УДК 004.89:340

А.Г. Бойков,
кандидат юридичних наук, старший науковий співробітник
ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-7439-1452

АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ЖИТТЄДІЯЛЬНОСТІ СУЧАСНОГО СУСПІЛЬСТВА: ПРАВОВИЙ АСПЕКТ

Стаття присвячена дослідженню автоматизованих систем управління інформаційною безпекою в життєдіяльності сучасного суспільства. Розглянуті питання нормативно-правового забезпечення інформаційної безпеки щодо діяльності установ та підприємств за допомогою автоматизованих систем управління. Звертається увага на необхідність впровадження та систематизацію норми інформаційного права із запровадженням відповідних законодавчих рішень для ефективного розвитку автоматизованих систем управління.

Ключові слова: *інформаційно-телекомунікаційна система; інформаційна безпека; ризик; система управління інформаційної безпеки; управління ризиками інформаційної безпеки.*

Статья посвящена исследованию автоматизированных систем управления информационной безопасностью в жизнедеятельности современного общества. Рассмотрен вопрос нормативно-правового обеспечения информационной безопасности в деятельности учреждений и предприятий с помощью автоматизированных систем управления. Обращается внимание на необходимость внедрения и систематизации нормы информационного права с введением соответствующих законодательных решений для эффективного развития автоматизированных систем управления.

Ключевые слова: *информационно-телекоммуникационная система; информационная безопасность; риск; система управления информационной безопасности; управления рисками информационной безопасности.*

Одним із найважливіших напрямів переходу до інформаційного суспільства в Україні є автоматизація управлінської діяльності установ та підприємств. Масштабні переваги та вплив інформаційних технологій на всі сфери діяльності людини надзвичайно великі. Нині сформувалися необхідні технологічні передумови, які можуть забезпечити здійснення управлінської діяльності в господарській сфері в абсолютно нових для них умовах. Також вони дозволяють підвищувати ефективність діяльності установ і підприємств на основі використання інновацій щодо інформаційних технологій, а також ефективність їх взаємодії з відповідними органами влади та громадянами.

Застосування в процесах управлінської діяльності установ та підприємств автоматизованих інформаційних систем (далі – АІС), що дає поштовх для розробки та застосуванні їх у сфері державного управління. Не так давно існувала думка, що технологічні мережі і системи ізольовані від зовнішнього світу, тому забезпечення інформаційної безпеки (далі – ІБ) у цій сфері не визнавалось актуальним. Однак останнім часом спостерігається активізація небезпечних кіберспільнот,

© Бойков А.Г., 2018

яка проявляється у формі кібертероризму, інформаційного шпигунства і навіть шантажу. Крім того, у всіх областях управлінської діяльності і на всіх рівнях функціонують сотні автоматизованих інформаційних систем. Внаслідок цього критично зростає доступність засобів та інструментів віддаленого впливу на інформаційну інфраструктуру, нерідко завдяки постійному вдосконаленню методів комерційного інформаційного злодійства і шахрайства.

Слід сказати, що держава приділяє велику увагу питанням організації захисту АСУ та інших інформаційних систем, які вважаються потенційно вразливими об'єктами. Відповідно до державної політики в галузі забезпечення безпеки АСУ Україна постійно розробляє та створює відповідні нормативно-правові акти, що стосуються інформаційної безпеки.

Необхідно зазначити, що законодавство України розвивається в напрямі переходу на обов'язкову електронну форму взаємодії учасників правовідносин – нині цей процес найбільш помітний у сфері надання державних послуг у різних сферах.

Проте в умовах значного впливу, який чинить автоматизація на процеси державного управління та на суспільство в цілому, ряд важливих відносин, пов'язаних з розробкою та застосуванням автоматизованих інформаційних систем, досі не мають правового регулювання.

На сьогодні врегульовані загальні питання, пов'язані з майновими відносинами з приводу АІС, авторськими правами на компоненти АІС (програмне забезпечення для ЕОМ та бази даних), забезпеченням безпеки АІС, захистом оброблюваних з допомогою АІС персональних даних тощо.

Законодавчо не врегульовані питання допустимості використання АІС. Сформована практика правового регулювання полягає у прийнятті нормативного правового акта, що легітимізує використання певної системи для автоматизації конкретних процесів на декларативному рівні. Такий нормативний правовий акт ніяк не прив'язаний до самої системи (зокрема, система може оновлюватися, змінюючи свої функціональні характеристики без необхідності внесення поправок у нормативно-правовий акт). Цей підхід не перешкоджає використанню некоректно функціонуючих систем (містять програмні помилки або некоректні припущення в процесі проектування), яке призводить до порушення норм українського права. Сучасне законодавство взагалі не містить поняття помилки в програмі і не торкається такого питання, як законність або незаконність використання певної АІС для автоматизації адміністративних процесів. Проте у судовій практиці вже з'являються випадки порушення прав і законних інтересів учасників цих процесів через використання некоректно функціонуючих АІС. Відсутній єдиний підхід щодо регулювання правового режиму АІС, що включає питання юридичного значення дій, які виконує АІС в автоматичному режимі стосовно документів і записів в базі даних, створених за допомогою АІС, та порядку її використання. Попри те, що окремі аспекти інформаційної безпеки та її правового забезпечення було розглянуто в роботах Арістової І.В., Бєлякова К.І., Бєлєвцевої В.В., Калюжного Р.А., Кормича Б.А., Кохановського О.В., Новицького А.М., Тація В.Я., Цимбалюка В.С. та інших науковців, поза увагою зазвичай залишається розгляд нормативного забезпечення захисту даних в інформаційних автоматизованих системах управління діяльністю установ та підприємств, що і є метою нашої статті.

В Україні приділяється велика увага питанням організації захисту АСУ та інших інформаційних систем управління, які забезпечують інформаційну безпеку управління в установах та на підприємствах (далі – ІБУУП). Відповідно до

державної політики в галузі забезпечення безпеки автоматизованих систем управління ІБУУП розробляються відповідні нормативно-правові акти щодо забезпечення інформаційної безпеки в Україні.

Захист всіх складових ІБУУП вимагає розробки методичного апарату і створення особливих інфраструктур. Завдання забезпечення ІБУУП ускладнюються тим, що інформаційний простір не має меж. Особливості роботи локальної мережі установи та мережі Інтернет створюють передумови для безконтрольної і безперешкодної міграції величезних масивів даних, що можуть містити відомості, обіг яких може бути заборонений або обмежений. Досліджуючи методологічні проблеми правового регулювання становлення інформаційного суспільства, І.В. Арістова зазначає, що існує декілька етапів розбудови інформаційного суспільства. Перший етап розвитку інформаційного суспільства переважно ґрунтується на досягненнях інформаційних технологій та технологій зв'язку, наступний етап його розбудови повинен допускати більш широкі соціальні, етичні та політичні параметри – це нове суспільство знань. Також відмічено, що в основі суспільства знання лежить можливість знаходити, виробляти, обробляти, перетворювати, поширювати та використовувати інформацію з метою отримання й застосування необхідних для людського розвитку знань. Таке бачення спирається на концепцію суспільства, яке сприяє розширенню прав і можливостей, що включає в себе поняття чисельності, інтеграції, солідарності та участі [1, с. 5].

Технології за допомогою яких здійснюються атаки на АСУ, розвиваються швидше захисних, тому навіть державні бази даних перебувають у зоні ризику. Можна зазначити, що для захисту державної таємниці застосовуються найдосконаліші технології. Проте щойно державна таємниця виходить з найбільш охоронюваного периметра, вона одразу потрапляє в зону ризику і стає об'єктом взаємодії державних установ з різноманітними організаціями або громадськими інститутами, у яких ступінь захисту істотно нижче. На нашу думку, керівництво установ та підприємств недостатньо обізнані в питаннях забезпечення ІБ АСУ і часто недооцінюють важливість вирішення завдань захисту інформації. Тому часто при замовленні АСУ для ІБУУП в кращому випадку намагаються перенести технології захисту "офісних" інформаційних систем, що далеко не завжди доцільно і ефективно. Мова йде про ускладнення управління ІБ за допомогою АСУ в умовах стрімкого зростання комп'ютерної та іншої інформаційної техніки яка використовується в установах та на підприємствах.

Розвиток інформаційної грамотності став загальносуспільною вимогою та умовою для виконання виробничих чи управлінських функцій, що обслуговують усі структури соціальної зайнятості. Кваліфікаційні вимоги до всіх професій і посад передбачають необхідний рівень вимог і забезпечують придбання знань і навичок в нових умовах роботи. Обов'язок адміністрацій – забезпечити раціональне використання інформаційної інфраструктури, з одного боку, а з іншого – якісно виконувати всі функції та операції, пов'язані з інформаційною діяльністю на будь-якому рівні при забезпеченні інформаційної безпеки [2, с. 65].

Також, на нашу думку, стрімкий розвиток інформаційного суспільства вимагає від сучасної держави створення та розвитку ефективної системи забезпечення інформаційної безпеки, яка теж в свою чергу вимагає від держави розробки відповідної державної політики та її закріплення і реалізації на всіх рівнях.

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає встановленням законних правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані

Конституцією умови існування і розвитку держави та всього суспільства. Кормич Б.А. зазначає, що ряд основних ознак інформаційної безпеки, що обумовлюються специфікою її об'єкта – зони інформаційної безпеки, перебувають на перехресті функції національної безпеки та інформаційної функції держави; питання інформаційної безпеки держави має екстериторіальний характер; суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними і різноплановими; компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави і її органів по регулюванню інформаційних процесів; у демократичному суспільстві державне регулювання інформаційної сфери можливе лише шляхом встановлення правових норм; політика інформаційної безпеки має багатовекторний характер [3, с. 93].

На думку дослідників, правову основу забезпечення інформаційної безпеки України становлять Конституція України [4], закони України "Про основи національної безпеки України" [5], "Про доступ до публічної інформації" [6], проект Закону України "Про інформаційний суверенітет та інформаційну безпеку України" [7] , інші закони та інформативно правові акти, а також ратифіковані або парафовані Україною міжнародні.

Відповідно до ст. 3 Конституції України визначено: "Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави" [4]. Крім того, в ст. 17 закріплена норма забезпечення інформаційної безпеки як однієї з найважливіших функції держави. Відповідальність за забезпечення державного суверенітету, в тому числі інформаційного, здійснення внутрішньої і зовнішньої політики держави, виконання Конституції і законів України, указів Президента України покладено на Кабінет Міністрів України. Важливими в контексті нашого дослідження є також положення п. 5 ст. 92 Конституції України, у якому закріплено, що виключно законом встановлюються засади організації транспорту та зв'язку, а також норма про те, що основи національної безпеки є складовою інформаційної безпеки.

На нашу думку, в Законі України "Про основи національної безпеки України" [5] також визначені деякі загрози ІБ для нашої держави: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; комп'ютерна злочинність та комп'ютерний тероризм.

Постійне реформування державного управління є однією з основних переваг розвитку інформаційного суспільства у країнах з переходом економіки до електронної системи державного управління, що є одним з основних факторів конкурентоспроможності держави в умовах європейської інтеграції. Прийняття державних програм та стратегій, метою яких є вдосконалення системи державного управління і підвищення конкурентоспроможного рівня країни в світі. Результатами реалізації програм та стратегій повинна стати більш ефективна система державного управління в інформаційному суспільстві. Зокрема, розпорядженням

Кабінету Міністрів України була затверджена Стратегія реформування державного управління України на період до 2021 (далі – Стратегія) [8]. Вказаною Стратегією затверджено План заходів з реалізації послуг в електронній формі, який нараховує перелік з 80 е-послуг. З огляду на це, доцільним є об'єднання зусиль з виконання зазначених заходів у державних органах та визначення ними спільно з громадськістю єдиного переліку найбільш популярних серед населення адміністративних послуг в електронній формі.

Також зазначена Стратегія визначає різні строки здійснення оптимізації процедур надання адміністративних послуг в електронній формі.

Необхідно зауважити, що в українському національному праві системоутворюючим чинником і поштовхом до виникнення і формування інформаційного права та ІБ можна вважати прийнятий у 1992 р. Закон України "Про інформацію" [9].

Серед проблем, які частково вирішуються ІБ в АСУ України стосовно забезпечення її безпеки щодо національних інтересів в інформаційній сфері, є прийняття наказу Міністерства внутрішніх справ України від 20.10.2017 № 870 "Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС". Метою Положення є вдосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності Національної поліції України.

Одним із прикладів систематизації норм у сфері захисту ІБ є угоди між Україною та іншими державами про співпрацю в наукових дослідженнях і розробках в інформаційній сфері. У цих документах перераховуються заходи довіри і способи протидії кібервійні, а також декларується створення загальної системи ІБ. Це є додатковим аргументом, який підтверджує необхідність створення міжнародної нормативно-правової бази стосовно боротьби з кіберзагрозами, що існують та слугують ризиком для держави. Використання інформаційних технологій в АСУ для ІБУУП стало звичною справою, і збиток від "кібернападів" на адресу держави виражається не лише в репутації, а й у фінансових втратах. ІБ і захист репутації держави повинні стати одним з інструментів в геополітичному протистоянні. Все це зміцнює ідею зосередження зусилля держави на вибудовуванні системи превентивних заходів, однією з яких може стати криміналізація злочинів у сфері АСУ для ІБУУП на максимально високому рівні. Такий підхід допоможе в боротьбі з кіберзлочинністю більше, ніж подолання наслідків інцидентів. Слід зазначити, що норми інформаційного права на сьогодні розпорошені у великій кількості нормативних актів, що суттєво знижує ефективність правового регулювання всієї інформаційної сфери. Тому підтримуємо позицію багатьох вчених (Баранова О.А., Бєлякова К.І., Цимбалюка К.І. та інших), які звертають увагу на необхідність щодо систематизації норм у цій сфері шляхом прийняття Інформаційного кодексу.

Підсумовуючи, слід зазначити, що АСУ для ІБУУП є взаємодією різних елементів, таких як управління інформацією, діяльністю суб'єктів та інформаційними технологічними процесами установи та підприємства. Інформаційні системи управління доцільно класифікувати за об'єктом управління, способом формування, функціональною ознакою. Для створення ефективної АСУ для ІБУУП необхідно систематизувати норми інформаційного права із запровадженням відповідних законодавчих рішень. Під час побудови АСУ для ІБУУП важливо враховувати забезпечення ІБ на міжнародному, державному та корпоративному рівні, яке передусім ґрунтується на нормативно-правовій базі, стандартах,

прогнозах та заходах щодо ІБ. При цьому в нормативно-правову базу має бути внесено зміни до законів України "Про інформацію" та "Про основи національної безпеки України" відповідно до сучасних вимог суспільного розвитку АСУ для ІБУУП. Також важливим завданням стає забезпечення на належному рівні створення інтегрованої інформаційної системи управління ІБ в інформаційне суспільство країни на державному рівні. Інтеграція в інформаційне суспільство відповідних локалізованих інтернет-ресурсів і неможливість повного контролю з боку держави над глобальними соціальними мережами є приводом для спільного пошуку шляхів вирішення надійного забезпечення національної безпеки в інтересах держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Арістова І.В.* Розбудова правової держави в Україні: правовий механізм забезпечення права на доступ до інформації в суспільстві знань. Правова інформатика. 2010. № 1(25). С. 3–13.

2. *Бєляков К.І.* Інформаційна діяльність: зміст та підходи до класифікації. Інформація і право. 2012. № 1(4). С. 63–69.

3. *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи: навч. посіб. Київ: Кондор, 2004. 382 с.

4. Конституція України від 28.06.96 № 254/96 ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

5. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV. Відомості Верховної Ради України. 2003. № 39.

6. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Відомості Верховної Ради України. 2011. № 32. Ст. 314.

7. Про інформаційний суверенітет та інформаційну безпеку України: проект Закону України від 12.08.1999 № 1207-д. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6670 (дата звернення: 12.11.2018).

8. Деякі питання реформування державного управління України: розпорядження КМУ від 24 червня 2016 № 474-р. URL: http://zakon2.rada.gov.ua/laws/show/474-2016-%D1%80 (дата звернення: 16.11.2018).

9. Про інформацію: Закон України від 02.10.92 № 2657-12. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

REFERENCES

1. *Aristova, I.V.* (2010) Rozbudova pravovoyi derzhavy v Ukrayini: pravovyy mekhanizm zabezpechennya prava na dostup do informatsiyi v suspilstvi znan. "Development of Legal State in Ukraine: a Legal Mechanism for Ensuring the Right to Access Information in the Knowledge Society". Legal Informatics 1(25), 3–13 [in Ukrainian].

2. *Bieliakov, K.I.* (2012) Informatsiyna diyalnist: zmist ta pidkhody do klasyfikatsiyi. "Information Activities: Content and Approaches to Classification". Information and Law 1 (4), 63–69 [in Ukrainian].

3. *Kormych, B.A.* (2004) Informatsiyna bezpeka: orhanizatsiyno-pravovi osnovy. "Information Security: Organizational and Legal Basis": manual. Kyiv: Condor. 382 p. [in Ukrainian].

4. Constitution of Ukraine dated June 28, 1996 No 254/96. Bulletin of the Verkhovna Rada of Ukraine. 1996. No 30. Art. 141 [in Ukrainian].

5. On the Fundamentals of National Security of Ukraine: Law of Ukraine dated June 19, 2003 No 964-IV. Bulletin of the Verkhovna Rada of Ukraine. 2003. No 39 [in Ukrainian].

6. On Access to Public Information: Law of Ukraine dated January 13, 2011 No 2939-VI. Bulletin of the Verkhovna Rada of Ukraine. 2011. No 32. Art. 314 [in Ukrainian].

7. About Information Sovereignty and Information Security of Ukraine: Draft Law of Ukraine No 1207-d dated August 12, 1999 [in Ukrainian].

8. Several Issues of the Reform of the Public Administration of Ukraine: CMU Decree No 474-r of June 24, 2016. URL: http://zakon2.rada.gov.ua/laws/show/474-2016-%D1%80 (Date of Application: 16.11.2018) [in Ukrainian].

9. About Information: Law of Ukraine dated 02.10.92 No 2657-12. Bulletin of the Verkhovna Rada of Ukraine. 1992. No 48. Art. 650 [in Ukrainian].

UDC 004.89:340

A.H. Boikov,
Candidate of Law, Senior Staff Scientist of the State Research
Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-7439-1452

AUTOMATED SYSTEMS OF INFORMATION SECURITY MANAGEMENT IN LIFE OF MODERN SOCIETY: LEGAL ASPECT

Office management through automated information systems leads to the development and implementation of them into the field of public administration. Not so long ago, technological networks and systems have been isolated from the surroundings, therefore the provision of information security in this area has not been recognized as relevant one. However, in recent years there has been an intensification of dangerous cyber-communities in obtaining information through espionage and even blackmail. In addition, hundreds of automated information systems operate in all areas of management activity and at all levels. As a result, the availability of means and tools for remote impact on information infrastructure is critically increasing, often due to the continuous improvement of methods of commercial information theft and fraud.

The state pays a great attention to the organization of the protection of automated control systems and other information systems that are considered potentially vulnerable objects. In accordance with the state policy in the field of insurance of the safety of automated control systems of Ukraine, relevant normative and legal acts concerning information security are constantly being developed and created. Ukrainian legislation is developing in the direction of the transition to a mandatory electronic form of an interaction of the parties of legal relations – nowadays this process is the most noticeable in the sphere of rendering state services in various spheres. However, in the context of the strong influence of automation on the processes of public administration and on society as a whole, a number of important relations related to the development and application of automated information systems, have not yet been legalized.

Today, general issues related to property relations concerning automated control systems, copyrights on the components of automated control systems and databases, etc. are regulated.

The issues of the admissibility of the use of automated control systems are not regulated by law. Current practice of legal regulation consists in the adoption of a normative legal act, which legitimizes the use of a particular system for the automation of specific processes at the declarative level. Such normative legal act is not bound to the system itself (in particular, the system can be updated, changing its functional characteristics without the need for amendments to the regulatory legal act). This approach does not prevent the use of incorrectly functioning systems (containing program errors or incorrect assumptions in the design process), which leads to the violation of Ukrainian law. Modern legislation in general does not contain the concept of error in the program and does not address such issues as the legitimacy or illegal use of certain AIS to automate administrative processes. Therefore, an important task is to ensure, at the appropriate level, the creation of an integrated information security information management system at the state level in the information society of the country. An integration into the information society of relevant localized Internet resources and the impossibility of full control by the state over global social

networks is the reason for a joint search for the solutions for the reliable security of national security in the interests of the state.

Keywords: information and telecommunication system; information security; risk; information security management system; information security risk management.

Отримано 21.11.2018