ISSN 1727-1584

ТЕОРІЯ І ПРАКТИКА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

С.Л. БЕРВЕНО

Київський національний університет внутрішніх справ

УДК 342.94[342.738+316.775.3]

НОРМАТИВНЕ РЕГУЛЮВАННЯ ПОРЯДКУ ПРОВЕДЕННЯ РОБІТ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ[1]

Відображено погляд автора на недоліки діючої нормативної бази у сфері технічного захисту інформації.

Із розвитком науково-технічного прогресу все більше зростає й об'єм інформаційних ресурсів людства. Це, насамперед, пов'язано з намаганням конкретних осіб та організацій своєчасно отримати важливу інформацію, яка надає їм економічні й політичні переваги над конкурентами.

Зараз принципово неможлива робота біржових структур, фондових ринків, крупних банків, інших споріднених організацій без розвиненої інформаційної мережі, до якої включені філіали, клієнти, партнери, інформаційні центри та інші учасники технологічного процесу.

Інформація стала реальною матеріальною цінністю. Валютні операції, що переводяться через систему електронного зв'язку, різноманітні "ноу-хау", політичні та комерційні таємниці – все це може бути використане злочинними елементами і перетворене ними у значний капітал. Тому, поряд із постійним зростанням цінності інформації, виникають і прогресують способи її несанкціонованого отримання, у тому числі із використанням спеціальних технічних приладів. Технічні засоби розвідки значно розширюють можливості несанкціонованого доступу до конфіденційної інформації. Офіційний продаж таких виробів обмежений, але на технічних ринках за бажанням можна знайти як фірмові зразки, так і розробки вітчизняних "майстрів".

У свою чергу, власники інформації докладають зусилля для захисту відповідної інформації від несанкціонованих впливів.

Окремої уваги заслуговує питання охорони інформації з обмеженим доступом, яка становить державну таємницю. Суспільна небезпечність розголошення державної таємниці досить висока. Практично кожний факт порушення встановлених правил поводження з державною таємницею становить джерело небезпеки. При розголошенні державної таємниці суспільна небезпечність полягає в створенні можливості потрапляння відомостей, що становлять державну таємницю, у розпорядження іноземної розвідки або інших організацій і осіб, які можуть використати їх на шкоду національним інтересам. У результаті вчинення цього злочину порушується конфіденційність секретної інформації: вона стає надбанням сторонніх осіб, які можуть передати ці відомості ще більш широкому колу осіб, у тому числі й представникам злочинних угруповань чи іноземних розвідувальних організацій. Таким чином, порушення конфіденційності державної таємниці створює загрозу заподіяння шкоди національній безпеці України. Розголошення таких відомостей може призвести до людських жертв та інших тяжких наслідків з великими матеріальними або моральними збитками: дипломатичних ускладнень, науково-технічних і технологічних втрат, загроз життю й свободі осіб, які співпрацюють із правоохоронними органами тощо.

Отже, захист інформації став однією з нагальних проблем сьогодення, без вирішення якої неможливе нормальне функціонування сучасного підприємства, установи, організації як приватної, так і державної форм власності.

Особливу роль і місце у сфері забезпечення безпеки інформації посідають заходи з технічного захисту. Технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

У державному стандарті ДСТУ 3396.0-96 [1] визначе-

[1] Первинна рекомендація з напрямку досліджень: канд. юрид. наук Ліпкан В.А. (КНУВС).

ISSN 1727-1584

но основні цілі технічного захисту інформації: запобігання витоку чи порушенню цілісності інформації з обмеженим доступом [1, с.3]. Згідно з даним документом досягнення цілей ТЗІ може бути реалізовано через побудову *системи захисту інформації (СЗІ),* яка являє собою організовану сукупність методів і засобів забезпечення ТЗІ [1, с.3].

Таким чином, система захисту інформації є утворенням, призначеним для досягнення цілей захисту інформації, а роботи з її створення та забезпечення функціонування – одним із головних напрямів діяльності у галузі технічного захисту інформації. Разом із цим, проведений нами контент-аналіз більше ніж 30 наукових досліджень та публікацій (зокрема, робіт Ю.Я. Самохвалова, В.О. Темнікова, В.О. Хорошко [2], Л.І. Северина, С.Л. Северина, А.В. Дудатьєва [3], В.В. Домарева [4], В.І. Ярочкіна [5]), дозволяє стверджувати, що сьогодні відсутній єдиний чітко визначений порядок проведення робіт із технічного захисту інформації. Більшість науковців пропонують своє бачення даного питання, почасти не узгоджуючи його з чинною нормативною базою сфери ТЗІ. Недостатня увага приділяється аналізу положень нормативно-правових актів з цього питання з метою встановлення істини.

У статті зроблено спробу провести аналіз окремих проблемних питань, що виникають у процесі створення систем захисту інформації внаслідок недосконалості діючої нормативної бази. При цьому ми не обмежуємося вивченням питань сфери ТЗІ, що вже достатньо досліджувалися раніше, а робимо спробу продемонструвати теоретичні та практичні погляди щодо якості нормативного регулювання проведення робіт у сфері технічного захисту інформації.

Порядок проведення означеного виду робіт нині урегульовуються сукупністю нормативних документів, які ми умовно класифікували на дві групи: 1) державні стандарти України в сфері ТЗІ та 2) накази Департаменту спеціальних телекомунікаційних систем та захисту інформації (ДСТСЗІ) Служби безпеки України (які, відповідно до Указу Президента від 06.10.2000 р. № 1120/2000 [6], є обов'язковими для виконання центральними і місцевими органами виконавчої влади, підприємствами, установами та організаціями і громадянами). Слід зауважити, що перша група нормативних документів регулювання відносин, що виникають при проведенні робіт, має своєю основною метою, тоді як накази ДСТСЗІ СБ України урегульовують дане питання опосередковано.

До державних стандартів України, що унормовують порядок проведення робіт з технічного захисту інформації, нами включено ті документи, які безпосередньо торкаються даного питання. Нині такими є ДСТУ 3396.0-96 (Технічний захист інформації. Основні положення) [1] та ДСТУ 3396.1-96 (Технічний захист інформації. Порядок проведення робіт) [7].

До наказів ДСТСЗІ СБ України ми включили наказ "Про затвердження Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації" від 29.12.2000 р. № 89/67 [8] та наказ "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23.02.2002 р. № 9 [9]. Шляхом здійснення аналізу діючого масиву наказів ДСТСЗІ ми дійшли висновку, що жоден інший наказ не містить положень, які безпосередньо регулюють порядок проведення робіт у сфері ТЗІ.

Проведений нами контент-аналіз дозволяє стверджувати, що положення зазначених вище документів мають певні неузгодженості, а також не в повній мірі врегульовують ряд основних питань, які мають бути вирішені в процесі побудови системи захисту інформації. Зокрема, це стосується змісту та послідовності робіт з протидії загрозам інформації або їхньої нейтралізації.

Обсяг статті не дозволяє розглянути весь комплекс проблемних моментів нормативної бази, що регламентує порядок проведення робіт з ТЗІ, тому ми обмежилися аналізом регулювання лише одного із основних видів робіт, що мають бути проведені в процесі створення системи захисту інформації – розроблення системи захисту інформації.

Відповідно до державного стандарту ДСТУ 3396.0-96 [1, с.4] на даному етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту інформації, визначити зони безпеки інформації. У документі зазначається, що порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з ТЗІ [1, с.4]. Тобто, розділ 4.2 (Розроблення системи захисту інформації) державного стандарту ДСТУ 3396.0-96, а відповідно і весь документ в цілому, *не містить* у собі *повного переліку заходів*, що мають проводитися на даному етапі робіт.

У державному стандарті ДСТУ 3396.1-96 відомості про порядок проведення робіт з розроблення системи захисту інформації міститься у розділі 5 (Організація розроблення системи захисту інформації) [7, с.4]. У зазначеному розділі пропонується на підставі матеріалів обстеження та окремої моделі загроз визначити головні задачі захисту інформації і скласти *технічне завдання* на розроблення системи захисту інформації [7, с.4]. Окремо зазначено, що основою функціонування системи захисту інформації є *план ТЗІ*. Також у розділі встановлено вимоги до даних документів та вказано, що технічне завдання і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями). Затверджує їх керівник підприємства [7, с.4]. Таким чином, розділ 5 державного стандарту ДСТУ 3396.1-96, а отже і весь документ в цілому, також *не містить* у собі *повного переліку заходів*, що мають проводитися на даному етапі робіт. Враховуючи, що цей стандарт установлює *вимоги до порядку проведення робіт з технічного захисту інформації* [7, с.1] *(виділено мною – Б.С.)*, така ситуація дозволяє нам дійти висновку про недосконалість досліджуваного стандарту, а з урахуванням результатів вивчення стандарту ДСТУ 3396.0-96 – про *відсутність у першій групі нормативних документів,* визначених нами, *повного переліку обов'язкових робіт, що мають бути проведені на етапі розроблення системи захисту інформації.*

Наказ ДСТСЗІ СБ України "Про затвердження Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації" від 29.12.2000 р. № 89/67 [8] визначає кваліфікаційні, організаційні, технологічні та інші вимоги до суб'єктів господарювання, виконан-

ISSN 1727-1584

ня яких є обов'язковою умовою провадження певних видів робіт та надання певних видів послуг у межах господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації.

Наказ ДСТСЗІ СБ України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб " від 23.02.2002 р. № 9 [9] визначає види та умови проведення робіт з технічного захисту інформації для власних потреб, які виконуються за дозволами ДСТСЗІ СБ України, встановлює порядок надання дозволів, контроль та відповідальність під час проведення визначених видів робіт.

Тобто, обидва накази регламентують порядок проведення робіт з технічного захисту інформації, відмінність полягає лише у суб'єктах регулювання: наказ від 29.12.2000 р. № 89/67 регламентує діяльність суб'єктів господарювання, що провадять *господарську діяльність* у галузі ТЗІ, а наказ від 23.02.2002 р. № 9 – органів державної влади, органів місцевого самоврядування, як мають намір проводити роботи з ТЗІ *для власних потреб* (пункт 1.3 наказу [9]). Враховуючи, що ця особливість не впливає на результати дослідження, а також той факт, що ряд положень наказів абсолютно ідентичні, ми провели комплексне дослідження обох наказів єдиним блоком.

Розділ 3 обох наказів встановлює види робіт, які виконуються в межах діяльності з технічного захисту інформації. Контент-аналіз зазначеного розділу дозволив нам виокремити три види робіт, що пов'язані зі створенням систем захисту інформації – це:

1. Розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля, надання консультативних послуг.

2. Розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали, надання консультативних послуг.

3. Розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу, надання консультативних послуг.

Порівняльний аналіз перелічених пунктів уможливлює дійти висновку, що розроблення системи захисту інформації визначено Законодавцем як один із основних видів робіт, що мають бути проведені в процесі створення системи захисту інформації. Разом з цим у розділі 2 (Терміни та визначення) наказу від 29.12.2000 р. № 89/67 (так само у розділі 2 (Визначення) наказу від 23.02.2002 р. № 9) розроблення комплексу (системи) технічного захисту інформації визначено як стадію життєвого циклу комплексу (системи) технічного захисту інформації, яка пов'язана із: складанням технічного завдання, ескізним, технічним (ескізно-технічним), робочим проектуванням; розробленням експлуатаційної документації, програм і методик приймальних (атестаційних) випробувань; виготовленням та випробуванням дослідних зразків, *приймальними випробуваннями (виділено мною – Б.С.)*. Дане визначення викликає ряд запитань.

По-перше, види документації, які містяться у даних наказах та у державному стандарті ДСТУ 3396.1-96, явно не співпадають (зокрема, у наказах ДСТСЗІ СБ України взагалі не йдеться про такий документ, як план ТЗІ), що, з урахуванням досвіду практичної роботи, призводить до необхідності проведення додаткових досліджень чинної нормативно-правової бази з метою визначення повного переліку документів, які мають бути розроблені на підприємстві при проведенні даного етапу робіт.

По-друге, не встановлено повний порядок розробки та узгодження основних документів, складання яких передбачено наказами. Зокрема – ким розробляються документи, ким підписуються та затверджуються, якщо потрібно – то з якими органами узгоджуються тощо.

По-третє, у наказах не розкрито поняття "приймальні випробування". Враховуючи, що *приймання, визначення повноти та якості робіт*, відповідно до положень ДСТУ 3396.1-96 [7, с.2], є окремим видом робіт поряд із *розробленням системи захисту інформації*, правильність віднесення у наказах ДСТСЗІ СБ України приймальних випробувань до етапу розроблення системи захисту інформації видається сумнівною.

Таким чином, можемо дійти висновку про наявність цілого ряду проблемних моментів, які не дозволяють у повній мірі встановити порядок і послідовність робіт з нейтралізації чинників негативного характеру та протидії загрозам інформації або їхньої нейтралізації на етапі розроблення системи захисту інформації.

Ураховуючи важливість даного етапу для створення якісної системи захисту інформації, існує нагальна потреба у приведенні нормативної бази, регулюючої відносини, що виникають при проведенні робіт у сфері ТЗІ, до єдиних стандартів. На нашу думку, доповнень, у першу чергу, вимагають державні стандарти України у сфері ТЗІ ДСТУ 3396.0-96 та ДСТУ 3396.1-96, а на наступному етапі, потребують детального аналізу і інші нормативні акти, що стосуються даного питання. Кінцевим результатом робіт має стати створення чіткої несуперечливої ієрархічної структури нормативних документів, у яких має бути закріплений повний та виключний перелік робіт, виконання яких дозволить у кінцевому підсумку отримати високоефективну систему захисту інформації.

ЛІТЕРАТУРА

1. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. –Введено вперше. Чинний від 1997-01-01. –К.: Держстандарт України, 1997. –15 с.

2. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації: Навчальний посібник /За ред. В.О. Хорошка. –К.: НАУ, 2002. -207 с.

3. Северин Л.І., Северин С.Л., Дудатьєв А.В. Правове забезпечення захисту інформації: Навчальний посібник. – Вінниця: ВНТУ, 2004. –145 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход. –К.: ООО «ТИД «ДС», 2004. –992 с.

5. Ярочкин В.И. Предприниматель и безопасность. – М.: «Экспертное бюро», 1994. -Ч.І. –64 с.

6. Указ Президента України "Питання Департаменту спеціальних телекомунікаційних систем та захисту інфо-

ISSN 1727-1584

рмації Служби безпеки України" від 06.10.2000 р., № 1120/2000 // Офіційний вісник України. -2000. -№ 41. -Ст.1745.

7. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт. –Введено вперше. Чинний від 1997-07-01. –К.: Держстандарт України, 1997. –11 с.

8. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації" від 29.12.2000 р., № 89/67 // Офіційний вісник України. -2001. -№ 4. -Ст.155.

9. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23.02.2002 р., № 9 // Офіційний вісник України. -2002. -№ 12. -Ст.624.

Надійшла до редколегії 20.04.2006

БЕРВЕНО С.Л. НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ПОРЯДКА ПРОВЕДЕНИЯ РАБОТ В СФЕРЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Отображен взгляд автора на недостатки существующей нормативной базы в сфере технической защиты информации.

***

BERVENO S.L. NORMATIVE REGULATION ABOUT WORK IN SPHERE OF TECHNICAL PROTECTION OF THE INFORMATION

The sight of the author on lacks of existing normative base of sphere technical protection of the information is displayed.

Р.А. БУЗУНОВ

Донецький юридичний інститут ЛДДУВС

УДК 354.31

ПРОБЛЕМИ ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ У ВИЩОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ СИСТЕМИ МВС[1]

Приділена увага проблемам організації навчального процесу в ВНЗ системи МВС при запровадженні інноваційних модульних систем навчання.

Останнім часом, стає актуальною проблема якісної та належної підготовки працівників ОВС. Детермінантою розгляду цього питання є певні сучасні вимоги до стану забезпечення громадської безпеки, рівня захисту прав та інтересів громадян. Проте, відомо, що належна професійна підготовка працівників ОВС прямо залежить від якісної організації навчального процесу у ВНЗ системи МВС. Працівник органів внутрішніх справ має бути чесною, моральною, професійною, компетентною особою, яка має здатність до постійного самовдосконалення та самонавчання, вправно виконує покладені на неї обов'язки із захисту життя, здоров'я, прав та законних інтересів громадян [1, с.111].

Ситуація що склалася в освітньому середовищі, сьогодні формує певну тенденцію змін в сфері організації навчального процесу в бік інноваційного підходу. Саме останній, зокрема в ВНЗ системи МВС, характеризується втіленням нових гнучких технологій навчання, що дозволяють тому, хто навчається в ВНЗ системи МВС, розвивати свої творчі здібності, отримати навички самоосвіти, самостійної роботи над навчальним матеріалом, отримати практичні навички тощо.

Одним із основних напрямів державної інноваційної політики в сфері відомчої освіти, зокрема, в ВНЗ системи МВС, є запровадження кредитно-модульної системи організації навчального процесу.

Сукупність праць в сфері організації навчального процесу таких авторів як М.І. Ануфрієв, О.М. Бандурка, О.Н. Ярмиш, Я.Я. Болюбаш, В.С. Венедиктов, В.В. Посметний, А.С. Нікуліна, Ю.Б. Максименко, Г.П. Матвєєв, С.А. Заславська, І.Є. Сілаєва, М.П. Костюченко, В.М. Молчанов, Т.Г. Грица та інших стали підґрунтям для цієї статті. Вказаними вченими багато уваги було приділено організації

[1] Первинна рекомендація з напрямку досліджень: докт. юрид. наук Шкарупа В.К. (Нац. академія ДПС).