УДК 349
DOI https://doi.org/10.32782/TNU-2707-0581/2023.2/13

Гнедюк В.Л.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АДМІНІСТРАТИВНО-ПРАВОВИЙ СТАТУС СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У статті розглядається адміністративно-правовий статус суб'єктів забезпечення кібербезпеки в Україні. Досліджено законодавчі норми та положення, які визначають статус і повноваження різних суб'єктів, що займаються захистом кіберпростору країни. Детально описано значення правових відносин у забезпеченні кібербезпеки України та окреслено коло учасників системи кібербезпеки, які забезпечують захист прав і свобод осіб у кіберпросторі згідно зі стратегією кібербезпеки країни. В статті також зазначені функції та повноваження Департаменту кіберполіції. Також описана роль Державного центру кіберзахисту та протидії кіберзагрозам у реалізації державної політики забезпечення кібербезпеки України. Центр виконує координаційні функції, спрямовані на ефективну взаємодію органів влади, операторів та провайдерів у попередженні та усуненні наслідків кіберінцидентів, а також забезпечує збір інформації про кіберінциденти та міжнародну координацію з питань кіберзахисту. Стаття закликає до перегляду інституційного механізму формування, координації та контролю за виконанням завдань забезпечення кібербезпеки, зокрема до врахування потреб усіх суб'єктів забезпечення кібербезпеки в Україні. Для досягнення цієї мети пропонується залучення не лише інституцій держави, але й бізнесу та громадського суспільства у процес формування і впровадження національної системи кібербезпеки. Стаття має важливе значення для наукового розуміння адміністративно-правового статусу суб'єктів забезпечення кібербезпеки в Україні. Вона розкриває проблеми та недоліки існуючого механізму координації та взаємодії, що потребують перегляду та удосконалення. Результати дослідження можуть бути використані як підстава для розробки та впровадження ефективної системи кібербезпеки в Україні, яка враховуватиме інтереси всіх зацікавлених суб'єктів та забезпечуватиме належний захист кіберпростору країни.

Ключові слова: *кіберпростір, Стратегія кібербезпеки, Департмаент кіберполіції, суб'єкт, кіберзлочинність, координація.*

Постановка проблеми. Актуальність адміністративно-правового статусу суб'єктів забезпечення кібербезпеки в Україні полягає в необхідності ефективного регулювання діяльності цих суб'єктів з метою забезпечення безпеки і захисту кіберпростору країни. Кіберзагрози постійно зростають, і це створює необхідність у зміцненні заходів з кібербезпеки та встановленні правових норм, що регулюють діяльність суб'єктів цієї сфери.

Забезпечення кібербезпеки є надзвичайно важливою задачею, оскільки інформаційні системи та мережі є необхідною складовою частиною сучасного суспільства та використовуються в різних сферах діяльності, включаючи державний сектор, бізнес, освіту, охорону здоров'я та особисте використання громадян.

Проблемою є недостатня гармонізація законодавства, що регулює кібербезпеку в Україні. Існують різні нормативно-правові акти, які визначають правила та вимоги щодо кібербезпеки, проте вони не завжди узгоджені та не мають єдиного підходу до визначення статусу суб'єктів забезпечення кібербезпеки. Це ускладнює роботу суб'єктів кібербезпеки, призводить до неповноцінного захисту кіберпростору та підвищує ризики кібератак.

Отже, актуалізація адміністративно-правового статусу суб'єктів забезпечення кібербезпеки в Україні має на меті вирішити цю проблему та забезпечити ефективне функціонування цієї сфери. Встановлення чіткого статусу допоможе унормувати діяльність суб'єктів, визначити їх повноваження, обов'язки та відповідальність, а також сприятиме покращенню співпраці з іншими суб'єктами правового простору, включаючи правоохоронні органи.

Аналіз останніх досліджень і публікацій. Робота ґрунтується на аналізі законодавства

України та зарубіжних країн, науково-методичної літератури, методичних посібників, наукових статей, періодичних видань та напрацювань сучасних та попередніх вчених і дослідників, серед них: С. Х. Барегамян, Т. В. Ткач, Є. І. Цифра, Л. Ю. Веселова тощо.

З основних невирішених частин проблеми адміністративно-правового статусу суб'єктів забезпечення кібербезпеки в Україні, які потрібують подальшого дослідження, можна виділити: недостатню координацію, потребу у скоординованому регулюванні, залучення бізнесу та громадського суспільства, підвищення освіти та свідомості.

Метою статті є аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки в Україні, визначення їх повноважень та ролі в системі кібербезпеки. Стаття також спрямована на виявлення проблем і недоліків існуючого механізму координації та взаємодії в цій сфері, а також пропонує шляхи поліпшення та розвитку національної системи кібербезпеки, залучаючи різні зацікавлені сторони, такі як державні органи, бізнес і громадське суспільство.

Виклад основного матеріалу. Правові відносини виступають як основний механізм управління суспільними відносинами за допомогою правових норм. Вони забезпечують виконання правових норм і включають в себе встановлення загальних правил поведінки, визначення суб'єктів, їх правового статусу, взаємних прав та обов'язків, а також заходів відповідальності за порушення правил. Однак, саме існування правових норм не призводить автоматично до виникнення правових відносин. Вони виникають лише в разі наявності обставин, передбачених відповідними нормами права. Тому важливим завданням при розробці моделі забезпечення кібербезпеки України є забезпечення можливості суб'єктів права стати учасниками правових відносин в сфері кібербезпеки і надання їм відповідної компетенції [9, с. 16].

Один з перших офіційних актів, який визначив систему суб'єктів забезпечення кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». В цьому документі було вперше використано термін «національна система кібербезпеки». Основними учасниками цієї системи є органи інформаційної безпеки, які забезпечують захист прав і свобод осіб у кіберпросторі. Згідно з главою 3 Стратегії, головними суб'єктами забезпечення кібербезпеки є Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, які можуть бути покладені спеціальні завдання відповідно до закону [3].

Інший перелік суб'єктів закріплено у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якої до основних суб'єктів забезпечення кібербезпеки віднесено: Раду національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, розвідувальні органи, тощо [8, с. 89]. Згідно зі статтею 5 Закону України «Про основні засади забезпечення кібербезпеки України», суб'єктами, які безпосередньо здійснюють заходи з забезпечення кібербезпеки в рамках своєї компетенції, є наступні:

– міністерства та інші центральні органи виконавчої влади;
– місцеві державні адміністрації;
– органи місцевого самоврядування;
– правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
– Збройні Сили України, інші військові формування, утворені відповідно до закону;
– Національний банк України;
– підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
– 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 [2].

Законом України «Про основні засади забезпечення кібербезпеки України» визначена загальна система суб'єктів забезпечення кібербезпеки. Кожен учасник правових відносин у сфері кібербезпеки має власні повноваження, які допомагають йому здійснювати свою діяльність і вживати заходів для підтримки належного стану кібербезпеки. Адміністративно-правовий статус кожного суб'єкта забезпечення кібербезпеки є індивідуальним і характеризується певними особливостями, відображеними в їх правах та обов'язках. Законодавство також встановлює мінімальний

набір повноважень, які є спільними для всіх учасників забезпечення кібербезпеки. В межах своєї компетенції суб'єкти забезпечення кібербезпеки:

– Здійснюють заходи для запобігання використанню кіберпростору воєнними, розвідувально-підривними, терористичними та іншими протиправними та злочинними цілями.

– Виявляють та реагують на кіберінциденти та кібератаки, усувають їх наслідки.

– Здійснюють обмін інформацією про реалізовані та потенційні кіберзагрози.

– Розробляють і впроваджують заходи у сфері кібербезпеки, кібероборони та кіберзахисту, включаючи запобіжні, організаційні, освітні та інші.

– Забезпечують проведення аудиту інформаційної безпеки, в тому числі на об'єктах, що перебувають у їхні управлінні або підпорядковані їм об'єкти.

– Здійснюють інші заходи щодо розвитку та забезпечення безпеки кіберпростору [8, с. 90–91].

Після аналізу переліку суб'єктів, зазначених у Законі, можна зробити висновок про дублювання деяких суб'єктів. Наприклад, Національна поліція України входить як правоохоронний орган як до числа суб'єктів, зазначених у статті 5, так і визначена як основний суб'єкт у статті 8. Також незрозумілим є включення Національного банку України і Збройних сил України як суб'єктів забезпечення кібербезпеки одночасно до статей 5 і 8 Закону.

Крім того, логіка статті 8 законодавчого акта передбачає наявність додаткових суб'єктів, окрім основних, але перелік таких додаткових суб'єктів не визначений законодавцем. Ці прогалини у законодавстві заважають створенню цілісної та ефективної організаційної структури системи суб'єктів забезпечення кібербезпеки в кібернетичній сфері.

Слід зазначити, що в Стратегії кібербезпеки України, яка є підзаконним нормативно-правовим актом, перелік органів у сфері забезпечення кібербезпеки сформульований більш виважено та логічно, порівняно з Законом [9, с. 17].

У Стратегії забезпечення кібербезпеки України та Законі про основні засади забезпечення кібербезпеки України закріплені специфічні повноваження основних суб'єктів національної системи кібербезпеки. Ці основні суб'єкти включають Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи та Національний банк України.

Закон про Державну службу спеціального зв'язку та захисту інформації України визначає загальні напрями діяльності та повноваження цієї служби у сфері забезпечення кібербезпеки України. Проте безпосередня реалізація державної політики в цій галузі покладена на спеціальний орган, що діє в складі Служби спецзв'язку – Державний центр кіберзахисту та протидії кіберзагрозам (Центр). Функції Центру передбачають переважно координаційну спрямованість і полягають у забезпеченні ефективної взаємодії органів державної влади з питань запобігання та усунення наслідків кіберінцидентів, координації діяльності операторів та провайдерів щодо збору інформації про кіберінциденти та міжнародної координації з питань кіберзахисту [13].

З урахуванням останніх тенденцій у сфері адміністративно-правового та організаційного забезпечення кібербезпеки як на міжнародному рівні, так і на внутрішньому рівні країн, у тому числі провідних держав світу, та з урахуванням змін в кібернетичній політиці національної безпеки, спостерігається активний процес модернізації секторів безпеки. Цей процес є необхідним для відповіді на сучасні виклики та загрози у кіберпросторі, зокрема враховуючи зростаючий потенціал використання кіберпростору у злочинних цілях [10, с. 144].

На сьогоднішній день провідні держави світу та суспільство загалом все більше покладаються на безперешкодне функціонування кіберпростору і визнають його значення. В цьому контексті відбувається модернізація кібербезпеки паралельно з активним реформуванням управлінських структур та впорядкуванням нормативного поля. Метою цих заходів є забезпечення цілісності державної політики в сфері кібербезпеки. Також важливими елементами є роз'яснювальна робота серед населення щодо кіберзагроз, збільшення чисельності підрозділів, зайнятих у системі кіберзахисту, розроблення кіберзброї та проведення пробних військово-розвідувальних акцій у кіберпросторі, а також посилення контролю за національним інформаційним простором, включаючи методи доступу і контент [4, с. 23].

Органи Національної поліції України відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» є важливими складовими елементами національної системи кібербезпеки. Україна активно формує цю систему відповідно до світових тенденцій в галузі кіберзахисту. Реалізація функціонування системи кібербезпеки є критичним фактором, оскільки

вона гарантує захист життєво важливих інтересів людей, громадян, суспільства та держави в кіберпросторі. За словами М. М. Присяжнюка і Є. І. Цифри, Україна потребує адекватної системи безпеки в умовах, коли національна безпека все частіше стикається з новими викликами, що відрізняються від традиційних загроз. Активна діяльність провідних держав у кіберпросторі, зміни в підходах до внутрішньої інформаційної політики, формування потужних транснаціональних злочинних груп, спеціалізованих у кіберзлочинах, ставлять перед Україною завдання визначення короткотермінових і довготермінових пріоритетів трансформації вітчизняного сектора безпеки [11, с. 65].

Основні органи національної поліції України, які займаються кібербезпекою, включають:

– Департамент кіберполіції: Це спеціалізована підрозділенаціональної поліції, яка спеціалізується на виявленні, розслідуванні та протидії кіберзлочинності. Вона має експертні знання та ресурси для виявлення кіберзагроз та розслідування кіберпреступності.

– Відділи кіберполіції на регіональному рівні: Окрім центрального Департаменту кіберполіції, на регіональному рівні також функціонують відділи кіберполіції, які виявляють та розслідують кіберзлочини на території конкретних регіонів України [1].

За визначенням В. В. Берези, Департамент кіберполіції Національної поліції України виконує комплекс функцій, визначених на нормативно-правовому рівні. Щоб виконати ці функції, Департамент кіберполіції повинен мати відповідні повноваження. В. В. Береза розкриває сутність повноважень Департаменту кіберполіції як суб'єкта протидії кіберзлочинам, враховуючи поняття «право» і «обов'язок». Право в цьому контексті означає закріплену на нормативно-правовому рівні поведінку, яку Департамент кіберполіції використовує для боротьби з кіберзлочинністю. Обов'язок, згідно з пропозицією науковця, означає встановлену на нормативно-правовому рівні необхідну поведінку, яку Департамент кіберполіції повинен дотримуватися в процесі боротьби з кіберзлочинністю [5, с. 32].

Після проведення аналізу Закону України «Про Національну поліцію» та Наказу Національної поліції України «Про Положення про Департамент кіберполіції Національної поліції України», можна виділити наступні функції Департаменту:

– Адміністративна: департамент кіберполіції організовує та контролює діяльність підпорядкованих підрозділів у сфері протидії кіберзлочинності з виконання вимог законодавства України.

– Оперативно-розшукова: департамент здійснює оперативно-розшукові заходи для викриття причин і умов, що призводять до кіберзлочинів. Він організовує виконання доручень слідчого та прокурора щодо проведення слідчих та розшукових дій у кримінальних провадженнях.

– Нормотворча: департамент вносить пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності та бере участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій галузі.

– Кадрова: департамент сприяє правильному підбору, розстановці, навчанню та вихованню кадрів у своїй структурі та підпорядкованих підрозділах.

– Інформаційного забезпечення: департамент забезпечує формування та наповнення інформаційних масивів даних та автоматизованих інформаційних систем.

– Превентивна та профілактична: департамент визначає, розробляє та забезпечує реалізацію організаційних та практичних заходів з метою запобігання та протидії кримінальним правопорушенням у сфері кіберзлочинності. Він також проводить роз'яснювальну роботу серед населення з питань дотримання законодавства України у сфері використання новітніх технологій, захисту та протидії кіберзагрозам у повсякденному житті [6, с. 86].

На сьогоднішній день, однією з основних проблем забезпечення кібербезпеки в Україні є відсутність належної координації між відповідними відомствами. Це призводить до неузгодженості дій у створенні окремих елементів системи кібербезпеки та відсутності загальнонаціонального координаційного центру, який би узгоджував і координував діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційного та кіберпростору України. Такий центр міг би також керувати проведенням комплексних навчань з кібербезпеки, подібних до навчань Cyber Storm, які проводяться в США, або Cyber Europe, які проводяться в ЄС.

Отже, для забезпечення належної координації дій всіх зацікавлених суб'єктів важливо реалізувати інструменти забезпечення та організації кібербезпеки. Також потрібно удосконалити інституціональний механізм формування, координації та контролю за виконанням завдань щодо розбудови кібернетичного суспільства. В цьому контексті важливим є розвиток механізмів парт-

нерства між державою, бізнесом та громадянами у сфері кібербезпеки. Ці механізми можуть включати обмін інформацією між державними ситуаційними центрами та центрами реагування на кіберзагрози з представниками бізнесу та громадського суспільства, поліпшення взаємодії між провайдерами інтернет-послуг та користувачами для інформування про кібервтручання.

Для досягнення цих цілей важливо створити центр взаємодії та координації, що об'єднуватиме всіх зацікавлених суб'єктів. Цей центр відіграватиме роль основного органу для узгодження і співпраці між різними структурами, залученими до кібербезпеки. Він буде відповідальний за забезпечення ефективної комунікації, обміну інформацією та координацію заходів з протидії кіберзагрозам. Такий центр стане центральним пунктом для спільного планування, організації навчань, обміну кращими практиками та розробки стратегій у сфері кібербезпеки [7, с. 20–21].

Враховуючи наведене, потрібно критично оцінити поняття національної системи кібербезпеки згідно з законодавством та переглянути обмеження, що стосуються основних суб'єктів забезпечення кібербезпеки та суб'єкта координації, які виключно належать державним інституціям. Важливо врахувати потреби всіх суб'єктів забезпечення кібербезпеки в Україні, згідно зі статтею 5 Закону України «Про основні засади забезпечення кібербезпеки України».

Сучасна організація структури системи кібербезпеки стикається з проблемою неефективності координації та взаємодії не лише між основними суб'єктами забезпечення кібербезпеки національної системи, але й всередині самої системи. Тому необхідно переглянути підхід до координації та забезпечення взаємодії між усіма суб'єктами, які здійснюють відносини в кіберпросторі.

Оновлений підхід повинен забезпечувати ефективну координацію та взаємодію між державними органами, бізнесом, громадянами та іншими суб'єктами, які мають відношення до кібербезпеки. Важливо створити механізми для обміну інформацією, спільного планування, навчання та розробки стратегій. Такий оновлений підхід сприятиме підвищенню ефективності системи кібербезпеки та забезпечить кращий захист інформаційного простору країни [12, с. 5].

Висновки і перспективи подальших досліджень. В адміністративно-правовому вимірі суб'єкти забезпечення кібербезпеки в Україні мають специфічний статус і регулюються законодавством, спрямованим на забезпечення безпеки та захисту інформації в кіберпросторі. Україна приділяє значну увагу кібербезпеці та впровадженню заходів для запобігання та протидії кіберзлочинності. Суб'єктами забезпечення кібербезпеки в Україні можуть бути державні органи, спеціалізовані служби, науково-дослідні установи, компанії, які надають послуги з кібербезпеки, та інші організації, що займаються захистом інформації та кіберпростору.

Органи державної влади в Україні приділяють значну увагу питанням кібербезпеки і розробляють стратегічні та тактичні плани для забезпечення цілісності та безпеки кіберпростору. Вони співпрацюють з іншими країнами та міжнародними організаціями з метою обміну інформацією та спільної протидії кіберзагрозам. Забезпечення кібербезпеки в Україні є важливим питанням національної безпеки і розвитку країни. Зростання кількості кіберзагроз та кібератак вимагає постійного удосконалення та модернізації заходів забезпечення кібербезпеки.

Суб'єкти забезпечення кібербезпеки несуть велику відповідальність за захист критичних інформаційних систем та мереж в Україні. Вони залучаються до розробки та впровадження стратегічних планів, створення технічних засобів захисту, проведення аудиту безпеки, навчання персоналу та проведення регулярних вправ та тренувань. Загалом, адміністративно-правовий статус суб'єктів забезпечення кібербезпеки України підтримує їх роль у захисті країни від кіберзагроз та виконанні завдань щодо забезпечення кібербезпеки.

Перспективи подальших досліджень в галузі кібербезпеки в Україні є широкими і важливими для забезпечення стійкості та безпеки кіберпростору. Деякі з можливих напрямків досліджень включають: аналіз та прогнозування кіберзагроз; розвиток захисту критичних інфраструктур кібербезпека в хмарних та мобільних середовищах.

Список літератури:

1. Про затвердження Положення про Департамент кіберполіції Національної поліції України: наказ Національної поліції України від 10.11.2015, № 85: веб-сайт. URL: http: // old. npu. gov. ua / mvs/-control / main / uk / publish / printable_article / 1816252 (дата звернення: 29.05.2023).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017, № 2470-IX: веб-сайт. URL: https: // zakon. rada. gov. ua/ (дата звернення: 27.05.2023).

3. Рішення Ради національної безпеки і оборони України від 27.01.2016. «Про Стратегію кібербезпеки України» Указ Президента України від 15.03.2016, № 96 / 2016: веб-сайт. https: // zakon. rada. gov. ua / laws / show / 96 / 2016#Text (дата звернення: 29.05.2023).

4. Барегамян С. Х. Система забезпечення безпеки кіберпростору в Україні. *Кібербезпека та системи захисту інформації: виклики сьогодення*: зб. матеріалів круглого столу. Маріупольський державний університет; Кафедра математичних методів та системного аналізу. Маріуполь, 2017. С. 23–26.

5. Береза В. В. Поняття та класифікація повноважень Департаменту кіберполіції Національної поліції України. *Вісник Харківського національного університету внутрішніх справ.* 2018. № 3 (82). С. 30–39.

6. Білобров Т. В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дисертація... канд. юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ: Національна академія внутрішніх справ, 2020. 209 с.

7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

8. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України: дисертація... канд. юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Суми: Ун-т сучасних знань, 2018. 221 с.

9. Веселова Л. Ю. Компетенція суб'єктів адміністративно – правового забезпечення національної безпеки України в кібернетичній сфері. *Право і суспільство.* 2019. № 5 (2). С. 14–20.

10. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис.* 2015. № 2. С. 144–147.

11. Присяжнюк М. М., Цифра Є. І. Особливості забезпечення кібербезпеки. *Реєстрація, зберігання і обробка даних.* 2017. Т. 19. № 2. С. 61–68

12. Ткач Т. В. Органи Національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень.* Вип. 11. Ч. 2. 2019. С. 111–118.

13. У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам: веб-сайт. URL: http: // www. dsszzi. gov. ua/ (дата звернення: 28.05.2023).

Gnediuk V.L. ADMINISTRATIVE-LEGAL STATUS OF CYBERSECURITY SUBJECTS IN UKRAINE

The article examines the administrative and legal status of subjects involved in ensuring cybersecurity in Ukraine. It explores the legislative norms and provisions that define the status and powers of different entities engaged in protecting the country's cyberspace. The article provides a detailed description of the significance of legal relations in ensuring Ukraine's cybersecurity and outlines the participants in the cybersecurity system who safeguard the rights and freedoms of individuals in cyberspace in accordance with the country's cybersecurity strategy. It also highlights the functions and powers of the Cyber Police Department. Additionally, it describes the role of the State Center for Cyber Protection and Countering Cyber Threats in implementing the state's cybersecurity policy. The Center performs coordination functions aimed at facilitating effective interaction among government bodies, operators, and providers in preventing and mitigating the consequences of cyber incidents. It also ensures the collection of information on cyber incidents and international coordination in cybersecurity matters. The article calls for a review of the institutional mechanism for the formation, coordination, and control of cybersecurity tasks, particularly taking into account the needs of all entities involved in ensuring cybersecurity in Ukraine. To achieve this goal, the involvement of not only state institutions but also businesses and civil society is proposed in the process of establishing and implementing a national cybersecurity system. The article holds significant value in advancing scholarly understanding of the administrative and legal status of entities involved in ensuring cybersecurity in Ukraine. It reveals the problems and deficiencies in the existing coordination and interaction mechanism that require revision and improvement. The research findings can serve as a basis for the development and implementation of an effective cybersecurity system in Ukraine that considers the interests of all stakeholders and ensures proper protection of the country's cyberspace.

Key words: *cyberspace, Cybersecurity Strategy, Cyber Police Department, subject, cybercrime, coordination.*