ПРАВООХОРОННА ДІЯЛЬНІСТЬ

Ганна Шорохова,
науковий співробітник
науково-дослідної лабораторії
з проблем організації навчального процесу
заочного та дистанційного навчання
Харківського національного університету
внутрішніх справ

УДК 351.74 (477)

Деякі аспекти інформаційної безпеки в забезпеченні інформаційно-правової діяльності органів внутрішніх справ України

В сучасних умовах для оперативного та ефективного забезпечення діяльності органів внутрішніх справ (далі ОВС) по профілактиці правопорушень, протидії злочинності, розкриттю і розслідуванню злочинів є комплексне застосування оперативно-технічних засобів, інформаційно-пошукових систем, інформаційно-телекомунікаційних засобів та технологій, що потребує запровадження надійної системи інформаційної безпеки. Це пов'язано зі специфікою завдань які вирішує ОВС, а саме з обробкою та передачею різних видів інформації, яка потребує захисту на всіх етапах її використання.

Зрозуміло, що застосування інформаційних систем та технологій є вимогами часу, які дозволяють швидко й точно збирати дані, оперативно вирішувати завдання щодо зміцнення правопорядку та законності, а також є запорука ефективної протидії злочинності. Але, весь цей процес інформатизації діяльності ОВС тягне за собою широкі можливості доступу до інформаційних ресурсів, каналів інформаційного обміну (радіоканали, оптоволоконні системи, супутникові системи передачі даних), телекомунікаційних систем та інших інформаційних інфраструктур які використовуються в роботі правоохоронних органів.

Це зумовлює необхідність проведення наукових досліджень у напрямках вдосконалення системи інформаційного захисту автоматизованих інформаційних систем ОВС.

Метою статті є здійснення аналізу та вивчення стану інформаційної безпеки в системі інформаційно-правового забезпечення ОВС, як чинник ефективної протидії злочинності.

При вивченні питань інформаційної безпеки необхідно, в першу

чергу, враховувати накопичений міжнародний досвід. У розвинутих країнах світу розробка правових заходів у боротьбі з комп'ютерною злочинністю і захисту інформаційного простору ведеться вже понад чверть століття. З метою уніфікації національних законодавств Рада Міністрів Європейського союзу в 1989 розробила список правопорушень у сфері комп'ютерної інформації, що рекомендований країнам-учасницям ЄС для створення кримінально-правової стратегії розробки законодавства [1, с. 162].

Вітчизняне нормативно-правове забезпечення інформаційної безпеки в правоохоронних органах базується на положеннях Конституції України, законах України «Про інформацію», «Про національну програму інформатизації», «Про захист інформації в автоматизованих системах», «Про телекомунікації», зміст відповідних статей Кримінального та інших кодексів України, Положенні про технічний захист інформації в Україні (Постанова Кабінету Міністрів України від 9 вересня 1994 р. № 632), Положенні про забезпечення режиму таємності під час обробки інформації, що становить державну таємницю, в автоматизованих системах (Постанова Кабінету Міністрів України від 16.02.98 р. № 180), Постанові Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 08.11.1997 р. № 1126, наказу МВС України «Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України» від 14.07.1998 р. та інших наказів МВС України, Департаменту інформаційно-аналітичного забезпечення, а також наказів Державної служби спеціального зв'язку та захисту інформації України (державний орган спеціального призначення, який забезпечує інформаційну безпеку у контексті національної безпеки України, створений на матеріально-технічній базі Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, що було ліквідовано).

Окремі питання дослідження нормативно-правових, організаційних і програмно-технічних заходів інформаційної безпеки в діяльності ОВС розглядались в роботах І. В. Арістової, О. М. Бандурки, О. В. Бойченко, Р. А. Калюжного, Б. А. Комича, В. О. Голубєва, В. Д. Гавловського та ін.

Проте необхідність подальшого наукового пошуку обґрунтовується наявністю проблем в системі забезпечення інформаційної безпеки в діяльності ОВС України з урахуванням стрімкого поширення практики застосування сучасних інформаційних технологій та широких можливостей криміногенних елементів доступу до конфіденційної інформації.

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної інформації, її несвоєчасного надходження, промислового шпигунство, комп'ютерної злочинності тощо. Тому у Конституції України гарантування інформаційної безпеки відноситься до найважливіших функцій держави. Так, згідно зі статтею 17 Конституції гарантування інформаційної безпеки - є справою усього суспільства [2].

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття "інформаційна безпека" розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах.

Відповідно до законодавства України поняття "інформаційна без-

пека" має таке визначення: "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" [3].

Під конфіденційністю розуміють властивість інформації бути захищеною від несанкціонованого ознайомлення

Цілісність – це властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знишення.

Доступність – це властивість інформації бути захищеною від несанкціонованого блокування. [4].

Розглянемо ще одне загальне визначення поняття інформаційна безпека**,** яке може вживатися без огляду на вигляд даних (електронний чи фізичний).

Інформаційна безпека - це стан 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") [5].

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають [5].

В діяльності ОВС України політика інформаційної безпеки має своє визначення: це колегіальне обговорення й документальне закріплення основних напрямів адміністративної діяльності, пов'язаної з процесами інформатизації МВС, захистом відомчої інформації, а також профілактикою і боротьбою з правопорушеннями, що вчиняються з використанням інформаційних технологій – комп'ютерними злочинами [6, с. 9].

Інформаційна безпека ОВС України – це стан інформації щодо діяльності ОВС України, при якому з нею ознайомлені лише суб'єкти, які передбачені чинним законодавством та виключено можливість надходження інформації до третіх осіб [7, с. 18].

Система інформаційної безпеки має бути спрямована на запобігання втрати інформації, її перекручення, несанкціонованого доступу та незаконного її використання під час проектування, впровадження та експлуатації інформаційних підсистем.

У цілому відомча політика інформаційної безпеки спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку інформаційно-аналітичного забезпечення ОВС у відповідності з її цілями [6, с. 9].

Під інформаційною загрозою розуміють потенційне порушення безпеки, або ступінь вірогідності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію [6, с. 49].

Існує багато способів класифікації інформаційних загроз, але найбільш базовою є класифікація за результатами можливого впливу на інформацію: загрози конфіденційності, цілісності та доступності.

На даний час основним напрямом протидії витоку інформації є забезпечення фізичного (технічні засоби, лінії зв'язку, персонал) та логічного (операційна система, прикладні програми, дані) захисту інформаційних ресурсів ОВС. При цьому безпека досягається завдяки використанню апаратних, програмних та криптографічних методів та засобів захисту, а також комплексом організаційних заходів.

Безпека та захист в інформаційних системах ОВС має будуватись з урахуванням комплексного підходу до побудови системи захисту, що передбачає об'єднання в єдиний комплекс необхідних заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

Система безпеки та захисту інформації має закладатись ще на етапі розробки технічного завдання на проектування інформаційних підсистем. Всі проекти, що розробляються, в обов'язковому порядку повинні мати розділ "Захист інформації", який, у свою чергу, розробляється відповідно до "Тимчасових рекомендацій щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи" [8].

Визначальним в безпеці та захисті системи інформаційного забезпечення є адміністрування інформаційних підсистем, яке запроваджується та контролюється інформаційною службою МВС України.

Безпека інформації забезпечується на технологічних етапах збирання, накопичення, обробки та передачі інформації. Відповідальність за безпеку інформації на відповідних технологічних етапах всіх рівнів інформаційного забезпечення несуть підрозділи, що їх здійснюють.

Організація загальної безпеки інформаційного забезпечення запроваджується департаментом інформаційно-аналітичного забезпечення МВС України, одним з основних завдань якого є створення умов для захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [9].

Згідно Положення про Департамент інформаційно-аналітичного забезпечення Міністерства внутрішніх справ України, затвердженого наказом МВС України № 1010 від 05.11.2012 основними функціями Департаменту з питань захисту інформації є:

- забезпечення захисту інформації, що обробляється в інформаційно-телекомунікаційних системах Департаменту, у тому числі персональних даних та іншої інформації, вимога щодо захисту якої встановлена законом (п. 2.6);
- координація та контроль за діяльністю органів і підрозділів внутрішніх справ щодо забезпечення захисту персональних даних (п. 3.7);
- надання методичної та практичної допомоги структурним підрозділам апарату Міністерства та органам внутрішніх справ з питань організації захисту персональних даних (п. 3.8);
- забезпечення створення спільно з режимно-секретним органом МВС комплексних систем захисту інформації інформаційно-телекомунікаційних систем, що експлуатуються ДІАЗ, та методичне керівництво цією роботою в підрозділах інформаційно-аналітичного забезпечення ОВС (п. 3.12);
- організація та здійснення постійного контролю за виконанням вимог законодавства з питань охорони державної таємниці та захисту інформації в автоматизованих системах ДІАЗ та підрозділів інформаційно-аналітичного забезпечення ОВС (п. 4.7) [10].

З метою виконання функцій щодо захисту інформації в інформаційних службах створюються відповідні підрозділи або призначаються відповідальні службовці на всіх рівнях системи інформаційного забезпечення, які у своїй роботі використовують відповідні накази та інструкції.

Але незважаючи на значні результати в області комп'ютеризації, інформатизації та запровадження новітніх інформаційних технологій в діяльність ОВС кінцева ефективність забезпечення інформаційної безпеки ОВС не завжди відповідає сучасним вимогам. Сучасні системи безпеки мають високі характеристики тільки по окремим напрямам забезпечення безпеки. Прямолінійне вирішення даної проблеми шляхом створення на кожну інформаційну систему ОВС власної системи безпеки не є ефек-

тивним та не забезпечує можливості практичної реалізації на всіх рівнях (фінансові обмеження, складність в експлуатації та координації дій). Логічним виходом з цієї ситуації є інтеграція окремих інформаційних систем ОВС та систем безпеки.

Отже можна зробити висновок, що інформаційна безпека органів внутрішніх справ України є однією із ключових в системі функціонування правоохоронних органів. Ефективна організація інформаційної безпеки в забезпеченні інформаційно-правової діяльності органів внутрішніх справ України може бути здійснена завдяки інтеграції інформаційних систем правоохоронних органів та систем безпеки всіх рівнів до єдиного інформаційного середовища на державному та міжнародному рівнях.

Список використаних джерел

1. *Бойченко О. В.* Інформаційна безпека як складова інформаційно-аналітичного забезпечення протидії злочинності // Кримський юридичний вісник /О. В. Бойченко. – 2008. – № 3. – С. 158-165.

2. *Конституція* України // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.

3. *Про* Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: закон України від 09 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

4. *Про* Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999р. № 1229/99.

5. *Інформаційна* безпека [Електронний ресурс] : матеріали з Вікіпедії- вільної енциклопедії. – Режим доступу: http://uk.wikipedia.org/wiki/ Інформаційна безпека.

6. *Бойченко О. В.* Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О.В. Бойченко. – Сімферополь : ВАТ «Сімферопольська міська друкарня», 2009. – 288с.

7. *Беззубов Д. О.* Інформаційна безпека органів внутрішніх справ у системі координації діяльності правоохоронних структур України // Міліція України : щомісяч. інформ.-попул. та наук.-практ. ілюстр. журн. / співзасн. МВС України та Держ. ощад. банк України. – 2012. – № 5/6. – С. 18-19.

8. *Система* безпеки та захисту інформації [Електронний ресурс] : Теорія управління органами внутрішніх справ: Підручник / [За ред. канд. юрид. наук Ю. Ф. Кравченка.] – К.: Національна академія внутрішніх справ України, 1999. – 702 с. – Режим доступу: http://www.pravo.vuzlib.su/book_z1136_page_173.html.

9. *Департамент* інформаційно-аналітичного забезпечення [Електронний ресурс] : Офіційний веб-сайт міністерства внутрішніх справ України. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544651.

10. *Про* затвердження Положення про Департамент інформаційно-аналітичного забезпечення МВС України : Наказ МВС України від 5 листопада 2012 р. № 1010. [Електронний ресурс] : Режим доступу: http://mvs.gov.ua

Шорохова Г. М. Деякі аспекти інформаційної безпеки в забезпеченні інформаційно-правової діяльності органів внутрішніх справ України

Процес інформатизації діяльності ОВС тягне за собою широкі можливості доступу до інформаційних ресурсів, які використовуються в діяльності міліції щодо протидії злочинності та забезпечення прав і свобод громадян. Тому підвищення ефе-

ктивності діяльності ОВС може бути вирішено через запровадження надійної системи інформаційної безпеки.

Ключові слова: інформація, інформаційна безпека, органи внутрішніх справ, інформатизація, міліція, інформаційна система.

Шорохова А. М. Некоторые аспекты информационной безопасности в обеспечении информационно-правовой деятельности органов внутренних дел Украины

Процесс информатизации деятельности ОВД влечет широкие возможности доступа к информационным ресурсам, которые используются в деятельности милиции по противодействию преступности и обеспечение прав и свобод граждан. Поэтому повышение эффективности деятельности ОВД может быть решено путем введения надежной системы информационной безопасности.

Ключевые слова: информация, информационная безопасность, органы внутренних дел, информатизация, милиция, информационная система.

Shorokhova A. Some aspects of information security in providing information and legal activities of internal affairs agencies of Ukraine

The process of informatization of internal affairs agencies activities entail broad possibilities of access to information resources that are used in the police work in combating crime and in the field of guaranteeing human rights and freedoms. Therefore, increasing the efficiency of the police activities can be solved through the implementation of a reliable system of information security.

Key words: information, information security, internal affairs agencies, informatization, police, information system.