змогу отримати динаміку розвитку та дані про поточні практики і проблеми застосування профайлінгу в практичній діяльності з виявленні загроз державній безпеці в мирний час та в умовах воєнного стану.

Отримані дані було опрацьовано та проаналізовано з використанням методів якісного, порівняльного та кількісного аналізу. Застосовувалися статистичні методи для виявлення закономірностей і тенденцій у використанні профайлінгу, проведено SWOT-аналіз (аналіз сильних і слабких сторін, можливостей і загроз) профайлінгу як інструменту забезпечення фізичної безпеки об'єктів. Крім того, використовувався кейс метод для детального розгляду конкретних випадків успішного та неуспішного застосування профайлінгу в реальних умовах.

На завершальному етапі дослідження проводився синтез теоретичних та емпіричних даних, в ході якого було сформульовано найбільш перспективні алгоритми дій щодо поліпшення практик застосування профайлінгу в умовах воєнного стану, заходи щодо інтеграції профайлінгу з іншими безпековими технологіями, розроблено рекомендації з навчання та підготовки персоналу, а також можливі заходи міжвідомчої взаємодії, що є одним з важних елементів системи державного управління та безпеки.

Для перевірки надійності та валідності результатів дослідження було проведено експертну оцінку запропонованих рекомендацій. Окремі результати дослідження та рекомендації було презентовано на наукових конференціях і семінарах, де вони отримали схвальні відгуки та зауваження, що дало змогу скоригувати та покращити запропоновані методи та підходи. Таким чином, методологія дослідження містила в собі комплексний підхід, який поєднував теоретичний аналіз, емпіричне дослідження та синтез отриманих даних, що дало змогу глибоко та всебічно вивчити застосування профайлінгу в безпекових процесах.

Виклад основного матеріалу та результати дослідження. Вагомим елементом забезпечення безпеки важливих об'єктів є підтримання належного рівня стійкого, безперервного функціонування цього процесу. Такий процес можна уявити як комплексний, синхронний алгоритм злагодженої взаємодії всіх його складових елементів.

Будь-який алгоритм – це, перш за все, сукупність, набір інструкцій, правил, дій, команд тощо, що направлені окремому складовому елементу (виконавцю) щодо досягнення визначеної місії, виконання задачі та досягнення необхідного результату. Порушення виконання (невиконання, неналежне виконання) дій таких алгоритмів веде (може призвести) до збоїв, затримці та\або неспроможності досягти визначеного необхідного результату. Таким чином, зважаючи на вищесказане, при розгляді великої кількості видів та типів загроз з групи ан-

тропогенних – кримінальні, терористичні, техногенні, інформаційні, соціальні, політичні тощо, – ми виділяємо людину як основне джерело виникнення антропогенного ризику та загрози – порушника.

В ході вивчення спеціалізованих науково-інформативних джерел, нами встановлено, що більшість визначає порушника як того, хто порушує, нехтує, протидіє чи не виконує набір визначених правил і, як правило, визначається терміном «особа порушника» [11,12, 19, 22].

Вивчаючи профайлінгові механізми в сфері виявлення загроз державного безпекового сектору, нами було встановлено, що при проведенні оцінювання людини, на безпеку чи загрозу, обов'язково необхідно враховувати та оцінювати поведінку людини по відношенню до середовища, в якому вона перебуває (може перебувати): соціуму, живим чи неживим предметам, об'єктам, процесам тощо. У такому разі одиницею виміру при оцінці людини є вчинок, тобто, окрема усвідомлена дія, реалізований акт по відношенню до когось чи чогось.

Розглядаючи поведінку через вчинок людини, крізь призму безпеки, моралі та права, його можна оцінювати як безпечний чи небезпечний, позитивний чи негативний, правомірний чи злочинний тощо. Відповідно до такої оцінки, особа порушника стає або може стати антропогенною загрозою у разі реалізації нею певної закінченої дії, а поведінку в такому випадку можна трактувати як небезпечну, ризиковану чи загрозливу.

У свою чергу для кожного окремого об'єкта, щодо якого здійснюється захист, може бути більшою або меншою мірою актуальний той чи інший вид порушника з відповідною небезпечною поведінкою – терорист, злодій, хуліган, диверсант, вбивця, шпигун тощо. У зв'язку із зазначеним, важливим завданням кінцевого виконавця – представником підрозділу охорони (захисту), – є знання та вміння визначити ознаки небезпечної поведінки порушника (поведінкові патерни), своєчасне виявлення, підготовка та реалізація заходів з реагування, припинення та\або локалізації реалізації загрози. Сукупність ознак небезпечної особи (порушника) в процесі здійснення профайлінгу визначають як профіль порушника, а сам процес виявлення – профайлінгом [16].

Водночас, в рамках дослідження авторами проведено опитування представників державних та приватних підрозділів, задіяних в безпосередніх заходах з охорони (захисту) об'єктів, в тому числі й державних та приватних об'єктів, що входять до об'єктів критичної інфраструктури. За результатами опитування співробітників підрозділів, що забезпечують охорону (захист) вищевказаних об'єктів, було виявлено таке: низький рівень розпізнавання емоційних станів людини (менше 40% вірних визначень) у зв'язку з низькою обізнаністю щодо фізіологічних особливостей прояву емоцій на обличчі людини; високий рівень визначення стану алкогольної сп'янілості (97% вірних відповідей), проте низькі показники визначення наркотичної сп'янілості (28% вірних відповідей); низький показник ідентифікації психічно хворих осіб з явними патологіями (>50% вірних відповідей). Окремо хочемо зауважити, що велика кількість респондентів, що виконувала обов'язки з охорони (захисту) об'єктів критичної інфраструктури, здебільшого відкидала можливість появи порушника на їхніх об'єктах з ознаками профілю терориста, шпигуна, диверсанта [17, С. 119-124].

Після початку масованого повномасштабного вторгнення ворога велика кількість важливих об'єктів, на яких перебували респонденти дослідження, зазнала диверсійних проявів та прямих атак ворога, в результаті чого респонденти отримали та адсорбували певний унікальний досвід, Це дало змогу нам провести повторне тестування та розглянути можливу ефективність й доцільність впровадження механізмів профайлінгу в умовах введення режиму воєнного стану та значного підвищення військових ризиків для важливих об'єктів.

За результатами опрацювання анкетних даних повторного опитування значної зміни зазнали результати позитивних відповідей щодо визначення патернів поведінки порушника з психічною хворобою (72% проти 48%), з залежністю та наркотичним сп'янінням (51% та 73% проти 29% та 38%). Також для більшості об'єктів особовим складом було визначено поведінкові патерни порушників з профілю «спостерігач», «фотограф», «диверсант», що включали в себе ознаки протиправної поведінки щодо отримання інформації про об'єкт охорони з подальшим нанесенням ворогом ракетно-дронових атак з повітря, терористично-диверсійних дій тощо. Наприклад, в ході проведення охоронних заходів на одному з державних об'єктів, що відносяться до критичної інфраструктури, за 2022 рік було виявлено та передано правоохоронним органам 134 особи, за 2023 рік – 799 осіб та за перше півріччя 2024 року – 260 осіб. Враховуючи, що при досить високому рівні визначених загроз станом на перше півріччя 2024 року не відбулось їхнього розвитку та перетворення в безпосередню небезпеку, можна говорити про високу ефективність впровадження профайлінгу в загальний комплекс системи безпекових заходів.

Окремо контрастує факт того, що після проведення анкетування в додаткових опитувальних бесідах у респондентів відмічається стійка впевненість, що їхній об'єкт в сучасних умовах є потенційною ціллю розвідувальної, диверсійної та терористичної діяльності ворожих елементів військових формувань та спеціальних служб. Водночас на момент аналогічного дослідження в умовах мирного часу більшістю респондентів даний факт категорично заперечувався, а при запропонуванні відкидався.

В процесі побудови, вдосконаленні чи проведенні інших безпекових заходів з підвищення ефективності функціонування комплексної системи фізичної безпеки, впровадження механізму моделювання об'єкту забезпечення охорони (захисту), аналізу дій порушника, розрахунку інших можливих сценаріїв виникнення та реалізації ризику тієї чи іншої загрози створюється можливість оцінювання потенційної небезпеки та розроблення як ефективних заходів, так і самої системи фізичної безпеки (охорони, захисту) з найбільш раціональним використанням ресурсів. Це дозволяє охопити більшість вимог, які необхідні для забезпечення та проведення безпекових заходів, основною задачею яких є недопущення та\або мінімізація реалізації ризику виникнення загрози.

Превентивність в даному випадку досягається перш за все тим, що при подоланні перших рубежів системи захисту, за підозрілими або небезпечними ознаками візуально та\або за допомогою технічних засобів виявляється та фіксується потенційний порушник. Співробітник підрозділу охорони посилює

увагу, фокусується на спостереженні та контролі ситуації, а у разі фіксації та розвитку небезпечної поведінки порушника, час, який необхідний на дії щодо реагування та припинення реалізації небезпеки скорочується, що значно підвищує ефективність виконання особовим складом завдань за призначенням.

Також проведення оцінки (розрахунку, моделювання) можливих ризиків і втрат з використанням елементів профайлінгу, а саме створення моделі, профілю порушника, при реалізації небезпеки дає змогу оцінити необхідний мінімум та\або максимум залучених сил і засобів необхідних для забезпечення безпеки важливим об'єктам.

Для зображення раціонального використання ресурсу з впровадженням профайлінгу далі наведемо приклад забезпечення фізичної безпеки об'єкту – посадовій особі, щодо якої здійснюється охорона. При здійсненні безпекових заходів було виявлено вразливість, а саме в режимній зоні, в місці постійного перебування об'єкта, було виявлено відкриту ділянку місцевості, яка створювала потенційному порушнику умови, що несли загрозу життю та здоров'ю об'єкта охорони, про що було сповіщено відповідний підрозділ. Після аналізу ризиків відповідний підрозділ забезпечення запропонував провести комплекс інженерних та технічних безпекових заходів щодо створення захисного бар'єру відповідного рівня захисту згідно будівельних норм та галузевих стандартів України (ГСТУ 78.11.002-1999; ДСТУ 3892-99) для мінімізації рівня ризику. Загальна сума забезпечення таких заходів склала близько 62 мільйонів грн.

Водночас, при розробленні моделювання об'єкту охорони з використанням профайлінгу порушника та аналізу шкоди у разі реалізації ризику в небезпеку, було отримано дані, які свідчать, що першочергово розроблені заходи з реагування на ризик мають низьку вірогідність зниження цього ризику до необхідного мінімального рівня при одночасному витрачанні значних сил та засобів, в тому числі й бюджетних фінансових ресурсів. Таким чином, провівши експериментальне дослідження та практичну апробацію результатів вищевказаних заходів, а саме програвання сценаріїв розвитку загрози різних профілів порушника відповідно до моделі об'єкту забезпечення безпеки, було встановлено, що для мінімізації ризику достатнім є проведення комплексу фізичних, інженерних та технічних заходів, що забезпечує витрачання фінансових ресурсів у 33,7 разів менше, ніж першочергово було заявлено.

Матриця об'єкту охорони, на якому перебуває особа, яка охороняється, показала, що основна увага приділяється таким аспектам: визначення рівня захищеності об'єкту; наявність і стан системи безпеки та охорони (захисту), режимних (закритих, обмежених), відкритих зон та порядку доступу в такі зони; наявність і стан інженерних загороджень; межі зон з доступом сторонніх; межі режимних зон з доступом визначеного кола осіб, які можуть бути оцінені на безпеку/загрозу, рівень ризику; наявність сил та засобів реагування – підрозділу фізичної охорони; рівень підготовки особового складу, їхнього оснащення тощо. Також здійснювалось моделювання та оцінка інших потенційних ризиків, загроз, розмір завданої шкоди у разі синергії ризиків і загроз.

При оцінюванні антропогенних небезпек (загроз), основну увагу було приділено профілю порушника як основному джерелу виникнення ризику, що в

процесі розвитку становив загрозу життю і здоров'ю особи, щодо якої впроваджувались заходи з забезпечення фізичної безпеки, тобто небезпека стосувалась фактично існування об'єкта охорони.

Основну увагу було зосереджено на наступних складових елементах профілю порушника:

– тип порушника (терорист, вбивця-найманець, диверсант тощо);

– мотиви (економічні, релігійні, особисті тощо);

– загальна модель небезпечної поведінки («суїцидальна маска», ейфорія, психічні вади, стани, розлади, окремі особливості протиправної поведінки порушника, за відсутності яких задуманий вчинок не відбудеться тощо);

– наявність знань та вмінь (освіта, життєвий чи професійний досвід, спеціальні вміння та навички тощо);

– обізнаність щодо об'єкту охорони (захисту) (знання об'єкту, способи отримання закритої інформації про об'єкт, наявність інформатора з середовища тощо);

– оснащеність порушника (наявність озброєння, техніки, приладдя тощо);

– ймовірна тактика дій при реалізації небезпеки;

– стійкий психоемоційний стан порушника (низька тривожність, холодність, агресія, беземоційність тощо);

– ознаки порушника (беземоційність у терориста-смертника, агресія у збудливого порушника, наявність сп'яніння тощо);

– загальний візуальний опис портрету порушника (наприклад: чоловік або жінка віком від 20 до 40 років, має гарну фізичну підготовку, з релігійними та особистими мотивами помсти; має спеціальні знання та вміння з вогневої підготовки, використовує холодну та\або вогнепальну зброю, вибухівку, а серед гардеробу переважають речі на 1-2 розміри більші від реального (за такими речами можна сховати вибухівку, зброю для здійснення злочину); емоції переважно відсутні, проте, в момент здійснення небезпечної дії, або при контакті з представниками сфери безпеки та правопорядку на обличчі можуть одночасно проявлятись емоції «злочинної трійки» (гнів + презирство + відраза) або ознаки стресу, страху; при здійсненні нападу буде вести себе зухвало, з використанням елементів несподіванки; може перебувати під дією стимуляторів або наркотичних речовин тощо).

В ході вивчення методичних настанов та наукових праць фахівців з безпеки, ми виявили, що існує велика кількість видів будови систем та структур фізичної безпеки [1, 2, 12, 19, 20, 21]. Проте, не зважаючи на існуюче розмаїття підходів, такі системи повинні вирішувати завдання з попередження, недопущення, виявлення, припинення (локалізації) реалізації небезпеки щодо об'єкту забезпечення безпеки (ОЗБ). Вказані завдання вирішуються шляхом побудови системи безпеки, яка містила б в собі фіксовані за послідовністю та місцем межі, які повинна подолати загроза в процесі її безпосереднього виникнення та реалізації небезпеки.

Відповідно до розробленої нами схеми, де особа порушника (людини) визначена як основний вид антропогенної загрози, ефективна система рубежів захисту (охорони) складається з наступних елементів:

1. Рубіж стримування повинен стримати особу (антропогенний ризик) від дій, що створюють небезпеку для об'єкту охорони (наприклад, «Статут гарні-

зонної та вартової служби» ЗС України (п.1.2 додатку 4) рекомендує попереджати сторонніх осіб інформаційними табличками зупиняючого, регулюючого чи заборонного характеру, що в свою чергу несе стримуючий ефект, а їхнє ігнорування потенційним порушником виявляє його заздалегідь) [14, с. 307];

2. Інформаційний рубіж повинен виявити та ідентифікувати ризик та\або небезпеку, та сповістити кінцевий елемент (співробітника), що буде реагувати – локалізувати, припиняти розвиток небезпеки тощо;

3. Інженерно-технічний рубіж повинен зупинити, затримати чи уповільнити розвиток небезпеки (наприклад, просування порушника шляхом встановлення інженерного загородження, паркану, турнікету, систем контролю доступу тощо);

4. Адміністративно-правовий рубіж створює необхідні можливості для реагування, локалізації та мінімізації наслідків у разі реалізації небезпеки (створення регулюючих нормативно-правових документів, що надають права співробітникам охорони та\або стримують у правах сторонніх осіб – інструкції, регламенти, порядки застосування сили, спеціальних засобів тощо);

5. Фізичний рубіж зупиняє загрозу шляхом здійснення фізичного реагування та вживання всіх необхідних заходів щодо припинення, локалізації розвитку чи мінімізації втрат (збитків) у разі розвитку небезпеки (співробітник підрозділу охорони, озброєння, спеціальна техніка, керовані засоби тощо).

Якщо таку систему візуалізувати, то схематично вибудований комплекс системи фізичного захисту буде мати наступний вид (рис. 1).

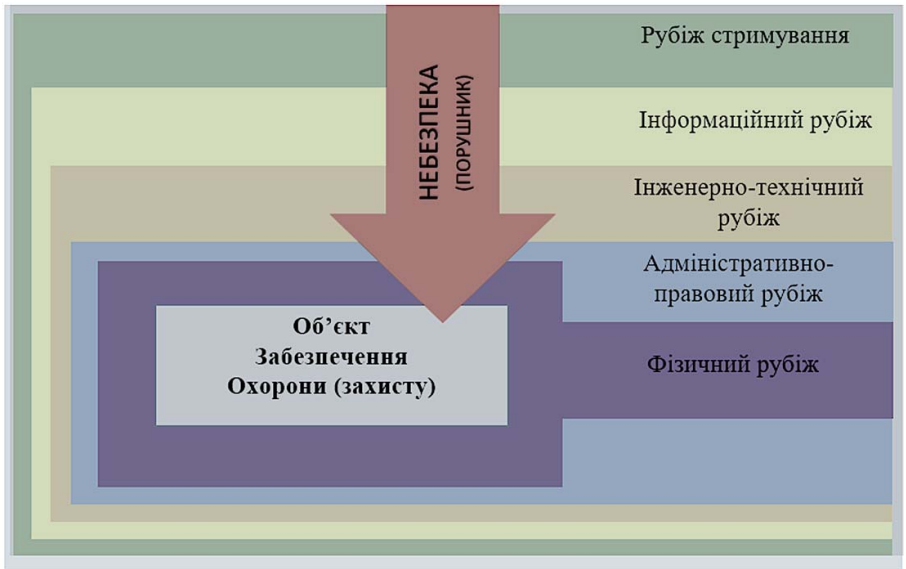

Рисунок 1. Схема побудови системи забезпечення фізичної безпеки об'єкту забезпечення охорони (захисту) з використанням багаторубіжної системи захисту

Figure 1. Scheme of building a physical security system for a security (protection) object using a multi-barrier protection system

Висновки та перспективи подальших досліджень. Таким чином, використовуючи профайлінг в комплексі безпекових заходів на важливих об'єктах, створюються сприятливі умови для ефективного виконання співробітниками охорони завдань за призначенням. Такими завданнями є виявлення, оцінка та реагування на ризики антропогенної групи шляхом ідентифікації потенційних чи реальних порушників та швидкого обрання найбільш ефективних стратегій щодо попередження чи припинення розвитку небезпеки та\або мінімізації негативних наслідків.

Фактично, можна зазначити, що використання профайлінгу дозволяє на 35% підвищити ефективність виявлення ризиків антропогенної групи, на 20% поліпшити релевантну оцінку та на 25% пришвидшити реагування на відповідні загрози.

В процесі організації заходів із забезпечення фізичного захисту, а саме моделювання профілю особи порушника та його оцінки, виникають умови щодо підвищення ефективності комплексного забезпечення безпеки об'єкту, шляхом навчання, перепідготовки кінцевих виконавців в системі захисту об'єкта – фізичного рубіжу, який уособлює собою співробітників фізичної безпеки.

Для швидкої оцінки та максимально точної верифікації моделі профілю особи, яка може становити потенційну небезпеку рекомендується створити практично-навчальний комплекс. Окрім програм тренінгів та навчання доцільно розробити програмне забезпечення, яке зможе працювати в якості віртуального тренажера на мобільних пристроях.

Також, можна зазначити, що додатково для підвищення ефективності процесу використання профайлінгу співробітниками відповідних служб доцільно використовувати засоби автоматичної фіксації та розпізнавання небезпек. Це дозволить на 40% збільшити вірогідність релевантної оцінки моделі поведінки потенційного порушника та оптимізує систему використання ресурсів всіх видів.

Практична апробація механізмів профайлінгу може дозволити вирішувати завдання з раціонального використання сил та засобів в ході побудови як загальної систем фізичної безпеки, так і її окремих елементів, а не тільки вирішувати завдання кінцевим виконавцем з поточного моніторингу, виявлення, ідентифікації, припинення та\або локалізації розвитку небезпеки чи заходів мінімізації завданих втрат у разі її реалізації.

Підсумовуючи все вищезазначене, ми можемо стверджувати, що профайлінг займає важливу роль в практично-прикладних процесах з організації безпекового середовища об'єкта забезпечення фізичної безпеки, в тому числі й об'єктів критичної інфраструктури в умовах воєнного стану. Адаптація та інтегрування методів профайлінгу порушника в практичну діяльність на різних рівнях управління (тактичний рівень – працівники підрозділів охорони (захисту); оперативний та стратегічний рівні – середня та вища управлінська ланка) дозволить підвищити ефективність виконання завдань за призначенням в частині забезпечення фізичного захисту об'єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3 (40). С. 77–86.

2. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній 266 інфраструктурі. *Стратегічні пріоритети. Серія: Економіка*. 2015. № 4 (37). С. 83 – 93.

3. Генеральний секретар НАТО обговорив захист критичної підводної інфраструктури, підтримку України з міністрами оборони країн ЄС. URL: http:www.nato.int/cps/uk/natohq/news_220058.htm (дата звернення 29.04.2024).

4. Гордонов В.П., Сухонько С.М. Методика оцінювання вразливості системи фізичного захисту ядерної установки від нападу озброєних злочинців. Честь і закон. *2018,№ 4(67)*. URL: https://typeset.io/pdf/metodika-otsiniuvannia-vrazlivosti-sistemi-fizichnogo-jhadome8cy.pdf

5. Громовенко К. В. Захист критично важливих об'єктів інфраструктури в контексті міжнародного миру та безпеки. *Юридичний науковий електронний журнал*. 2021. № 9. С. 329-331.

6. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ, 2020. 28 с. URL: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastructury_0.pdf (дата звернення 29.04.2024).

7. ЄС і НАТО представили рекомендації для захисту критичної інфраструктури. *Європейська правда*. URL: http: //www.eurointegration.com.ua/ news/2023/06/29/7164693/ (дата звернення 29.04.2024)

8. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 21.06.2024 р. URL: http://zakon.rada.gov.ua/laws/show/1882-IX#Text (дата звернення 29.04.2024)

9. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Дата оновлення: 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-VIII#Text (дата звернення 29.04.2024).

10. Оніщенко Ю.М., Чукалов К.Е., Синжерян А.А. Щодо захисту об'єктів критичної інфраструктури в Україні. *The 12th International scientific and practical conference "Scientific research in the modern world"*: Toronto, Sep. 21-23, 2023. Toronto, 2023. P. 258-266. URL: https://univd.edu.ua/science-issue/issue/6890 (дата звернення 29.04.2024).

11. Портал української мови. *Словник*. URL: https://slovnyk.ua/index.php?swrd=%D0%BF%D0%BE%D1%80%D1%83%D1%88%D0%BD%D0%B8%D0%BA#:~:text=%D0%A2%D0%BB%D1%83%D0%BC%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%96%D0%B7%20%22%D0%A1%D0%BB%D0%BE%D0%B2%D0%BD%D0%B8%D0%BA%D0%B0%20%D1%83%D0%BA%D1%80%D0%B0%D1 (дата звернення 29.04.2024).

12. Правила фізичного захисту ядерних установок та ядерних матеріалів (НП 306.8.126-2006): затв. наказом Держатомрегулювання України від 04.08.2006 р. № 116, зареєстр. Мін'юстом від 21.09.2006 р. за № 1067/12941. URL: https://zakon.rada.gov.ua/laws/show/z1067-06#Text.

13. Пригунов П. Я., Янчук А. О., Карпова К. В. Концептуальні підходи до формування сучасного нормативно-правового забезпечення діяльності підрозділів безпеки суб'єктів господарської діяльності. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2016. №1 (48). С. 61-71.

14. Статути збройних сил України: збірник законів: чинне законодавство із змінами та допов. на 05 вересня 2023 року: оф. тексти. Київ, 2023. 436 с.

15. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики. *Стратегічні пріоритети*. 2016. № 3 (40). С. 62 – 75.

16. Тихоненко О. О. Стан профайлінгу в сфері забезпечення державної безпеки, на прикладі емпіричного дослідження. *Публічне управління і адміністрування в Україні*. 2020. № 18. С. 119-124.

17. Тихоненко О.О. Механізми профайлінгу в сфері виявлення загроз в державній безпеці : дис. … канд. наук з держ. упр. : 25.00.05. Харків, 2021. 287 с.

18. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпекова діяльність: системний підхід. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2017. № 1. С. 154–163.

19. Bennett, H.A. EASI approach to physical security evaluation. USA, 1977. 35 p.

20. Convention on the Physical Protection of Nuclear Material. *IAEA. Legal Series.* Vienna, 1982. № 12. P. 386.

21. Franchuk V., Pryhunov P., Melnyk S. Safety of Critical Infrastructure Facilities in Ukraine: Organizational and Regulatory Problems and Approaches. *Social and Legal Studios*. 2021. № 4(3), P. 142-148. URL: https://doi.org/10.32518/2617-4162-2021-3-142-148 (дата звернення 29.04.2024).

22. Woodhouse B., Petherick W. Metacognition in criminal profiling. *Profiling and Serial Crime (Third Edition): Theoretical and Practical Issues*. 2014. №3. P. 185–206. DOI: 10.1016/B978-1-4557-3174-9.00010-0.

Стаття надійшла до редакції 30.04.2024
Стаття рекомендована до друку 20.05.2024

Sergiy Lukin, Doctor of Science in Public Administration, Associate Professor,
Director of the Regional Centre for Advanced Training in Kyiv Region,
Lesia Ukrainka Square, 1, Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0001-6516-5605 e-mail: serge.lukin77@gmail.com

Oleksandr Tikhonenko, PhD in Public Administration,
Lecturer at the Regional Centre for Advanced Training of Kyiv Region,
Lesia Ukrainka Square, 1, Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0002-5140-3737 e-mail: tikhonenko4mail@gmail.com

APPLICATION OF PROFILING IN SECURITY SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

Abstract. The article offers the author's vision of the possibility and effectiveness of applying modern scientific methods in systems for ensuring the safety of important objects of various forms of ownership, including objects of critical infrastructure. The purpose of this article is to continue the study of profiling mechanisms in the field of identifying threats to state security. This field is especially critical in the context of global geopolitical changes that become prerequisites for increasing military, criminal, terrorist and other threats. The author also considers the concept of safety as a state and process and highlights the actual need for finding and developing effective practical methods to achieve such a state. Profiling as a method for predicting the behavior of the anthropogenic type of threats to the offender and related events is an essential practical tool in the arsenal of the ultimate executor — the security officer. The article examines the theoretical and practical basis of implementation in practical processes of ensuring the security of an object of critical infrastructure in conditions of increased military risks. The author considers ways of integrating profiling with other technologies for ensuring physical security, including modern video surveillance systems,

access control and management, artificial intelligence and others. It is shown that effective provision of physical security requires not only modern equipment of security systems and high qualification of end performers — employees able to respond quickly to threats. But also the creation of a certain environment in which the use of such equipment and employees will have the most productive level, while attracting the minimum necessary resources. On the basis of the conducted studies, it is concluded that it is necessary to develop a unified methodology and standards and protocols for the use of profiling in the construction of physical security systems for critical infrastructure facilities. This will increase the efficiency of detection and prevention of threats, minimize the level of risks to the civilian population, and ensure the stable functioning of critical facilities. Even in conditions of military instability, rational use of resources, forces, and means. Prospects for further research in the field of profiling and its integration with promising technologies aimed at improving the level of state security are considered.

Keywords: *profiling, national security, public administration, critical infrastructure*.

In cites: Lukin, S. Yu., & Tikhonenko, O. O. (2024). Application of Profiling in Security Systems of Critical Infrastructure Objects. *Theory and Practice of Public Administration*, 1 (78), 168–182. http://doi.org/10.26565/1727-6667-2024-1-10 [in Ukrainian].

REFERENCES:

1. Bobro, D.G. (2016). Methodology for assessing the level of criticality of infrastructure objects. *Strategic priorities,* 3 (40), 77-86 [in Ukrainian].
2. Bobro, D.G. (2015). Determination of criteria for assessing and threats to critical 266 infrastructure. *Strategic priorities*. *Series: Economics,* 4 (37), 83-93 [in Ukrainian].
3. NATO Secretary General discusses protection of critical underwater infrastructure, support for Ukraine with EU defence ministers. URL: http: www.nato.int/cps/uk/natohq/news_220058.htm [in Ukrainian] (accessed 29.04.2024).
4. Gordonov, V.P., & Sukhonko, S.M. (2018). Methodology for Assessing the Vulnerability of the Physical Protection System of a Nuclear Installation from an Armed Criminal Attack. *Honour and Law,* 4 (67). URL: https://typeset.io/pdf/metodika-otsiniuvannia-vrazlivosti-sistemi-fizichnogo-jhadome8cy.pdf [in Ukrainian] (accessed 29.04.2024).
5. Protection of Critical Infrastructure Objects in the Context of International Peace and Security (2021). *Legal scientific electronic journal,* 9, 329-331 [in Ukrainian].
6. State system of critical infrastructure protection in the system of national security: analytical supplement (2020) / edited by O. Sukhodola. Kyiv, 28. URL: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastructury_0.pdf [in Ukrainian] (accessed 29.04.2024).
7. The EU and NATO presented recommendations for the protection of critical infrastructure. *Yevropeiska pravda*. URL: http: //www.eurointegration.com.ua/news/2023/06/29/7164693/ [in Ukrainian] (accessed 29.04.2024).
8. On critical infrastructure: Law of Ukraine No. 1882-IX (2021, November 16). URL: http://zakon.rada.gov.ua/laws/show/1882-IX#Text [in Ukrainian] (accessed 29.04.2024).
9. On National Security of Ukraine: Law of Ukraine No. 2469-VIII (2018, June 26). URL: https://zakon.rada.gov.ua/laws/show/2469-VIII#Text [in Ukrainian] (accessed 29.04.2024).
10. Onishchenko, Y.M., Chukalov, K.E., & Synzherian, A.A. (2023). On the protection

of critical infrastructure facilities in Ukraine. *The 12th International scientific and practical conference 'Scientific research in the modern world'*: Toronto, Sep. 21-23, 258-266. URL: https://univd.edu.ua/science-issue/issue/6890 [in Ukrainian] (accessed 29.04.2024)

11. Portal of the Ukrainian language. *Dictionary.* URL: https://slovnyk.ua/index.php?swrd=%D0%BF%D0%BE%D1%80%D1%83%D1%88%D0%BD%D0%B8%D0%BA#:~:text=%D0%A2%D0%BB%D1%83%D0%BC%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%96%D0%B7%20%22%D0%A1%D0%BB%D0%BE%D0%B2%D0%BD%D0%B8%D0%BA%D0%B0%20%D1%83%D0%BA%D1%80%D0%B0%D1 [in Ukrainian] (accessed 29.04.2024).

12. Rules for Physical Protection of Nuclear Facilities and Nuclear Materials (NP 306.8.126-2006): Approved by Order of the SNRIU of 04.08.2006, No. 116, registered by the Ministry of Justice of 21.09.2006. Ministry of Justice of 21.09.2006, No. 1067/12941. URL: https://zakon.rada.gov.ua/laws/show/z1067-06#Text [in Ukrainian] (accessed 29.04.2024).

13. Pryhunov, P. Y., Yanchuk, A. O., & Karpova, K. V. (2016). Conceptual approaches to the formation of modern regulatory and legal support for the activities of security units of business entities. *Scientific works of the Interregional Academy of Personnel Management. Legal sciences,* 1 (48), 61-71 [in Ukrainian].

14. Statutes of the Armed Forces of Ukraine: a collection of laws: current legislation as amended and supplemented as of 05 September 2023: official texts. Kyiv, 436 [in Ukrainian].

15. Protection of critical infrastructure in a hybrid war: problems and priorities of state policy (2016). *Strategic priorities,* 3 (40), 62-75 [in Ukrainian].

16. The state of profiling in the field of state security, on the example of an empirical study (2020). *Public management and administration in Ukraine,* 18, 119-124 [in Ukrainian].

17. Tikhonenko, O. (2021). Mechanisms of profiling in the field of identifying threats to state security: PhD in Public Administration: 25.00.05. Kharkiv, 287 [in Ukrainian].

18. Security activity: a systematic approach (2017). *Scientific Bulletin of Lviv State University of Internal Affairs. Economic Series,* 1, 154-163 [in Ukrainian].

19. Bennett, H.A. (1977). EASI approach to physical security evaluation. USA, 35 [in English].

20. Convention on the Physical Protection of Nuclear Material (1982). IAEA. *Legal Series.* Vienna, 12, 386 [in English].

21. Franchuk, V., Pryhunov, P., & Melnyk, S. (2021). Safety of Critical Infrastructure Facilities in Ukraine: Organizational and Regulatory Problems and Approaches. *Social and Legal Studios,* 4 (3), 142-148. DOI: https://doi.org/10.32518/2617-4162-2021-3-142-148 (date of application 29.04.2024) [in English].

22. Woodhouse, B., & Petherick, W. (2014). Metacognition in criminal profiling. *Profiling and Serial Crime (Third Edition): Theoretical and Practical Issues*, 3, 185–206. DOI: 10.1016/B978-1-4557-3174-9.00010-0 [in English].

The article was received by the editors 30.04.2024
The article is recommended for printing 20.05.2024