19. Докладніше див., наприклад: Кузнецов С. А. О таможенной (морской) зоне Украины // Митна справа. — 2002. — № 4. — С. 68–80; Кузнецов С. А. Административно-юрисдикционная компетенция таможенных органов Украины в открытом море // Митна справа. — 2002. — № 6. — С. 28–31.
20. Ми не можемо погодитись із твердженнями деяких авторів про те, що прилегла зона це «лишь часть (зона) исключительной экономической зоны прибрежного государства». Див., наприклад: Шемякин А. П. Современное международное морское право и перспективы его развития. — О., 2002. — С. 188.
21. Докладніше про цю частку відкритого моря див., наприклад: Баймуратов М. А., Досковский В. Г. Международно-правовой режим континентального шельфа: Монография. — О., 2001.
22. Див., наприклад: Высоцкий А. Ф., Цемко В. П. Черноморско-Азовский бассейн: (Правовые вопросы использования пространств и ресурсов) / АН УССР. Ин-т государства и права; Отв. ред. Ю. С. Шемшученко. — К., 1991.

УДК 347.77:004

Б. А. Кормич,
канд. юрид. наук, доцент кафедри морського та митного права ОНЮА

ПРАВОВІ ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Однією з ознак сучасної системи управління є широке і ефективне використання автоматизованих систем передачі даних. Тому питання правового регулювання функціонування таких систем є важливою проблемою, яку необхідно вирішувати в процесі реформування управлінської діяльності держави. Цей аспект має особливе значення і при вирішенні проблем інформаційної безпеки. Тож юридична наукова думка не може обходити такі складні і разом з тим теоретично та практично значимі питання.

Окремі аспекти цієї проблеми досліджувались в роботах О. А. Баранова, В. А. Копилова, Р. А. Калюжного, В. І. Ярочкина та інших фахівців правознавців [1; 2; 3]. Однак немало аспектів залишається недостатньо вивченими, що і обумовило формулювання теми даної статті.

Важливим напрямом захисту інформаційної безпеки є встановлення правових засад захисту інформації, що передається або обробляється за допомогою комунікаційних та автоматизованих систем. Основним нормативно-правовим актом в цій галузі вважається Закон «Про захист інформації в автоматизованих системах» [4].

Згідно з цим Законом (ст. 1) автоматизована система (далі — АС) визначається як система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

Визначено п'ять типів неправомірних дій щодо інформації в автоматизованих системах та самих автоматизованих систем (ст. 1), до яких належать:

1) витік інформації — результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

2) втрата інформації — дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

3) підробка інформації — навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС;

4) блокування інформації — дії, наслідком яких є припинення доступу до інформації;

5) порушення роботи АС — дії або обставини, які призводять до спотворення процесу обробки інформації.

Об'єктами захисту від неправомірних зазіхань є інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Захист інформації здійснюється шляхом застосування сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Також Законом «Про захист інформації в автоматизованих системах» визначаються: відносини між суб'єктами в процесі обробки інформації в автоматизованих системах, загальні вимоги щодо захисту інформації в АС і порядок організації цього захисту, відповідальність за порушення норм цього закону та засади міжнародного співробітництва України в сфері автоматизованих систем.

Зокрема передбачено (ст. 11), що вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, визначаються відповідними нормативно-правовими актами. Ці вимоги є обов'язковими для власників АС, де така інформація обробляється і мають рекомендаційний характер для інших суб'єктів права власності на інформацію. Тобто, захист інформації в АС побудовано на тих самих засадах, що захист інформації взагалі, згідно з якими захист державної, службової таємниці, особистих даних побудовано на вимогах правових актів, що визначають режим доступу до цієї інформації, а захист комерційної таємниці — на основі права власності на цю інформацію.

Політика в галузі захисту інформації в АС визначається Верховною Радою України, а державне управління в цій сфері здійснюється Кабінетом Міністрів.

Державне управління в сфері захисту інформації в автоматизованих системах здійснюється шляхом:

– проведення єдиної технічної політики щодо захисту інформації;

– розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в АС;

– затвердження порядку організації, функціонування та контролю за виконанням заходів, спрямованих на захист оброблюваної в АС інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації — власності юридичних та фізичних осіб;

– організації випробувань і сертифікації засобів захисту інформації в АС, в якій здійснюється обробка інформації, яка є власністю держави;

– створення відповідних структур для захисту інформації в АС;

– проведення атестації сертифікаційних (випробувальних) органів, центрів і лабораторій, видачі ліцензії на право проведення сервісних робіт в галузі захисту інформації в АС;

– здійснення контролю захищеності оброблюваної в АС інформації, яка є власністю держави;

– визначення порядку доступу осіб і організацій зарубіжних держав до інформації в АС, яка є власністю держави, або до інформації — власності фізичних та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження.

Взагалі, коли мова йде про захист інформації, то більшість дослідників погоджується з тим, що цей захист може мати лише комплексний характер. Але в цій комплексній системі можна виділити цілий спектр напрямків діяльності суб'єктів захисту інформації, які характеризуються властивими специфічними методами і способами захисту інформації. Зазвичай виділяють:

– правовий захист — спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;

– організаційний захист — це регламентація виробничої діяльності і взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює завдання якої-небудь шкоди виконавцям;

– інженерно-технічний захист — використання різних технічних засобів, що попереджають завдання шкоди інформації [3].

Але слід зазначити, що в будь-якому випадку в основі всіх перерахованих заходів лежать правові норми, якими регламентується діяльність в сфері захисту інформації. Крім того, правовий захист інформації, який було розглянуто в попередніх розділах, стосується так би мовити інформації в «чистому» вигляді, незалежно від її носія. А от наступні — організаційний і інженерно-технічний аспекти захисту інформації, спрямовані не безпосередньо на інформацію, а на системи, об'єкти та носії, на яких ця інформація збирається, зберігається, обробляється та розповсюджується.

Так, наприклад, головні напрями підвищення безпеки передачі інформації, що є власністю держави, визначено в Указі Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» [5]. Зокрема передбачається запровадити щодо органів виконавчої влади, інших державних органів, а також підприємств, установ та організацій, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється згідно із законодавством: спеціальний порядок підключення до іноземних і міжнародних мереж передачі даних, у тому числі до мережі Інтернет; спеціальний порядок придбання комп'ютерної та телекомунікаційної техніки, засобів програмного забезпечення; та здійснення передачі даних глобальними мережами виключно через підприємства (операторів), що визначатимуться Державним комітетом зв'язку та інформатизації України. Органам місцевого самоврядування також рекомендується

здійснювати передачу даних глобальними мережами в порядку, передбаченому вищезазначеним Указом.

Комплексний характер захисту інформаційної інфраструктури реалізується і в національному законодавстві. Так, зокрема відзначається, що захист державних інформаційних ресурсів в автоматизованих системах, що входять до складу інформаційно-телекомунікаційних систем, здійснюється шляхом запровадження комплексної системи захисту інформації (КСЗІ). КСЗІ складається з комплексу технічних, криптографічних, організаційних та інших заходів і засобів, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації [6].

Основними елементами комплексної системи захисту інформації можна вважати заходи технічного та криптографічного захисту інформації, а також комплекс заходів організаційного характеру, який включає встановлення відповідних режимів діяльності об'єктів інформаційних систем, контроль за дотриманням правил і норм здійснення захисту інформації, контроль за діяльністю суб'єктів захисту інформації тощо.

Згідно з відповідним Указом Президента України, технічний захист інформації (ТЗІ) представляє собою «діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації» [7]. Комплекс заходів щодо технічного захисту інформації може здійснюватися лише в інформаційній системі або на іншому об'єкті інформаційної інфраструктури. Рівень безпеки інформації, яка обробляється в системах та на об'єктах інформаційної інфраструктури визначається комплексом її властивостей, який включає три компоненти:

1) конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення;

2) цілісність — властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

3) доступність — властивість інформації бути захищеною від несанкціонованого блокування.

Лише забезпечення всіх трьох характеристик інформації, що підлягає захисту, є умовою ефективного і безпечного використання суб'єктами інформаційних процесів необхідних об'єктів інформаційної інфраструктури.

Технічний захист інформації повинен здійснюватись за допомогою системи технічного захисту інформації, яка представляє собою «сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правову та їхню матеріально-технічну базу» [8].

Суб'єктами цієї системи є:

– Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України;

– органи державної влади, органи місцевого самоврядування, органи управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством, відповідні підприємства, установи та організації, щодо яких здійснюється ТЗІ);

– державні наукові, науково-дослідні та науково-виробничі підприємства, установи та організації, що належать до системи Служби безпеки України і виконують завдання ТЗІ;

– військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з ТЗІ за відповідними дозволами або ліцензіями;

– навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з ТЗІ.

Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їхніх керівників. Основними завданнями суб'єктів системи ТЗІ є:

– забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

– видання у межах своїх повноважень нормативно-правових актів із питань технічного захисту інформації;

– здійснення контролю за станом технічного захисту інформації.

Безпосередні організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, визначаються окремими нормативно-правовими актами, які в основному мають конфіденційний характер.

Неодмінно слід відзначити існування диференціації щодо вимог та стандартів технічного захисту інформації. Ця диференціація залежить від суб'єкта власності інформації, що захищається, та її правового режиму. Так, відносно захисту конфіденційної інформації, яка знаходиться у приватній власності і режим якої визначається її власником, положення більшості нормативно-правових актів з ТЗІ мають рекомендаційний характер. В той же час ці нормативно-правові акти обов'язкові для органів державної влади та органів місцевого самоврядування, які здійснюють технічний захист інформації, необхідність охорони якої визначена законодавством.

Роботи з ТЗІ проводяться організаціями, які мають ліцензії на право провадження господарської діяльності у цій галузі. Також передбачена можливість здійснення робіт з ТЗІ для власних потреб органами державної влади та місцевого самоврядування у дозвільному порядку. Ліцензування господарської діяльності з ТЗІ, а також надання дозволів на проведення таких робіт для власних потреб здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ.

Також встановлено класифікацію основних видів робот з ТЗІ, які виконуються за дозволами Департаменту. Ця класифікація побудована з урахуванням основних можливих шляхів витоку інформації що охороняється, яким кореспондують відповідні заходи захисту і включає розроблення, впровадження, дослідження ефективності та обслуговування систем щодо:

– захисту інформації, носіями якої є акустичні поля;

– захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;

– захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу;

– виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності [9].

Велика увага, також, приділяється експертно-контрольній діяльності в сфері технічного захисту інформації, здійснення якої входить до функцій Інспекції з питань захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Згідно з «Положенням про контроль за функціонуванням системи технічного захисту інформації» [8], ця діяльність здійснюється у формі контрольно-інспекційної роботи з питань ТЗІ та атестації виділених приміщень.

Контрольно-інспекційна робота з питань ТЗІ представляє собою діяльність, спрямовану на визначення та вдосконалення стану ТЗІ органів, щодо яких здійснюється ТЗІ, та на проведення контролю за виконанням суб'єктами системи ТЗІ завдань або проведенням діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями.

Контрольно-інспекційна робота з цих питань включає планування та проведення перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій щодо вдосконалення відповідних заходів в зазначених органах та перевірок інших суб'єктів системи ТЗІ щодо виконання ними завдань або провадження діяльності в цій галузі за відповідними дозволами та ліцензіями.

Самі перевірки бувають трьох видів: комплексні, цільові (тематичні) та контрольні. Під час перевірок контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ у виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Ще одним напрямом контрольної діяльності є атестація виділених приміщень, в рамках якої здійснюється комплекс спрямованих на реалізацію заходів з ТЗІ робіт, метою яких є приведення виділених приміщень у відповідність до вимог нормативних документів з ТЗІ та визначення відповідності захищеності виділеного приміщення встановленій категорії.

Також в Україні діє Державна експертиза в сфері технічного захисту інформації, яка проводиться з метою оцінки захищеності інформації, яка обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, приміщеннях, інженерно-технічних спорудах тощо (об'єктах інформаційної діяльності), та підготовки обґрунтованих висновків для прийняття відповідних рішень [10].

Важливим інструментом державного управління технічним захистом інформаційних систем є, також, стандартизація і сертифікація їхньої діяльності. Для цих цілей, зокрема, встановлено, що Державний комітет стандартизації, метрології та сертифікації затверджує проекти державних стандартів технічного захисту інформації та проводить реєстрацію нормативних документів, відповідно до яких виготовляються засоби забезпечення технічного захисту інфор-

мації, виключно за погодженням з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки [11].

На нашу думку, для інформаційної безпеки визначальними є два питання правової регламентації електронних інформаційних ресурсів:

1) засади створення і використання цих баз їх власником, щоб виключити можливість порушення прав та законних інтересів третіх осіб;

2) компетенцію та обов'язки органів публічної влади щодо ведення баз даних та надання інформації з них. Це надасть можливість зацікавленим особам звернутися до цих органів за необхідною інформацією.

Підбиваючи деякі підсумки аналізу основних нормативно-правових актів із захисту інформаційної інфраструктури ми можемо говорити про те, що, високі темпи інформатизації в світі привели Україну до того рубежу, за яким використання виключно внутрішнього досвіду і старих напрацювань не є достатнім (особливо враховуючи наше хронічне відставання в інформаційній сфері). Розрив між розвинутими країнами і рештою світу невпинно збільшується. Нові реалії висувають і нові вимоги в правовому регулюванні захисту інформації, який повинен стати каталізатором запровадження нових технічних та організаційних засобів.

Література

1. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: Організаційно-правові питання теорії і практики / За ред. Р. А. Калюжного та В. О. Шамаря. — К., 2002.
2. Копылов В. А. Информационное право. — 2-е изд., перераб. и доп. — М.: Юристъ, 2002.
3. Ярочкин В. И. Информационная безопасность. — М.: Междунар. отношения, 2000. — С. 32–33.
4. Про захист інформації в автоматизованих системах: Закон України від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. — 1994. — № 31. — Ст. 286.
5. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних: Указ Президента України від 24 вересня 2001 р. № 891/2001.
6. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 24 грудня 2001 р. № 76.
7. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 р. № 1229.
8. Про Положення про контроль за функціонуванням системи технічного захисту інформації: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 22 грудня 1999 р. № 61.
9. Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 23 лютого 2002 р. № 9.
10. Про Положення про державну експертизу в сфері технічного захисту інформації: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 р. № 62.
11. Про деякі питання захисту інформації, охорона якої забезпечується державою: Постанова Кабінету Міністрів від 13 березня 2002 р. № 281.