

УДК 351.746:007

Ліпкан Володимир Анатолійович – професор кафедри управління в ОВС Національної академії внутрішніх справ, доктор юридичних наук, доцент,

Баскаков Володимир Юрійович – здобувач Національного університету біоресурсів і природокористування України

Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю

У статті здійснено аналіз сучасного стану захисту інформації з обмеженим доступом у вітчизняному законодавстві в умовах боротьби з організованою злочинністю та визначено основні шляхи його удосконалення.

Ключові слова: захист інформації з обмеженим доступом, інформація з обмеженим доступом, державна таємниця, службова таємниця, конфіденційна інформація, організована злочинність.

Розвиток інформаційно-телекомунікаційних технологій та впровадження їх у різні сфери життя суспільства й функціонування органів державного управління має як позитивні, так й негативні наслідки. З одного боку, законне використання можливостей вищезазначених технологій допомагає кожній людині, суспільству в цілому та державному апарату краще задовольняти власні інтереси та реалізовувати покладені на них обов'язки. З іншого, – використання можливостей інформаційно-телекомунікаційних технологій у протизаконних цілях сприяє кримінальним структурам, поодиноким злочинцям учиняти найзухваліші злочини, незважаючи на відстань, розташування, місцезнаходження тощо.

Зокрема, несанкціонований доступ до інформаційних ресурсів, незаконне копіювання інформації в інформаційних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуск програм-вірусів, установка програмних і апаратних закладних пристроїв, знищення і модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, викрадення програмних чи апаратних ключів і засо-

бів криптографічного захисту інформації, поставка “інфікованих” компонентів інформаційних систем тощо є новими способами вчинення протизаконних діянь.

Отже, становлення інформаційного суспільства, де стратегічну роль і значення мають інформаційно-телекомунікаційні технології, сприяє необхідності забезпечення безпеки в умовах транспарентності.

З низки проблем, що присвячені розгляду питанню інформаційної безпеки, найбільш вивченими та досліджуваними є проблеми захисту інформації, яка циркулює в банківській сфері. Передусім, це пов’язано з тим, що інтереси організованої злочинності спрямовані, в першу чергу, на банківсько-кредитну сферу, де активно використовуються інформаційні технології [1, с. 235]. Інформаційна революція в фінансових установах пояснюється тим, що за допомогою інформаційно-телекомунікаційних технологій можна проводити різноманітні фінансові операції без посередників і, незважаючи на відстань, що значно знижує комісійні збори та прискорює обіг фінансових активів. Більше половини зарубіжних банківських установ надають фінансові послуги за допомогою мережі Інтернет у режимі онлайн.

Звичайно, що можливості новітніх технологій активно використовуються криміналітетом задля задоволення протизаконних інтересів, зокрема організованою злочинністю, й в інших сферах. Особливо небезпечною є та категорія протиправних, суспільно небезпечних діянь, що вчиняється у сфері таємної, конфіденційної та службової інформації тощо.

У зв’язку з чим актуальним напрямом наукової діяльності є окреслення засад захисту інформації з обмеженим доступом в умовах боротьби з організованою злочинністю, що і детермінувало написання цієї роботи авторами. З цією метою було поставлено такі завдання:

- виділити основні риси інформації з обмеженим доступом;
- надати авторське визначення поняття “інформація з обмеженим доступом”;
- визначити основні напрями боротьби з організованою злочинністю з метою захисту інформації з обмеженим доступом.

Окремі аспекти забезпечення інформаційної безпеки розглядаються в працях О. Ф. Белова, А. В. Возженікова, І. Ф. Бінька, О. М. Гончаренка, Б. А. Кормича, С. І. Головащенко, В. О. Косевцова, В. А. Ліпкана, В. Н. Лопатіна, О. А. Гаврилова, В. А. Копилова, Р. А. Калюжного, Ю. Є. Максименко, В. С. Цимбалюка та ін. Роботи цих науковців були ретельно вивчені авторами й використані при написанні даної статті.

Нині в Україні відсутні адекватні заходи захисту інформації з обмеженим доступом. Більше того, на законодавчому рівні відсутнє уніфіковане визначення інформації з обмеженим доступом. У вітчизняному законодавстві застосовується кілька десятків термінів на позначення того чи іншого виду інформації з обмеженим доступом (секретна інформація, таємна інформація, конфіденційна інформація, конфіденціальна інформація, нерозк-

рита інформація, незагальновідома інформація тощо), що ускладнює реалізацію норм права в практичній площині, оскільки їх правовий режим не забезпечений необхідним правовим регулюванням. Відсутність законодавчо встановленого правового режиму інформації з обмеженим доступом унеможлиблює ефективну правоохоронну, превентивну діяльність у зазначеній вище сфері.

З метою доведення тези про те, що інформація з обмеженим доступом має самостійне правове значення і наділена властивостями, що істотно відрізняють її від інших видів інформації, більшість дослідників окреслюють її характерні риси:

1) зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми у тій мірі, в якій вони використовуються суспільством, особою;

2) відомості, що складають зміст інформації з обмеженим доступом по своїй суті ідеальні (нематеріальні);

3) інформація з обмеженим доступом існує винятково в рамках взаємодії суб'єктів суспільних відносин: окремих індивідуумів, їхніх груп, а також таких соціальних утворень, як держава, муніципальні утворення та юридичні особи;

4) інформація з обмеженим доступом нерозривно не пов'язана з матеріальним носієм. Вона є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія;

5) інформація з обмеженим доступом має кількісні та якісні характеристики. Співвідношення кількісних і якісних властивостей інформації має нелінійний характер (якість інформації з обмеженим доступом не залежить від її кількості);

6) інформація з обмеженим доступом не є загальнодоступною;

7) інформація з обмеженим доступом відома і використовується чітко визначеним колом осіб;

8) суб'єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації;

9) інформація з обмеженим доступом має особливу соціальну цінність у силу її дійсної або потенційної невідомості третім особам. Поширення такої інформації може спричинити заподіяння істотної шкоди зацікавленим особам;

10) зміст інформації з обмеженим доступом відповідає обмеженням, установленим законодавством [2, с. 72–73].

У цілому підтримуючи виокремлені вище ознаки інформації з обмеженим доступом, що доводять тезу про те, що вона має самостійне правове значення і наділена властивостями, які істотно відрізняють її від інших видів інформації, вважаємо, що ряд ознак потребує уточнення.

По-перше, інформацією, до якої може буде застосований обмежений режим доступу, є така, що не суперечить чинному законодавству Укра-

їни. Кожна країна має власний перелік інформації, до якої не може бути застосований обмежений режим доступу в силу її соціальної цінності. У пункті 4 статті 21 Закону України “Про інформацію” до інформації обмеженим доступом не можуть бути віднесені такі відомості про:

стан довкілля, якість харчових продуктів і предметів побуту;
аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

стан здоров’я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також соціально-демографічні показники, стан правопорядку, освіти і культури населення;

факти порушення прав і свобод людини і громадянина;
незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб;

інші відомості, доступ до яких не може бути обмежено відповідно до законів і міжнародних договорів України, згода на обов’язковість яких надана Верховною Радою України [3].

По-друге, крім власника цієї інформації, доступ до такої інформації мають лише ті, хто, не порушуючи норми чинного законодавства, отримав дозвіл від власника на доступ до такої інформації, тобто є добросовісним користувачем.

По-третє, інформація з обмеженим доступом має особливу цінність для вищезазначеної категорії суб’єктів (моральну, матеріальну, особисту тощо) в силу невідомості її іншим, стороннім суб’єктам.

По-четверте, власники та добросовісні користувачі інформації з обмеженим доступом мають здійснювати певні адекватні заходи з метою унеможливлення доступу сторонніх осіб. При чому ці заходи також мають ґрунтуватися на правових приписах, тобто бути законними.

По-п’яте, за порушення заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації, які вживаються суб’єктом такої інформації (власником чи добросовісним користувачем) має обов’язково бути встановлений один із видів юридичної відповідальності (цивільно-правова, кримінальна, адміністративна відповідальність тощо). У разі відсутності юридичної відповідальності неможливо говорити про порушення режиму доступу.

Беручи до уваги зазначені нами вище коментарі, конститутивними ознаками інформації з обмеженим доступом є:

1) інформація з обмеженим доступом – це, насамперед, відомості, дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

2) інформацією, до якої може буде застосований обмежений режим доступу, є така, що не суперечить чинному законодавству України;

3) певне коло користувачів отримало доступ до неї виключно на законних підставах (добросовісні користувачі);

4) інформація з обмеженим доступом має особливу цінність для вищезазначеної категорії суб'єктів (моральну, матеріальну, особисту тощо) в силу невідомості її іншим суб'єктам;

5) власники та добросовісні користувачі інформації з обмеженим доступом здійснюють адекватні законні заходи з метою унеможливлення доступу сторонніх суб'єктів;

б) за порушення вищезазначених заходів встановлено юридичну відповідальність.

Отже, під інформацією з обмеженим доступом, на нашу думку, слід розуміти **відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах.**

На законодавчому рівні також не визначено критерії, за допомогою яких можна однозначно кваліфікувати ті чи інші відомості (дані) як інформацію з обмеженим доступом чи виділити основні її види. Закон України "Про доступ до публічної інформації" лише містить норму, згідно з якою інформацією з обмеженим доступом є: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація.

В окремих статтях вищезазначеного Закону України надається легальна дефініція конфіденційної та таємної інформації, а також деталізується законодавцем розуміння службової інформації. Так, "*конфіденційна інформація*" визначається як інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. "*Таємна ж інформація* – це інформація, розголошення якої може завдати шкоди особі, суспільству та державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю. До *службової* може належати така інформація: 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрішньомочу службову кореспонденцію, відповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, в сфері оборони країни, яку не віднесено до державної таємниці" [4].

Приспосовуючись до нових соціально-економічних умов, криміналітет при вчиненні терористичних дій, наркоторгівлі, торгівлі людьми, відмиванні “брудних” коштів, використовує новітні інформаційні та технічні доробки. Об’єктом злочинних дій організованих кримінальних угруповань стає конфіденційна комерційна, фінансова, банківська інформація, а також державна таємниця.

Як вірно зазначають науковці (М. В. Гуцалюк, В. С. Цимбалюк), цілі злочинців не змінилися, а змінилися лише засоби досягнення цих цілей “з розвитком міжнародної системи Інтернет, інтеграції її з супутниковим і радіозв’язком, стільниковою телефонією [5]”.

Відповідно до Закону України “Про основи національної безпеки України” від 19 червня 2003 р. на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційній сфері є:

- прояви обмеження свободи слова та доступу громадян до інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп’ютерна злочинність і комп’ютерний тероризм;

- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [6].

Отже, згідно з вищезазначеним законом, така загроза національній безпеці в інформаційній сфері як розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства і держави, займає лише передостаннє місце, хоча аналіз сучасних вітчизняних наукових розвідок дає підстави стверджувати, що найбільшу шкоду національним інтересам може завдати саме розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства та держави.

Успішні атаки хакерів на сервери Центрального розвідувального управління, Федерального бюро розслідування, Пентагону, Сенату, інших урядових, комерційних, наукових установ США, які мають значний досвід захисту інформаційних систем, мали б активізувати правоохоронні та законодавчі органи України у сфері боротьби з комп’ютерною злочинністю. У той же час, ще раз повторимось, в Україні відсутнє відповідне законодавство, що регулює суспільні відносини у сфері захисту інформації з об-

межею доступом, у тому числі деліктне законодавство потребує удосконалення, оскільки містить ряд порушень, санкції яких передбачають незначні покарання за їх вчинення чи взагалі відсутні нові види правопорушень (кіберхуліганство).

Більшість розвинених країн створили спеціальні підрозділи, завданням яких є не тільки захист від хакерських атак чи розслідування скоєного правопорушення, але й превентивний кібернетичний наступ на криміналітет, який використовує інформаційно-телекомунікаційні технології задля реалізації злочинних цілей.

Таким чином, специфіка злочинів у сфері високих технологій вимагає розробки принципово нової превентивної стратегії, тактики та методики, наявності спеціальних технічних засобів, внесення змін до чинного законодавства, створення центрів підготовки відповідних фахівців, спеціалізованих інформаційних систем оперативного сповіщення, проведення взаємних зустрічей та операцій, обміну досвідом між силовими відомствами різних країн.

Список використаної літератури

1. Лопатин В. Н. Информационная безопасность России : Человек. Общество. Государство / В. Н. Лопатин ; С.-Пб. ун-т МВД России. — СПб. : Фонд “Университет”, 2000. — 428 с.
2. Кулініч О. О. Інформація з обмеженим доступом як об’єкт цивільних прав : дис. ... канд. юрид. наук : 12.00.03 / Ольга Олексіївна Кулініч. — О., 2006. — 200 с.
3. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
4. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI / [Електронний ресурс]. — Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>.
5. Романюк Б. Інтернет і злочин / Б. Романюк, М. Гуцалюк // Міліція України. — 2001. — № 11. — С. 22–23.
6. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV // Офіц. вісник України. — 2003. — № 29. — Ст. 1433.

В статье проведен анализ современного состояния сферы защиты информации с ограниченным доступом в отечественном законодательстве в условиях борьбы с организованной преступностью и определены основные направления его усовершенствования.

The article is dedicated to the analysis of the modern state of the information with limit access in the domestic legislation in combating organized crime and the ways of it improvement are determined.

Стаття надійшла до редакції журналу 20 квітня 2011 року.