**УДК 343.9**

***Шеломенцев Володимир Петрович –***
заступник начальника Управління МВС України, кандидат юридичних наук

# Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення

*У статті розкриваються питання організації системи кібернетичної безпеки України, аналізується сучасний стан організаційного забезпечення такої системи та напрями його удосконалення.*

**Ключові слова:** кібернетична безпека, суб'єкти забезпечення кібернетичної безпеки, кібернетичний простір, інформаційно-телекомунікаційні системи.

Зростання залежності людини, суспільства та національних інфраструктур (енергетичної, транспортної, телекомунікаційної) від належної роботи інформаційно-телекомунікаційних систем робить їх уразливими для протиправного впливу з кібернетичного простору, що, в свою чергу, підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України.

Вивчення розбудови систем кібернетичної безпеки у провідних державах світу свідчить, що основними тенденціями у цій сфері є проведення відповідної системної реорганізації сектору безпеки та створення спеціалізованих органів із захисту національних інтересів у кіберпросторі.

Окремі аспекти розбудови системи кібернетичної безпеки України розглядали В. М. Бутузов, В. Д. Гавловський, Д. В. Дубов, Н. А. Ожеван, М. А. Погорецький, К. В. Титуніна, О. М. Юрченко та інші науковці.

Проте, аналіз наукових джерел свідчить, що дослідниками розглянуті лише загальні питання розбудови національної системи кібернетичної безпеки. Водночас, розкриття сутності організаційного забезпечення такої системи дозволить визначити найбільш доцільні напрями його удосконалення, що значно підвищить захищеність життєво важливих інтересів людини, суспільства, держави у кібернетичному просторі.

**Метою статті** є розкриття сутності організаційного забезпечення системи кібернетичної безпеки України та визначення напрямів його удосконалення.

Враховуючи різні наукові підходи до визначення безпеки [1], під кібернетичною безпекою пропонується розуміти стан захищеності життєво важливих інтересів і громадянина, суспільства і держави від зовнішніх та внутрішніх загроз, пов'язаних з використанням ресурсів кіберпростору (іншими словами ресурсами інформаційно-телекомунікаційних систем), за якого в державі забезпечуються сталий розвиток інформаційного суспільства.

Водночас, кібернетичну безпеку слід розглядати як складову інформаційної безпеки. Кібернетична безпека охоплює лише ту частину інформаційної сфери, в якій для обробки інформації застосовуються інформаційно-телекомунікаційні системи. Крім того, відповідно до Доктрини інформаційної безпеки України [2] інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційна безпека розглядається і як невід'ємна складова кожної зі сфер національної безпеки, і як важлива самостійна сфера забезпечення національної безпеки.

Як система кібернетичної безпеки (система кібербезпеки) розглядається сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються.

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки. При цьому, вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави.

Слово "забезпечення" тлумачиться як дія за значенням забезпечити, тобто створювати надійні умови для здійснення чого-небудь, гарантувати щось [3, С. 375], а "організаційне" – пов'язаний з організацією чого-небудь [3, С. 853].

Відносно системи кібербезпеки, слово "організація" розглядається як сукупність процесів або дій, що призводять до утворення та удосконалення взаємозв'язків між частинами цілого [4, С. 931], "організовувати" – налагоджувати, належно впорядковувати що-небудь [3, С. 853].

Тобто, організаційне забезпечення системи кібербезпеки слід розглядати як створення відповідних умов для удосконалення, належного упорядкування взаємозв'язків між елементами такої системи.

Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкту забезпечення кібербезпеки, пов'язану зі:

– створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

– впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Організаційне забезпечення системи кібербезпеки характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їх функціями, повноваженнями, а також підставами, умовами і напрямами їх взаємодії при здійсненні заходів із забезпечення безпеки у кіберпросторі.

Водночас, вибір і впорядкування (розвиток) відповідної організаційної структури обумовлюються потребами забезпечення безпеки певних об'єктів у кібернетичному просторі. Міжнародний досвід із забезпечення кібернетичної безпеки вказує на необхідність надання першочергового кібернетичного захисту об'єктам національної критичної інфраструктури.

До об'єктів критичної національної інфраструктури пропонується віднести об'єкти, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків як: надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення.

Проте, функціонування не всіх об'єктів національної критичної інфраструктури забезпечується інформаційно-телекомунікаційними системами. Тобто, не всі такі об'єкти потребують кібернетичного захисту. А лише ті, керування якими здійснюється в автоматичному або автоматизованому режимі за допомогою відповідних інформаційно-телекомунікаційних систем.

Крім того, слід зауважити, що відповідно до Закону України "Про Концепцію Національної програми інформатизації" [5] такі системи слід розглядати як окремі складові національної інформаційної інфраструктури або національної інфраструктури інформатизації. Тому, правильніше буде розглядати об'єктами кібербезпеки або інформаційно-телекомунікаційні системи об'єктів національної критичної інфраструктури, або об'єкти національної інформаційної критичної інфраструктури.

Лише визначивши об'єкти критичної національної інфраструктури та встановивши для них основні зовнішні та внутрішні загрози кібернетичного характеру можна приступити до формування системи безпеки, ефективність якої буде обумовлена підбором:

– найбільш ефективних заходів захисту від різних видів кібернетичних загроз;

– суб'єктів, здатних забезпечити вжиття відповідних заходів захисту.

Серед суб'єктів забезпечення кібернетичної безпеки виділяють загальні та спеціальні.

До загальних суб'єктів забезпечення кібернетичної безпеки відносяться: Президент України; Верховна Рада України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Збройні Сили України; Служба безпеки України; Служба зовнішньої розвідки України; Національний банк України; інші міністерства та центральні органи виконавчої влади; місцеві державні адміністрації та органи місцевого самоврядування; суб'єкти підприємницької діяльності різних форм власності у сфері виробництва інформаційних продуктів та надання інформаційних послуг.

Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки і оборони України здійснює загальне керівництво у сфері кібернетичної безпеки України.

Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої основи національної політики у сфері кібернетичної безпеки, формує законодавчу базу в цій сфері.

Рада національної безпеки і оборони України (далі – РНБО України) координує та контролює діяльність органів виконавчої влади у сфері кібернетичної безпеки; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії кібернетичної безпеки України.

Крім того, ще у 2002 році при РНБО України було утворено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки [6], до складу якої за посадою входять керівники чи заступники міністерств, відомств, правоохоронних органів, представники Генерального штабу Збройних Сил України, державних комітетів, комітетів Верховної Ради України, наукових та дослідних установ, діяльність яких пов'язана з проблематикою інформаційної безпеки.

Як вбачається, Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при РНБО України повинна забезпечити й вироб-

лення пропозицій щодо визначення, коригування засад внутрішньої й зовнішньої політики у сфері забезпечення кібернетичної безпеки України.

До основних завдань Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України доцільно віднести: аналіз стану кібернетичної безпеки і можливих кібернетичних загроз національній безпеці України та узагальнення міжнародного досвіду щодо формування та реалізації політики у сфері забезпечення кібернетичної безпеки; аналіз здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією центральними органами виконавчої влади державної політики у сфері кібернетичної безпеки; розроблення і внесення вищим органам влади пропозицій щодо: визначення концептуальних підходів до формування державної політики у сфері забезпечення кібернетичної безпеки; удосконалення системи правового, наукового забезпечення кібернетичної безпеки та підготовки кадрів у зазначеній сфері; удосконалення системи оперативного інформаційно-аналітичного забезпечення вищих органів влади у сфері кібернетичної безпеки.

Міністерство оборони України у межах своїх повноважень бере участь у формуванні та реалізації державної політики кібернетичної безпеки у воєнній сфері й сфері оборони, а саме: планує та здійснює заходи протидії й нейтралізації кібернетичних загроз національним інтересам України у воєнній сфері; бере участь у підготовці об'єктів національної критичної інфраструктури до функціонування в особливий період і в умовах воєнного стану; забезпечує розвиток і безпеку власної інформаційної інфраструктури та ресурсів, впроваджує новітні інформаційні технології у сфері оборони.

Генеральний штаб Збройних Сил України: організовує заходи щодо кібернетичного захисту в сфері оборони та контролює їх виконання; координує роботу зі створення та захисту єдиної автоматизованої системи управління Збройними Силами України, впроваджує сучасні інформаційні технології в діяльність органів військового управління; здійснює стратегічне планування застосування Збройних Сил у кібернетичній війні.

Слід відмітити, що з метою забезпечення інформаційної безпеки інфраструктури та Збройних Сил держави в Російській Федерації (далі – РФ) у складі Управління радіоелектронної боротьби, або Головного оперативного управління Генштабу планується створення кіберкомандування. Куратор проекту – начальник Генштабу. Мета й завдання кіберкомандування РФ будуть формуватися на досвіді аналогічних західних структур, а саме: проведення інформаційних операцій і атак проти ворожих комп'ютерних мереж; розробка бойових стратегій та статутів щодо проведення інформаційних операцій; комплектування професійними й креативними кадрами, які будуть здатні зробити свій

внесок у формування концептуальних засад проведення кібероперацій (ФСБ, МВС та Збройні сили РФ); вироблення практичного механізму функціонування відповідного кіберкомандування [7].

Служба зовнішньої розвідки України в межах своїх повноважень забезпечує виконання передбачених Конституцією і законами України, актами Президента України, Кабінету Міністрів України завдань щодо захисту.

Національний банк України відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах кібернетичної безпеки України; регулювання відносин у сфері електронних платіжних систем.

Міністерство з надзвичайних ситуацій України в межах своїх повноважень повинно забезпечувати ліквідацію можливих наслідків кібернетичних атак на об'єкти національної критичної інфраструктури.

Спеціальними суб'єктами забезпечення кібернетичної безпеки є державні органи, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури. До таких суб'єктів відносяться: Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України.

Міністерство внутрішніх справ України, у межах повноважень відповідно до законів України, повинно забезпечити: реалізацію державної політики у сфері боротьби з кіберзлочинністю, розроблення пропозицій щодо визначення концептуальних підходів до формування такої політики; відслідковування та аналіз криміногенних процесів у національному сегменті кіберпростору, виявлення кіберзагроз кримінального характеру життєво важливим інтересам людини і громадянина, суспільства і держави та вжиття заходів щодо їх нейтралізації; організацію та проведення необхідних заходів щодо попередження, своєчасного виявлення, припинення й розкриття кіберзлочинів, установлення осіб, які їх вчинили; здійснення у межах своїх повноважень на підставах і в порядку, встановлених чинним законодавством, гласні та негласні оперативно-розшукові заходи у кібернетичному просторі; викриття причин та умов, що сприяють вчиненню кіберзлочинів, здійснення профілактики кібернетичних правопорушень; належне функціонування цілодобової національної контактної мережі реагування на кіберзлочини.

До повноважень Служби безпеки України у сфері забезпечення кібернетичної безпеки слід віднести: забезпечення контррозвідувального захисту інформаційних ресурсів держави у кіберпросторі; вжиття

заходів з протидії кібернетичному тероризму, попередження, виявлення та припинення кібернетичних злочинів, які посягають на основи національної безпеки або інші життєво важливі інтереси держави; здійснення організаційних, адміністративних, технічних (відповідними програмними та технічними засобами) заходів щодо оцінки стану захищеності об'єктів національної критичної інфраструктури від кібернетичних загроз.

Державна служба спеціального зв'язку та захисту інформації України, у межах повноважень відповідно до законів України, у сфері забезпечення кібернетичної безпеки повинна здійснювати: формування і реалізацію державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (далі – ІТС), криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, технічне регулювання у сферах захисту державних інформаційних ресурсів у ІТС, криптографічного та технічного захисту інформації, організовує та проводить оцінку відповідності, розробляє в установленому порядку стандарти, технічні регламенти і технічні умови; методичне керівництво та координацію діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності у сферах криптографічного та технічного захисту інформації, протидії технічним розвідкам, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в ІТС, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІТС тощо.

Міністерство юстиції у межах своїх повноважень відповідно до законів України відповідає за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт осіб, винних у вчиненні кіберзлочинів (щодо запитів судів), за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам.

Генеральна прокуратура України у межах своїх повноважень відповідно до законів України відповідає за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт осіб, винних у вчиненні кіберзлочинів (щодо запитів органів досудового слідства), за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам (щодо доручень органів досудового слідства).

Узагальнення вищенаведеного дозволяє зробити висновок про доцільність виокремлення у системі кібернетичної безпеки України таких основних елементів:

– загальнодержавна система протидії кіберзлочинності та кібертероризму;

– загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури.

При цьому, під загальнодержавною системою протидії кіберзлочинності та кібертероризму розуміється сукупність спеціальних суб'єктів протидії кіберзлочинності та кібертероризму, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються.

Загальнодержавну систему кібернетичного захисту об'єктів критичної національної інфраструктури пропонується розглядати як сукупність спеціальних суб'єктів забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних й технічних заходів.

При цьому, при розробці критеріїв віднесення об'єктів національного сегменту кіберпростору до критичної інфраструктури слід виходити зі значення даного об'єкту для забезпечення життєво важливих інтересів людини, суспільства, держави у кіберпросторі, а також оцінки рівня прогнозованої шкоди від кібератаки на цей об'єкт.

З урахуванням визначених критеріїв має бути сформований та офіційно затверджений Кабінетом Міністрів України Перелік об'єктів національної критичної інфраструктури незалежно від форми власності та підпорядкування. До зазначеного Переліку, в першу чергу, слід включити інформаційні системи, які використовуються в процесі державного управління, забезпеченні обороноздатності, національної безпеки, а також системи управління стратегічно важливими та техногенно небезпечними об'єктами. Відповідне завдання Кабінету Міністрів України визначено Рішенням Ради національної безпеки і оборони України від 17 листопада 2010 року [8].

Узагальнюючи зазначене, організаційне забезпечення системи кібербезпеки України можна розглядати як створення відповідних умов для удосконалення, належного упорядкування взаємозв'язків між елементами такої системи, якими є суб'єкти забезпечення кібернетичної безпеки, засоби та методи, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних і технічних заходів, що ними здійснюються.

Тобто, під організаційним забезпеченням безпеки у кіберпросторі слід розуміти створення умов для належного упорядкування:

– стану системи відповідних державних органів, що здійснюють відповідну діяльність, який характеризує її організаційну структуру,

місце та роль кожного державного органу та їх спеціалізованих підрозділів у цій системі, їх функції, повноваження, а також підстави, умови й напрями взаємодії;

– діяльності зі створення керованих систем (організаційних структур) кібернетичної безпеки та їх впорядкування (розвиток) до ступеня, що забезпечує найбільшу ефективність вирішення завдань щодо забезпечення належного рівня кібернетичної безпеки;

– діяльності із впорядкування (налагодження) процесу управління (та його окремих стадій) у сфері забезпечення кібернетичної безпеки, створення оптимальних умов для прийняття та реалізації управлінських рішень у цій сфері.

Враховуючи, що слово "удосконалення" тлумачиться як дія за значенням удосконалити (удосконалювати) і удосконалитися (удосконалюватися), тобто робити досконалішим, кращим [3, С. 1497, 1498], під удосконаленням організаційного забезпечення системи кібернетичної безпеки України слід розуміти покращення умов, за яких забезпечується належне упорядкування взаємозв'язків між елементами такої системи.

Тобто, створення покращення наявних умов належного упорядкування взаємозв'язків між суб'єктами забезпечення кібернетичної безпеки, засобами та методами, що ними використовуються, а також відповідних взаємопов'язаних правових, організаційних і технічних заходів, що ними здійснюються, дозволяє підвищити ефективність системи кібернетичної безпеки.

Розбудова ефективної системи кібернетичної безпеки в Україні вимагає вирішення таких питань організаційного характеру, як:

– чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподілу повноважень між ними;

– забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів;

– розробка та впровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки;

– запровадження дієвих стимулів для залучення до такого роду діяльності фахівців високого рівня кваліфікації.

До основних напрямів удосконалення організаційного забезпечення системи кібернетичної безпеки України слід віднести:

– створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору;

– забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки;

– зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму;

– забезпечення максимальної ефективності Збройних Сил у кіберпросторі та їх здатності давати адекватну відповідь реальним і потенційним кібернетичним загрозам Україні;

– посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

– забезпечення необхідних умов для реалізації прав інтелектуальної власності у національному сегменті кіберпростору;

– створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів.

Підсумовуючи викладене, можна констатувати, що розуміння сутності організаційного забезпечення системи кібернетичної безпеки України дозволить суттєво підвищити рівень стійкості такої системи та забезпечити належний рівень захисту інтересів людини, суспільства, держави у кібернетичному просторі.

### *Список використаних джерел*

1. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні: кримінологічний аспект / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал ; Міжвід. наук.-досл. центр з проблем б-би з орг. злоч. при РНБО України. – 2010. – № 22. – С. 215–222.

2. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісн. України. – 2009. – № 52. – Ст. 1783. – С. 7. – 20 лип.

3. Великий тлумачний словник сучасної української мови / уклад. і гол. ред. В. Т. Бусел. – К. ; Ірпінь : ВТФ "Перун", 2009. – 1736 с.

4. Советский энциклопедический словарь / гл. ред. А. М. Прохоров. – [3-изд.]. – М. : Сов. энциклопедия, 1985. – 1600 с.

5. Про Концепцію Національної програми інформатизації : Закон України від 4 лют. 1998 р. № 75/98-ВР // Голос України. – 1998. – 7 квіт.

6. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : Указ Президента України від 22 січ. 2002 р. № 63/2002 // Офіц. вісн. України. – 2002. – № 4. – С. 17. – Ст. 132. – Код акту 21253/2002. – 8 лют.

7. Прежде всего речь идет о проведении атак против вражеских компьютерных сетей / [Электронный ресурс]. – Режим доступа :

http://slon.ru/russia/_prezhde_vsego_rech_idet_o_provedenii_atak_protiv_vrazheskikh_kompyuternykh_setey-767330. xhtml.

8. Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 року "Про виклики та загрози національній безпеці України

у 2011 році" : Указ Президента України від 10 груд. 2010 р. № 1119/2010 [Електронний ресурс]. – Режим доступу :
http://www. president. gov. ua/documents/12624. html.

*В статье раскрываются вопросы организации системы кибернетической безопасности Украины, анализируется современное состояние организационного обеспечения такой системы и направления его усовершенствования.*

*The article is dedicated to the questions of organization of the cybernetic security system of Ukraine, the modern state of the organizational ensuring of such system and the ways of its improvement are analysed.*

*Стаття надійшла до редакції журналу 14 листопада 2012 року.*