УДК 351.74/.76
DOI: 10.35340/2308-104X.2019.82-1-16

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

REGULATORY AND LEGAL SUPPORT OF INFORMATION SECURITY IN THE ACTIVITY OF THE SECURITY SERVICE OF UKRAINE

ХАРЧЕНКО С. О.,
здобувач Національної академії Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький)

KHARCHENKO S.,
post-graduate at the National Academy of the State Border Guard Service of Ukraine named after Bohdan Khmelnytskyi (Khmelnytskyi)

Стаття присвячена питанням визначення сучасного стану нормативно-правове забезпечення інформаційної безпеки в діяльності Служби безпеки України та формування пропозицій з його удосконалення. Дослідження правових актів національного законодавства дозволило виділити такі ієрархічні рівні правового регулювання організації забезпечення інформаційної безпеки в діяльності СБУ: конституційно-законодавчий, міжнародний, підзаконний та відомчий. Зазначені правові норми являють собою певну сукупність, хоч і не мають об'єктивно наданої їм систематизованої форми. Між цими нормами наявні внутрішні правові зв'язки, вони взаємозумовлені і характеризуються взаємовпливом. На сучасному етапі більш нормативно опрацьованими є питання забезпечення кібернетичної безпеки. Водночас, сьогодні необхідно забезпечити закріплення у відомчій нормативній базі таких заходів як здійснення контролю у інтернет просторі (проблема блокування сайтів) та створення інтегрованого банку даних про загрози і небезпеки у сфері інформаційної безпеки в діяльності СБУ.

Ключові слова: *правове забезпечення; юридична сила; ієрархія; інформаційна безпека; відомча нормативна база.*

Статья посвящена вопросам определения современного состояния нормативно-правового обеспечения информационной безопасности в деятельности Службы безопасности Украины и формирования предложений по его усовершенствованию. Исследование правовых актов национального законодательства позволило выделить такие иерархические уровни правового регулирования организации обеспечения информационной безопасности в деятельности СБУ: конституционно-законодательный, международный, подзаконный и ведомственный. Указанные правовые нормы представляют собой определенную совокупность, хотя и не имеют объективно предоставленной им систематизированной формы. Между этими нормами существуют внутренние правовые связи, они взаимообусловлены и характеризуются

взаимовлиянием. На современном этапе более нормативно проработанными являются вопросы обеспечения кибернетической безопасности. В то же время, сегодня необходимо обеспечить закрепление в ведомственной нормативной базе таких мероприятий как осуществление контроля в интернет пространстве (проблема блокировки сайтов) и создание интегрированного банка данных об угрозах и опасности в сфере информационной безопасности в деятельности СБУ.

Ключевые слова: *правовое обеспечение; юридическая сила; иерархия; информационная безопасность; ведомственная нормативная база.*

The article is devoted to the issues of identifying the current state of the normative and legal provision of information security in the activities of the Security Service of Ukraine and the formation of proposals for its improvement. The study of legal acts of the national legislation allowed to specify the following hierarchical levels of legal regulation of the organization of ensuring information security in the SSU activities: constitutional and legislative, international, sub-legislative and departmental. These legal norms represent a certain set, although they do not have a systematized form provided to them objectively. Between these norms there are internal legal relations; they are mutually interconnected and characterized by mutual influence. At the present stage, the issues of ensuring cybernetic security are more normatively elaborated. At the same time, today it is necessary to ensure the consolidation in the departmental regulatory framework of such measures as the implementation of control in the Internet space (the problem of blocking sites) and the creation of an integrated database of threats and danger in the field of information security in the activities of SSU.

Keywords: *legal support; legal force; hierarchy; informational security; departmental normative base.*

Постановка проблеми Інформаційна безпека, як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [2], є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній, соціальній, економічній та інших сферах державної діяльності.

СБУ у межах компетенції має здійснювати: моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій. Розвідувальні органи України у процесі здійснення розвідувальної діяльності мають сприяти реалізації

та захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави, а державна служба спеціального зв'язку та захисту інформації України забезпечуватиме в межах компетенції формування і реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України.

Актуальність дослідження нормативно-правових актів, які визначають правові засади організації забезпечення інформаційної безпеки в діяльності СБУ, обумовлюється також наступним. По-перше, належний рівень правового регулювання впливає на ефективність організації забезпечення інформаційної безпеки в діяльності СБУ, сприяє забезпеченню публічних інтересів та прав громадян. По-друге, динамічний розвиток суспільних відносин у нашій державі, економічний стан та події на сході України, що призводять до постійного збільшення кількості спроб порушення вимог забезпечення інформаційної безпеки в діяльності СБУ, а отже правові норми в цій сфері повинні бути спрямовані на те, щоб коригувати організаційно-правові та оперативні заходи відповідно до вимог сьогодення.

Аналіз останніх досліджень і публікацій. Питанням нормативно-правового забезпечення інформаційної безпеки в діяльності СБУ присвячувалися праці О. М. Бандурки, О. Ф. Долженкова, І. П. Козаченка, М. В. Корнієнка, В. Л. Ортинського, М. М. Перепелиці, В. І. Янушко та ін.

Мета дослідження. Метою статті є визначення сучасного стану нормативно-правове забезпечення інформаційної безпеки в діяльності Служби безпеки України та формування пропозицій з його удосконалення.

Виклад основного матеріалу дослідження. Дослідження правових актів національного законодавства дозволило нам виділити такі рівні правового регулювання організації забезпечення інформаційної безпеки в діяльності СБУ: конституційно-законодавчий, міжнародний, підзаконний та відомчий. Це вибудовує певну ієрархію нормативно-правових актів, створює певний порядок та є підставою для узгодження нормативно-правових актів: як певну обов’язковість акта взагалі, так і пріоритетність його щодо іншого.

Найвищий ступінь такої пріоритетності виявляється у верховенстві таких видів нормативно-правових актів, як Конституція України, закони; у їх здатності безпосередньо регулювати суспільні відносини. Класифікація нормативно-правових актів за юридичною силою має теоретичне та практичне значення, оскільки дозволяє з’ясувати правову природу того чи іншого акта, його ознаки, призначення.

Юридична сила нормативно-правового акта – специфічна властивість мати суворо означене місце серед інших нормативно-правових актів, дотримуватися встановленої субординації. Зазвичай юридична сила акта залежить за формальною обов’язковістю від рівня та обсягу повноважень органу, який видає (приймає) цей акт, тобто суб'єкта нормотворчості. Юридична сила нормативно-правових актів визначається Конституцією України і Законом про нормативні акти. Протягом останніх десяти років здійснювалася цілеспрямована робота з удосконалення правового підґрунтя забезпечення інформаційної безпеки в діяльності СБУ. Також сформовано цілісну систему

правових норм щодо юридичної відповідальності за порушення законодавства у сфері забезпечення інформаційної безпеки в діяльності СБУ, створено нормативну базу для реформування відомства.

Конституційно-законодавчу базу організації забезпечення інформаційної безпеки в діяльності СБУ становлять Конституція України, Закон України Законом України «Про Службу безпеки України»; Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII; Закон України «Про оперативно-розшукову діяльність»; Закон України «Про організаційно-правові основи боротьби з організованою злочинністю»; Закон України «Про конртрозвідувальну діяльність» Закон України «Про Концепцію Національної програми інформатизації», а також Закон України «Про інформацію», Закон України «Про державну таємницю», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про телекомунікації», Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки».

До «додаткових» джерел нормативно-правового регулювання, забезпечення інформаційної безпеки в діяльності СБУ можна віднести: Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, Кримінальний процесуальний кодекс України, Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з ратифікацією Конвенції Ради Європи про заходи щодо протидії торгівлі людьми». Наприклад, кримінальне законодавство України передбачає наявність складу злочину та встановлює підстави кримінальної відповідальності за протиправні дії щодо державної таємниці (статті 114, 328 та 329 КК України), інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст.361-2 КК України), відомостей військового характеру, що становлять державну таємницю (ст.422 КК України), службової інформації, зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст.330 КК України).

Частиною національного законодавства виступають міжнародно-правові акти. У ст. 9 Конституції України передбачено: «Чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Укладення міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України». У статті 18 Конституції України зазначено: «Зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права». Уточнення суттєвої ролі міжнародних договорів за юридичною силою зазначено у ч. 2 ст. 19 Закону України «Про міжнародні договори» 2004 р.: «…якщо міжнародним договором України, який набрав чинності в установленому порядку, встановлено інші правила, ніж ті, що передбачені у відповідному акті законодавства України, то застосовуються правила міжнародного договору» [1].

До числа найбільш вагомих міжнародних актів у частині організації ефективного прикордонного контролю відносимо: положення Загальної декларації ООН прав людини; Конвенції про захист прав людини і основних свобод 1950 року; Міжнародного пакту про громадянські і політичні права 1966 року; Європейської конвенції з прав людини; Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру 1981 року; а також, − Окінавська хартія глобального інформаційного суспільства; Страсбурзька Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру 1981 року; Конвенція про кіберзлочинність від 2001 року; Рекомендація Ради Європи № R (81) 19 1981 р. «Про право доступу до інформації, яка перебуває в розпорядженні органів державної влади»; Регламент (1049/2001) загального доступу до документів Європейського Парламенту, Ради Європи та інші міжнародно-правові джерела серед яких десятки міжнародних угод про взаємний захист секретної інформації (наприклад, Закон України "Про ратифікацію Протоколу між Кабінетом Міністрів України та Урядом Республіки Молдова про внесення змін до Угоди між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації".)

Третій рівень організації забезпечення інформаційної безпеки в діяльності Служби безпеки України (підзаконний) становлять: Указ Презедента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» №47/2017 [3]; Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 р. № 1229; Указ Президента України від 14.12.2004 № 1483/2004 «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації» та інші.

На сьогодні четвертий рівень організації забезпечення інформаційної безпеки в діяльності СБУ (відомчий) становлять такі накази СБУ: Правила забезпечення охорони інформації НАТО з обмеженим доступом в Україні, затверджені наказом ЦУ СБУ від 29.01.2018 № 109/ДСК, (зареєстровано в Міністерстві юстиції України 20.02.2018 № 201/31633, має гриф обмеження доступу); Звід відомостей, що становлять державну таємницю, затверджений наказом СБУ від 12.08.2005 № 440, (зареєстровано в Міністерстві юстиції України 17.08.2005 за № 902/11182) та інш.

Зазначені акти складають «основну» нормативно-правової бази організації забезпечення інформаційної безпеки в діяльності СБУ. Так, положення ст. 17 Конституції України, у якому йдеться про те, що «забезпечення державної безпеки і захист державного кордону України покладається на військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначається законом», знайшло своє відображення у спеціальному Законі України.

Мова йде про комплексний захист інформаційної безпеки в діяльності СБУ, сам е як стану захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше

використовують термін «захист інформації»). Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. В умовах проведення Росією гібридної війни проти України одним з найпоширеніших та найнебезпечніших механізмів кібервпливу стали комплексні APT-атаки, які передбачають використання шкідливого програмного забезпечення, методів соціальної інженерії, а також задіяння прихованих можливостей віддаленого доступу через недокументовані функції у програмному забезпеченні російського виробництва.

Наголосимо, що нажаль, досі не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Серед завдань, покладених на СБУ ст.2 Закону України «Про Службу безпеки України», можна виділити забезпечення охорони державної таємниці та іншої секретної інформації (секретна інформація − інформація, документ або матеріал, що містить державну таємницю, зокрема військову, політичну, економічну, наукову, технічну або будь-яку іншу інформацію, що включена до переліку відомостей, що становлять державну таємницю, погодженого відповідно до національного законодавства держав Сторін, і втрата або несанкціоноване розкриття якої, може завдати шкоди національній безпеці, економічним або політичним інтересам держав Сторін) [4]. Окремо наголосимо, що у нормативно-правовому порядку чітко визначено об єкти інформаційної безпеки, як підлягають захисту СБУ (вимоги та порядок створення системи захисту встановлюються Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ).

Нещодавно прийнятий Закон України «Про національну безпеку України» також визначає основи забезпечення кібербезпеки, повноваження СБУ, Державною службою спеціального зв'язку та захисту інформації України у сфері забезпечення кібербезпеки, порядок підготовки і схвалення Стратегії кібербезпеки, запровадження комплексного огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Крім того, 5 жовтня 2017 року був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. Він наразі є основним документом, який регулює сферу кіберзахисту в країні, створює державну систему кіберзахисту і розподіляє функції між правоохоронцями та спецслужбами. Також вказаним Законом визначений порядок діяльності і повноваження Державного центру реагування на кібератаки, підрозділ якого CERT-UA здійснює моніторинг і виявляє потенційні кіберзагрози. Закон України «Про Концепцію Національної програми інформатизації» проголошує, що «інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки». У ст. 23 «Воєнної доктрини України» прямо вказується, що «здійснення заходів щодо забезпечення інформаційної безпеки є одним із основних завдань Збройних сил України в мирний час». А в ст. 20 зазначається, що характерними рисами сучасної збройної боротьби, серед іншого, є

«зростання ролі і значущості протиборства в інформаційній сфері, використання новітніх інформаційних технологій».

У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» надається визначення поняття «інформаційна безпека» – це «… стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Водночас, ст. 6 Закону України «Про державну таємницю» від 21.08.1994 р. забороняє відносити до державної таємниці будь-які відомості, якщо цим будуть порушуватися конституційні права і свободи людини і громадянина, завдаватиметься шкода здоров'ю і безпеці населення [5, ст. 93].

Разом з цим у Законі України «Про інформацію» визначення «інформаційна безпека» взагалі немає. А в Законі України «Про основи національної безпеки України», який є основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття. Як бачимо, у наведених документах надаються лише загальні визначення терміну «інформаційна безпека» до того ж, не узгоджені між собою. Але ці документи не містять системних підходів до забезпечення інформаційної безпеки в Україні, не визначають суб'єктів інформаційної діяльності та не розподіляють повноважень між ними. У той же час, більш нормативно опрацьованими є питання кібернетичної безпеки. Так, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94 затверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Останнім часом розроблено низку нових законопроектів стосовно інформаційної безпеки держави, а саме «Про засади інформаційної безпеки України», «Про кібернетичну безпеку України», «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». У цих законопроектах частково враховано зазначені недоліки вітчизняного законодавства. Слід зазначити, що події в інформаційному просторі України, викликані агресією з боку РФ, змусили керівництво держави до більш рішучих кроків у цей сфері.

Важливо визначити, що являють собою групи правових норм, які регулюють сферу суспільних відносин щодо провадження діяльності з організації інформаційної безпеки в діяльності СБУ – чи становлять ці норми певну визначену сукупність, чи ні? Тобто необхідно з'ясувати, чи існують внутрішні зв'язки між правовими нормами, що містяться в різних нормативно-правових актах. Вважаємо, що відповідь на це запитання може бути

однозначною: зазначені правові норми являють собою певну сукупність, хоч і не мають об'єктивно наданої їм систематизованої форми. Між цими нормами наявні внутрішні правові зв'язки, вони взаємозумовлені і характеризуються взаємовпливом.

Висновки і перспективи подальших досліджень. Детальний аналіз правових засад свідчить про невідкладну потребу проведення кодифікаційних робіт у справі систематизації даного правового матеріалу на ґрунті визначених спільних підходів. Це продиктовано потребою швидкого вирішення низки питань, про які йшлося вище. Так, сьогодні необхідно забезпечити закріплення у відомчій нормативній базі таких заходів: здійснення контролю у інтернет просторі (проблема блокування сайтів); створення інтегрованого банку даних про загрози і небезпеки у сфері інформаційної безпеки в діяльності СБУ; узгодження зусиль з міжнародними партнерами з протидії незаконній діяльності у інтернет просторі; апробування автоматизованої системи реагування на загрози інформаційної безпеки в діяльності СБУ (через використання елементів штучного інтелекту); організація поточного моніторингу загроз інформаційної безпеки в діяльності СБУ. Результатом кодифікаційних робіт може стати проект Закону України «Про інформаційну безпеку», у реалізації положень якого СБУ відіграватиме чільне місце.

Література:

1. Інформаційна безпека України. Юридична енциклопедія. / за ред. кол. Ю. С. Шемшученко (відп. ред.) Київ: Українська енциклопедія ім. М. П. Бажана, 1998. Т. 2: Д-Й. 744 с.

2. Про міжнародні договори України: Закон України від 29.06.2004 № 1906-IV. Верховна Рада України URL: http://zakon3.rada.gov.ua/laws/show/1906-15

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 29 грудня 2016 року №47/2017. URL https://www.president.gov.ua/documents/472017-21374

4. Угода між Кабінетом Міністрів України та Урядом Латвійської Республіки про взаємну охорону секретної інформації. від 04 червня 2004 1761-IV. Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/428_025/ed20041022/find?text=%D1%E5%EA%F0%E5%F2%ED%E0+%B3%ED%F4%EE%F0%EC%E0%F6%B3%FF

5. Про державну таємницю: Закон України від 21 січня 1994 року // *Відомості Верховної Ради України*. 1994. №16. Ст.93.

References:

1. Informatsiina bezpeka Ukrainy. (1998) Yurydychna entsyklopediia. / za red. kol. Yu. S. Shemshuchenko (vidp. red.). Kyiv: Ukrainska entsyklopediia im. M. P. Bazhana.

2. Pro mizhnarodni dohovory Ukrainy: Zakon Ukrainy vid 29.06.2004 № 1906-IV. Verkhovna Rada Ukrainy. available at: http://zakon3.rada.gov.ua/laws/show/1906-15

3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezedenta Ukrainy vid 29 hrudnia 2016 p. №47. available at: https://www.president.gov.ua/documents/472017-21374

4. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezedenta Ukrainy vid 29 hrudnia 2004p. 1761-IV. Verkhovna Rada Ukrainy. available at: https://zakon.rada.gov.ua/laws/show/428_025/ed20041022/find?text=%D1%E5%EA%F0%E5%F2%ED%E0+%B3%ED%F4%EE%F0%EC%E0%F6%B3%FF

5. Pro derzhavnu taiemnytsiu (1994): Zakon Ukrainy vid 21 sichnia 1994 p. *Vidomosti Verkhovnoi Rady Ukrainy*. №16. St.93.

Information security is one of the essential components of the national security of the country. The development of a thorough national information strategy would greatly contribute to ensuring success in solving problems in the political, social, economic and other spheres of state activity.

The purpose of the article is to identify the current state of the normative and legal provision of information security in the activities of the Security Service of Ukraine and the formation of proposals for its improvement. The proper level of legal regulation affects the effectiveness of the organization of ensuring information security in the SSU activities, promotes the protection of public interests and the rights of citizens.

The study of legal acts of the national legislation has allowed to specify the following hierarchical levels of legal regulation of the organization of ensuring information security in the SSU activities: constitutional and legislative, international, sub-legislative and departmental. It builds a certain hierarchy of normative legal acts, creates a certain order and is the basis for the coordination of regulatory legal acts: both a certain obligation of the act in general and its priority relative to another one.

At the present stage, the issues of ensuring cybernetic security are more normatively elaborated. At the same time, we consider it necessary to ensure the consolidation in the departmental regulatory framework of the following measures: control in the Internet space (the problem of blocking sites); creation of an integrated data bank on threats and dangers in the field of information security in the SSU activities; coordination of efforts with international partners to counter illegal activities in the Internet; testing of an automated system for responding to threats to information security in the SSU activities (through the use of elements of artificial intelligence); organization of the current monitoring of threats to information security in the SSU activities. The result of codification works can be the draft Law of Ukraine “On Information Security”, in the implementation of which the Security Service of Ukraine will play a prominent place.