УДК 007–049.5:34:356.13

І. П. Кушнір
кандидат юридичних наук,
старший викладач кафедри теорії та історії
держави і права та приватно-правових дисциплін
Національної академії Державної прикордонної
служби України імені Богдана Хмельницького

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Сучасне інформаційне суспільство дозволяє оперативно вирішувати багато питань у роботі органів державної влади завдяки досягнутому рівню інформатизації. Загалом, процеси інформатизації формують умови для задоволення інформаційних потреб, реалізації прав громадян і суспільства шляхом формування, розвитку, використання інформаційних систем (далі – ІС), мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислювальної та комунікаційної техніки [1]. Ю. Є. Максименко підкреслює, що перехід суспільства до інформаційного змінив статус інформації. Нині вона може бути як засобом убезпечення, так і загрозою та небезпекою [2, с. 1]. Отже, інформація залишається ключовим, відправним началом, основою функціонування інформаційних систем.

Переваги, пов'язані із впровадженням процесів інформатизації, розширюються та конкретизуються в окремих сферах діяльності держави та суспільства. У сфері охорони державного кордону це і оброблення великого обсягу персональних даних осіб, що перетинають державний кордон, і спрощення управління персоналом, і зменшення часу для здійснення прикордонного контролю, і своєчасне реагування на повідомлення про загрози прикордонній безпеці тощо. Використання ІС у сфері охорони державного кордону, безперечно, має багато переваг, водночас актуальним залишається питання збереження цілісності та захисту інформації, що зберігається (обробляється) в ІС. Саме це зумовлює дослідження проблематики обраної теми.

Науковим розробленням інформаційної безпеки та захисту інформації цікавилися такі вчені, як: І. В. Діордіца, О. О. Климчук, Б. А. Кормич, О. І. Крюков, В. А. Ліпкан, О. В. Логінов, Ю. Є. Максименко, О. В. Олійник, О. О. Тихомиров, Н. А. Ткачук, О. В. Шепета та багато інших. Однак сьогодні питання захисту інформації в ІС Державної прикордонної служби України (далі – ДПСУ) залишається відкритим і потребує нових досліджень.

Мета статті полягає в здійсненні комплексного аналізу організаційно-правового захисту інформації в ІС ДПСУ.

У ДПСУ з урахуванням кращих європейських прикордонних практик упроваджені інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи ДПСУ, зокрема міжвідомчі, бази (банки) даних, інші електронні інформаційні ресурси за компетенцією [3]. Такі комунікаційні системи мають гарантувати високий рівень безпеки інформації та відповідати сучасним вимогам прикордонної безпекової політики. Розвиток ІС у ДПСУ сьогодні є об'єктивною потребою, яка реалізується з урахуванням світової тенденції побудови й інтеграції мереж, засобів і послуг зв'язку [4, с. 168]. Функціонування та постійний розвиток ІС базується на захисті інформації, розпорядником якої є ДПСУ. В ІС захист інформації від різних загроз відбувається синхронно, з обробленням інформації під час використання технічних і програмних засобів.

На виконання положення Стратегії розвитку Державної прикордонної служби України у 2018 р. щодо «забезпечення розвитку інформаційної складової частини системи охорони державного кордону» заплановано модернізацію центральної підсистеми системи «Гарт» для забезпечення фіксації біометричних даних іноземців; інтегрованої міжвідомчої інформаційно-телекомунікаційної системи щодо контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон («Аркан»); інформаційно-телекомунікаційної системи «Гарт-5» [5; 9; 4, с. 13]. З удосконаленням ІС посилюються захисні спроможності, які знижують рівень загрозливого впливу, спрямованого проти інформації, яка в них обробляється.

Під час використання ІС для накопичення, оброблення та збереження інформації, розпорядником якої є ДПСУ, повинні бути створені та підтримуватись умови для виключення несанкціонованого витоку такої інформації, тобто для безпечного функціонування кіберпростору ДПСУ. Ю. Є. Максименко в цьому контексті вживає термін «інформаційно-технічна безпека», управління потенційними чи реальними загрозами з метою захисту інформаційно-телекомунікаційної інфраструктури, зокрема, від комп'ютерної злочинності та комп'ютерного тероризму [2, с. 9].

© Кушнір І. П., 2018

Інформаційні технології та технології у сфері телекомунікації відіграють чи не найважливішу роль у розвитку країн. Але разом із запровадженням нових технологій і відкриттям величезного інформаційного простору з'являються й невідомі до цього моменту проблеми, серед яких варто назвати кібернетичні злочини – правопорушення, що становлять загрозу не лише для окремих громадян, а й для державної безпеки країн [6, с. 96].

Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що центральні органи виконавчої влади є суб'єктами, які в межах своєї компетенції вжиають заходів для кібербезпеки [7, ч. 4 ст. 5]. Державну політику у сфері захисту державного кордону реалізує Адміністрація ДПСУ [8], а також відповідає за кібербезпеку в цій сфері.

Кібербезпека передбачає захищеність життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [7, ст. 1]. Тобто стан, за якого будь-які загрози чи інший негативний вплив не можуть порушити цілісність, конфіденційність та режим доступу до інформації в інформаційно-комунікаційному просторі ДПСУ.

Дотримання належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню й удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектора для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки [9, с. 312].

З урахуванням цього та з метою реалізації Стратегії розвитку Державної прикордонної служби України у 2018 р. серед основних напрямів діяльності – впровадження державної політики з питань захисту державних інформаційних ресурсів та інформації, розгортання спеціальної телекомунікаційної системи шифр «СТС-Д» для криптографічного захисту службової інформації [5, п. 9.5, с. 13], а також посилення протидії інформаційним загрозам [5, п. 22.2, с. 15].

Інформаційна безпека, кібербезпека та кіберзахист є невід'ємними елементами національної безпеки України та необхідним складником функціонування ІС ДПСУ. Це зумовлено необхідністю забезпечення захисту прав людини на доступ до публічної інформації в прикордонній сфері, захисту ІС, мереж та електронних інформаційних ресурсів ДПСУ, розширення застосування інформаційних технологій у системі управління прикордонними підрозділами та під час надання державних послуг, надійного обміну інформацією з питань контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон у межах функціонування інтегрованої міжвідомчої автоматизованої системи, а також унеможливлення несанкціонованого втручання в інші відомчі інформаційні ресурси. Тому питання захисту змісту інформації, що обробляється (передається, зберігається) у комунікаційних (технологічних) системах ДПСУ, визначає необхідність постійного вжиття заходів щодо недопущення втручання в прикордонний кіберпростір.

Відносини у сфері захисту інформації в ІС регулюються Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [10]. Відповідно до цього Закону, для забезпечення захисту інформації в прикордонній сфері органам управління в ДПСУ необхідно виконувати такі його основні положення: по-перше, визначити чіткий порядок доступу до інформації в ІС [10, ч. 1 ст. 4]; по-друге, надавати доступ до інформації тільки встановленому переліку користувачів, відповідно до їхніх повноважень стосовно цієї інформації [10, ч. 1 ст. 4]; по-третє, дотримуватися порядку доступу до державних інформаційних ресурсів або інформації з обмеженим доступом і тільки тих користувачів, перелік та повноваження стосовно цієї інформації яких визначено законодавством [10, ч. 2 ст. 4]; по-четверте, забезпечувати доведення до користувачів відомостей про правила і режим роботи ІС та забезпечити їм доступ до інформації в системі відповідно до визначеного порядку доступу [10, ст. 6]; по-п'яте, функціонування служби захисту інформації [10, ст. 9]; по-шосте, контроль із боку керівництва органів і підрозділів ДПСУ за забезпеченням захисту інформації та діяльністю служби захисту інформації [10, ст. 9]; по-сьоме, забезпечення притягнення до відповідальності особи, винної в порушенні законодавства про захист інформації в ІС, згідно із законодавством [10, ст. 11].

Загальні вимоги й організаційні засади забезпечення захисту державних інформаційних ресурсів урегульовані постановою Кабінету Міністрів України «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. № 373. Положення цієї постанови визначають, що система захисту інформації в ІС призначена для

захисту відомостей: від витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні й інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів оброблення інформації, інших технічних засобів і комунікацій; несанкціонованих дій з інформацією, зокрема з використанням комп'ютерних вірусів; спеціального впливу на засоби оброблення інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [11, п. 16].

Забезпечення захисту інформації й інформаційної безпеки в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДПСУ покладається на службу захисту інформації – Головний центр зв'язку, автоматизації та захисту інформації [3], у складі якого діють: Група режиму і захисту інформації, Центр інформаційних систем, Центр телекомунікаційних систем, Центр технічного захисту інформації, Центр кібербезпеки, які відповідальні за збереження та захист інформації в окремих ІС чи напрямах, відповідно до їхньої компетенції.

Окремо варто зазначити створення 2018 р. спеціального структурного підрозділу, призначеного для досягнення кібербезпеки у сфері охорони державного кордону України, – Центру кібербезпеки [3]. Центр кібербезпеки ДПСУ відповідає за аналіз стану кіберзахисту інформаційно-телекомунікаційних систем ДПСУ, виявляє й усуває чинники, що негативно впливають на захищеність відомчих інформаційних ресурсів, здійснює контроль за виконанням заходів щодо убезпечення інформації в інформаційно-телекомунікаційних системах ДПСУ; своєчасно реагує на кіберзагрози тощо. Тобто відповідає за інформаційну безпеку та захист інформації, розпорядником якої є ДПСУ, обробляє і зберігає її у відомчих ІС за використання сучасних інформаційних технологій.

Інформаційна безпека в частині кіберзахисту в ДПСУ набула належного визнання як складник національної безпеки України. Водночас необхідно враховувати те, що кібератаки стають усе більш комплексними та складними, їхні наслідки становлять загрозу ключовим національним інтересам. Тому для побудови системи кібербезпеки необхідно вдосконалення державного управління в цій сфері, створення нормативно-правової бази для забезпечення такої діяльності [12, с. 179]. Одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки [13, с. 76].

Питання захисту змісту інформації, що обробляється (передається, зберігається) в ІС ДПСУ, зумовлює необхідність застосування всіх дієвих механізмів захисту не тільки правових, організаційних і технічних, але і кримінально-правових. Протиправне використання інформаційних технологій є особливою загрозою не тільки для прикордонної, але й для національної безпеки країни, тому використання комп'ютерних технологій у діяльності ДПСУ зумовлює необхідність застосування правових механізмів технічного захисту інформаційної безпеки, що відображено в окремому розділі Кримінального кодексу України, а саме в р. XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Інформація в прикордонній сфері, що зберігається в інформаційних ресурсах, має загальнодержавне та персональне значення, тому в межах діяльності ДПСУ повинен забезпечуватися її захист від несанкціонованого доступу і витоку, зокрема, технічними каналами й правовими засобами.

Висновки. Акивне використання ІС у діяльності ДПСУ сприяє не тільки прискоренню інформаційних процесів, але й виконанню всіх завдань, які стоять перед прикордонним відомством. Водночас оброблення інформації в таких системах створює додаткову загрозу для порушення її цілісності й безпеки. Тому одночасно з веденням, обробленням, передачею даних в ІС, забезпеченням їх функціонування необхідно постійно вживати заходів з убезпеченням змісту інформації. Такі заходи повинні мати комплексний характер (правові, організаційні, технічні, здійснення контролю, притягнення винних до відповідальності тощо) та реалізовуватися всіма посадовими особами ДПСУ, які мають доступ до функціонування ІС. Налагоджена робота спеціальних структурних підрозділів, призначених для захисту інформації в межах діяльності Головного центру зв'язку, автоматизації та захисту інформації Адміністрації ДПСУ, залучення кращих фахівців у сфері захисту інформації до їх складу, а також надання можливості їхнього професійного зростання підвищить ефективність протистояння інформаційним загрозам у досліджуваній сфері.

Література

1. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. № 75/98-ВР. Відомості Верховної Ради України. 1998. № 27. Ст. 182.

2. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. ... канд. юрид. наук. К., 2007. 20 с.

3. Головний центр зв'язку, автоматизації та захисту інформації. URL: https://dpsu.gov.ua/ua/structure/chastini-centralnogo-pidporyadkuvannya/golovniy-centr-zvyazku-avtomatizacii-ta-zahistu-informacii/.

4. Боровик О. В., Боровик Л. В., Трасковецька Л. М. Дослідження характеристик ефективності функціонування інформаційно-телекомунікаційної системи

«Гарт-1» на основі застосування методів імітаційного моделювання. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія «Військові та технічні науки. 2015. № 1. С. 167–182.

5. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2018 р. Прикордонник України. 2018. № № 3–4 (5593–5594).

6. Коваленко Н. В. Про правовий режим кібербезпеки в Україні. Актуальні проблеми вітчизняної юриспруденції. 2016. № 3. С. 96–100.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

8. Положення про Адміністрацію Державної прикордонної служби України: постанова Кабінету Міністрів України від 16 жовтня 2014 р. № 533. Урядовий кур'єр. 2014. № 195.

9. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320.

10. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

11. Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. Офіційний вісник України. 2006. № 13. Ст. 878.

12. Ліпкан В. А., Діордіца І. В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174–180.

13. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3. С. 75–83.

Анотація

Кушнір І. П. **Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України.** – Стаття.

У статті проаналізовано організаційно-правове забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. Зроблено висновок, що захист інформації відбувається одночасно з уведенням, обробленням, передачею даних в інформаційних системах. Система їх захисту має комплексний характер та забезпечується усіма посадовими особами Державної прикордонної служби України, які мають доступ до функціонування цих систем.

Ключові слова: інформація, захист інформації, інформаційні системи, Державна прикордонна служба України.

Аннотация

Кушнир И. П. **Организационно-правовые вопросы обеспечения защиты информации в информационных системах Государственной пограничной службы Украины.** – Статья.

В статье проанализировано организационно-правовое обеспечение защиты информации в информационных системах Государственной пограничной службы Украины. Сделан вывод о том, что защита информации происходит одновременно с внесением, обработкой, передачей данных в информационных системах. Система их защиты носит комплексный характер и обеспечивается всеми должностными лицами Государственной пограничной службы Украины, которые имеют доступ к функционированию этих систем.

Ключевые слова: информация, защита информации, информационные системы, Государственная пограничная служба Украины.

Summary

Kushnir I. P. **Organizational and legal issues of information protection in information systems of the State border guard service of Ukraine.** – Article.

The article analyzes the organizational and legal support for the protection of information in information systems. Information is protected from various threats in information systems synchronously with the processing of information when using technical and software tools. Protection of information in the information systems of the State border guard service of Ukraine is complex. It is implemented by all officials of the State border guard service of Ukraine, who have access to the functioning of information systems.

Key words: information, information protection, information system, State border guard service of Ukraine.