УДК 004.056.5:343.326
DOI https://doi.org/10.51989/NUL.2024.5.10

УДОСКОНАЛЕННЯ КООРДИНАЦІЇ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Федорченко Олександр Сергійович,
orcid.org/0009-0007-7358-7753
молодший науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України

У статті висвітлено проблеми координації діяльності суб'єктів забезпечення національної системи кібербезпеки. Аналізуються законодавчі акти України у сфері забезпечення кібербезпеки. У контексті взаємодії суб'єктів забезпечення національної системи кібербезпеки звертається увага на пріоритети забезпечення кібербезпеки, які викладені у Стратегії кібербезпеки України та інших стратегічних документах. У досліджуваному аспекті визначаються основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Проаналізовано наявні системи забезпечення захисту об'єктів критичної інфраструктури, серед яких виділяється: національна системи забезпечення кібербезпеки; єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків; державна система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання. Розкрито зміст кожної із системи та визначено коло уповноважених, визначених відповідальними за координацію діяльності суб'єктів сектору безпеки й оборони в кожній системі. Виявлено проблеми міжвідомчої координації такої діяльності на рівні реалізації державної політики забезпечення кібербезпеки. Встановлено ризики дублювання повноважень уповноважених суб'єктів щодо координації діяльності інших суб'єктів забезпечення національної системи кібербезпеки. Зроблено висновок про доцільність визначити єдиний уповноважений орган для координації діяльності суб'єктів національної системи захисту критичної інфраструктури, у межах якого слід утворити підрозділи, відповідальні за координацію окремих секторів критичної інфраструктури.

Ключові слова: *законодавство, кібербезпека, координація суб'єктів національної системи кібербезпеки, об'єкти критичної інфраструктури, суб'єкти національної системи кібербезпеки, удосконалення.*

Fedorchenko Oleksandr. Improvement of coordination of activities of entities providing the national cyber security system

The article highlights the problems of coordinating the activities of the subjects of ensuring the national cyber security system. Legislative acts in the field of cyber security are analyzed. In the context of the interaction of the subjects of ensuring the national cyber security system, attention is drawn to the priorities of ensuring cyber security outlined in the Cyber Security Strategy of Ukraine. In the studied aspect, the main goals, directions and principles of state policy in the field of cyber security, the powers of state bodies, the main principles of coordination of their activities to ensure cyber security are defined. The content of each of the systems is revealed and the circle of authorized persons determined to be responsible for the coordination of the activities of the subjects of the security and defense sector in each system is defined. The problems of interdepartmental coordination of such activities at the level of implementation of the state policy of ensuring cyber security have been identified. It is noted that the modern system of coordination and interaction of subjects of the national critical infrastructure protection system needs improvement from the point of view of centralization of the state policy of critical infrastructure protection. It was concluded that it is expedient to define a single authorized body for the coordination of the activities of the subjects of the national system of critical infrastructure protection, within which units responsible for the coordination of individual sectors of critical infrastructure should be formed.

Key words: *legislation, cyber security, improvement, coordination of subjects of the national cyber security system, critical infrastructure objects, subjects of the national cyber security system.*

Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96, визнає забезпечення кібербезпеки одним із найважливіших пріоритетів у системі національної безпеки України [1].

У розділі 2 цієї Стратегії міститься аналіз ефективності стану реалізації попередньої Стратегії кібербезпеки України, де, зокрема, зазначається, що «діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань… Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки» [1]. Незважаючи на розбудову національної системи кібербезпеки та значний масив прийнятих протягом останнього часу нормативно-правових актів з питань забезпечення кібербезпеки, проблема координації суб'єктів забезпечення цієї системи залишається актуальною і сьогодні.

Різні аспекти діяльності суб'єктів забезпечення національної системи кібербезпеки висвітлювалися в роботах В. В. Бухарєва [2], І. А. Білан [3], С. А. Краснікова, Я. О. Страхніцького [4], А. В. Тарасюка [5], Т. Ю. Ткачука [6] та ін. Водночас проблема вдосконалення координації діяльності цих суб'єктів окремо не розглядалася в цих роботах. Ця проблема загострюється в умовах правового режиму воєнного стану, де злагоджена робота суб'єктів забезпечення національної системи кібербезпеки є важливою передумовою протидії кібератак та інших кіберінцидентів. Також важливим є дослідження позитивного зарубіжного досвід у цій сфері з метою його запозичення в національне законодавство та соціальну практику.

Метою статті є удосконалення координації діяльності суб'єктів забезпечення національної системи на підставі аналізу чинного законодавства з питань забезпечення кібербезпеки України.

Стратегія забезпечення державної безпеки серед пріоритетних напрямів державної політики у сфері забезпечення державної безпеки виділяє розмежування повноважень і завдань між суб'єктами сектору безпеки й оборони, удосконалення взаємодії та координації дій між ними, а також з іншими державними органами (п. 23). При цьому оптимізація координації таких суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі визнається одним з основних завдань державної політики у сфері забезпечення державної безпеки (п. 24) [7].

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівнях, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС і держав – членів НАТО [1].

У цій Стратегії заслуговують на увагу чинники інституційного характеру, які зумовлюють кіберзагрози. До таких чинників Стратегія обґрунтовано відносить: відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом; відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки [1]. З іншого боку, серед чинників, які зумовлюють кіберзагрози, згадується недосконалість нормативно-правової бази у сфері кібербезпеки.

Наведене свідчить про потребу в удосконаленні механізмів координації діяльності суб'єктів національної системи кібербезпеки. Не випадково вдосконалення взаємодії цих суб'єктів є однією зі стратегічних цілей згаданої Стратегії.

Ціль В.1 цієї Стратегії «Зміцнення системи координації» звучить так: «Україна створить умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів, скоординує діяльність усіх заінтересованих сторін задля подолання надзвичайних (кризових) ситуацій у кіберпросторі» [1].

Для системного захисту України від загроз національній безпеці Стратегія

національної безпеки України «БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА УКРАЇНИ» (затверджена Указом Президента України від 14 вересня 2020 року № 392/2020) визначає за потрібне створення системи ефективного управління та координації діяльності органів сектору безпеки й оборони, що вдосконалить її архітектуру (п. 63) [8].

Згідно з ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [9] національна система кібербезпеки – «це сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [9].

Ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» визначає систему суб'єктів забезпечення кібербезпеки, серед яких виділяються: 1) міністерства й інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи й організації, віднесені до об'єктів критичної інфраструктури; 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [9]. Слід погодитися з позицією І. Тімкіна, що система забезпечення національної безпеки виступає як організаційна система державних і недержавних інституцій, інших суб'єктів, покликаних вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб [10].

У межах своєї компетенції суб'єкти забезпечення кібербезпеки здійснюють: заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення й реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційний обмін щодо реалізованих і потенційних кіберзагроз; розробку й реалізацію запобіжних, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; проведення аудиту інформаційної безпеки, у т. ч. на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; інші заходи із забезпечення розвитку та безпеки кіберпростору [9].

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України (ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України») [9].

Для злагодженої роботи таких суб'єктів потрібна координація їхньої діяльності у сфері кібербезпеки. Згідно з ч. 1 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» така координація як складова національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Глава держави її здійснює через Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України [9]. Цей центр здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України [9].

Водночас окремі функції координації у цій сфері забезпечують деякі правоохоронні органи й органи виконавчої влади із спеціальним статусом, які опікуються реалізацією державної політики у сфері захисту критичної інфраструктури відповідно до положень згаданого Закону.

Державна служба спеціального зв'язку та захисту інформації України, зокрема, координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA [9].

Служба безпеки України, зі свого боку, здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру й безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні й оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом і кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки (п. 3 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України») [9].

Із цього приводу слід погодитися з А. Тарасюком, який вважає, що відповідні законодавчі новації з питань забезпечення кібербезпеки зумовлюють ризик взаємного дублювання повноважень Центру кібербезпеки, СБУ та Державної служби спеціального зв'язку та захисту інформації України [5, с. 123]. Вважаємо, що це є однією з причин удосконалення механізмів міжвідомчої координації у сфері забезпечення кібербезпеки.

Водночас існують інші сфери захисту критичної інфраструктури, де координація діяльності суб'єктів сектору безпеки й оборони грає не менш важливу роль у контексті забезпечення безпеки об'єктів критичної інфраструктури.

Так, Рада національної безпеки та оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України. РНБО України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони (ч. 1 ст. 107 Конституції України) [11]. Цей орган може подавати Президенту свої пропозиції, що стосуються важливих стратегічних питань із захисту критичної інфраструктури, і приймає відповідні рішення [12].

Поряд із національною системою забезпечення кібербезпеки функціонує Єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків, у межах якої здійснюється: реагування на акти кібертероризму, усунення їх причин і умов, мінімізація суспільно небезпечних наслідків; забезпечення антитерористичного захисту об'єктів можливих терористичних посягань. Система суб'єктів боротьби з тероризмом визначена ст. 4 Закону України «Про боротьбу з тероризмом, а головним органом у загальнодержавній системі боротьби з терористичною діяльністю є СБУ (ч. 4 ст. 4 Закону України «Про боротьбу з тероризмом») [13]. До суб'єктів, які безпосередню здійснюють боротьбу з тероризмом, належать: Міністерство внутрішніх справ України; Національна поліція; Міністерство оборони України; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику у сфері цивільного захисту; центральний орган виконавчої влади, що реалізує державну політику у сфері захисту державного кордону; центральний орган виконавчої влади, що реалізує державну політику у сфері виконання кримінальних покарань; Управління державної охорони України; Збройні Сили України [13].

До компетенції цих суб'єктів віднесено запобігання терористичної діяльності на об'єктах можливих терористичних посягань, у т. ч. забезпечення захисту від терористичних посягань об'єктів Збройних Сил України, об'єктів, охорону яких доручено Управлінню державної охорони України, та інших особливо важливих об'єктів критичної інфраструктури.

Координацію діяльності суб'єктів, які залучаються до боротьби з тероризмом, здійснює Антитерористичний центр при Службі безпеки України, а суб'єкти боротьби з тероризмом надають йому необхідні сили й засоби, забезпечують їх

ефективне використання під час проведення антитерористичних операцій (ст. 5 Закону України «Про боротьбу з тероризмом») [13].

Відповідно до п. 1 Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України, затвердженого Указом Президента України від 14 квітня 1999 року № 379, АТЦ при СБУ здійснює координацію діяльності суб'єктів боротьби з тероризмом у запобіганні терористичним актам щодо державних діячів, критичних об'єктів життєзабезпечення населення, об'єктів підвищеної небезпеки, актам, що загрожують життю і здоров'ю значної кількості людей, та їх припиненні [14].

Координуючі та контрольні функції цього органу з питань ефективності здійснення заходів із забезпечення антитерористичної захищеності об'єктів передбачені у Правилах антитерористичної безпеки (затверджені постановою Кабінету Міністрів України від 15 жовтня 2024 р. № 1172) [15].

Крім названих систем захисту об'єктів критичної інфраструктури, існує державна система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання, у межах якої здійснюються заходи з протидії кібердиверсій, кіберінцидентів на об'єктах фізичного захисту. Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання визначена як «сукупність організаційно-правових та інженерно-технічних заходів, що здійснюються з метою створення умов, спрямованих на мінімізацію можливості вчинення диверсії, крадіжки або будь-якого іншого неправомірного вилучення радіоактивних матеріалів та зміцнення режиму нерозповсюдження ядерної зброї» [16].

До об'єктів державної системи фізичного захисту належать ядерні об'єкти й установки, призначені для поводження з радіоактивними відходами, радіоактивні відходи, ядерні матеріали, радіоактивні матеріали, виявлені в незаконному обігу, інші джерела іонізуючого випромінювання (п. 3 Порядку функціонування державної системи фізичного захисту, затвердженого постановою Кабінету Міністрів України від 21 грудня 2011 р. № 1337) [17].

До суб'єктів державної системи фізичного захисту віднесено: орган державного регулювання ядерної та радіаційної безпеки; центральні органи виконавчої влади, які здійснюють державне управління, та Національна академія наук України щодо фізичного захисту; Служба безпеки України; Національна гвардія України; центральні органи виконавчої влади, які провадять правоохоронну діяльність [16].

Відповідно до Порядку функціонування державної системи фізичного захисту, затвердженого постановою Кабінету Міністрів України від 21 грудня 2011 р. № 1337, Держатомрегулювання як уповноважений орган в межах компетенції: координує діяльність інших суб'єктів системи щодо підвищення рівня культури захищеності; бере участь у формуванні державної політики у сфері фізичного захисту, а також розробляє механізм реалізації зазначеної державної політики [17].

Водночас СБУ в межах наданих їй повноважень координує діяльність інших державних органів під час проведення оцінки проєктної загрози [17]. Отже, у державній системі фізичного захисту функціонує кілька державних органів, які здійснюють координацію інших суб'єктів цієї системи. На нашу думку, наявність на законодавчому рівні кількох систем забезпечення захисту об'єктів критичної інфраструктури, з уповноваженими органами, відповідальними за координацію діяльності відповідних суб'єктів у кожній із систем, зумовлюють ризик взаємного дублювання їх повноважень. Отже, механізм координації системи суб'єктів забезпечення кібербезпеки потребує подальшого розвитку й удосконалення. Ми солідарні із думкою І. Білан, яка вважає, що «досягненню стратегічних цілей у сфері забезпечення кібербезпеки сприятиме: відпрацювання механізму надання відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки інформації про кібератаки, кіберінциденти; визначення переліку питань, що підлягають обміну такою інформацією

між усіма суб'єктами забезпечення кібербезпеки на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікація форматів обміну інформацією; залучення до вирішення завдань у цій сфері суб'єктів господарювання, громадських об'єднань та окремих громадян України» [3, с. 192].

Аналіз законодавства України у сфері забезпечення кібербезпеки свідчить про розгалужену систему суб'єктів забезпечення кібербезпеки. Сучасні прояви кібердиверсії, кібертероризму, інших кіберінцидентів загрожують багатьом об'єктам критичної інфраструктури, захист яких відбувається в межах різних державних систем.

Сьогодні в Україні існує кілька не пов'язаних між собою систем захисту об'єктів критичної інфраструктури: національна системи забезпечення кібербезпеки; єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків; державна система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання. У межах кожної з наведених систем виділяється визначене коло суб'єктів, відповідальних за координацію діяльності інших суб'єктів забезпечення захисту об'єктів критичної інфраструктури. З огляду на значну кількість таких суб'єктів, які одночасно функціонують у різних системах захисту об'єктів критичної інфраструктури, існують ризики дублювання їх повноважень, що знижує ефективність їх узгодженої взаємодії та ускладнює міжвідомчу координацію у цій сфері.

Сучасна система координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури потребує удосконалення з погляду централізації державної політики захисту такої інфраструктури. Вважаємо за доцільне визначити єдиний уповноважений орган для координації діяльності суб'єктів національної системи захисту критичної інфраструктури, у межах якого слід утворити підрозділи, відповідальні за координацію окремих секторів критичної інфраструктури. Удосконаленню координації діяльності таких суб'єктів сприяє розвиток державно-приватного партнерства у сфері забезпечення кібербезпеки.

ЛІТЕРАТУРА:

1. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.21 № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.10.2024).

2. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

3. Білан І. А. Координація діяльності суб'єктів національної системи кібербезпеки. *Інноваційні наукові дослідження: теорія, методологія, практика* : матеріали VIII Міжнародної науково-практичної конференції (м. Київ, 28–29 лютого 2024 р.) / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. Запоріжжя : АА Тандем, 2024. С. 190–192.

4. Страхніцький Я. О. Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури. *Публічне управління та регіональний розвиток*. 2024. № 1 (23). С. 28–52. DOI: https://doi.org/10.34132/pard2024.23.02 (дата звернення: 30.10.2024).

5. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2020. Т. 31 (70). Ч. 2. № 2. С. 119–124. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf (дата звернення: 30.10.2024).

6. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

7. Стратегія забезпечення державної безпеки : затв. Указом Президента України від 16.02.2022 № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 30.10.2024).

8. Стратегія національної безпеки України «БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА КРАЇНИ» : затв. Указом Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.10.2024).

10. Тімкін І. Ф., Новікова Н. Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua (дата звернення: 30.10.2024).

11. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 30.10.2024).

12. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення: 30.10.2024).

13. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 30.10.2024).

14. Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України : затв. Указом Президента України від 14.04.1999 № 379. URL: https://zakon.rada.gov.ua/laws/show/379/99#Text (дата звернення: 30.10.2024).

15. Правила антитерористичної безпеки : затв. постановою Кабінету Міністрів України від 15 жовтня 2024 р. № 1172. URL: https://zakon.rada.gov.ua/laws/show/1172-2024-%D0%BF#Text (дата звернення: 30.10.2024).

16. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19.10.2000 № 2064-III. URL: https://zakon.rada.gov.ua/laws/show/2064-14#Text (дата звернення: 30.10.2024).

17. Порядок функціонування державної системи фізичного захисту : затв. постановою Кабінету Міністрів України від 21.12.2011 № 1337. URL: https://zakon.rada.gov.ua/laws/show/1337-2011-%D0%BF#Text (дата звернення: 30.10.2024).