УДК 351.74: 004.056.55 (477)

ТЕНДЕНЦІЇ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ПРОВЕДЕННЯ РОБІТ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ МВС УКРАЇНИ

Оверченко І.С., здобувач

Національний університет біоресурсів і природокористування України

У статті досліджується діюче законодавство України, яким врегульовується порядок проведення робіт з технічного захисту інформації в системі МВС України.

Ключові слова: інформація, захист інформації, органи внутрішніх справ, технічний захист інформації.

Оверченко И.С. ТЕНДЕНЦИИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОВЕДЕНИЯ РАБОТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ МВД УКРАИНЫ / Национальный университет биоресурсов и природопользования Украины, Украина

В статье исследуется действующее законодательство Украины, которым регулируется порядок проведения работ по технической защите информации в системе МВД Украины.

Ключевые слова: информация, защита информации, органы внутренних дел, техническая защита информации.

Overchenko I.S. TRENDS OF LEGAL REGULATION OF CONDUCT OF WORK ON TECHNICAL PROTECTION OF INFORMATION IN THE SYSTEM OF INTERNAL AFFAIRS OF UKRAINE / National university of life and environmental sciences of Ukraine, Ukraine

The article investigates the current legislation of Ukraine, which regulates the work on technical protection of information in the system of Internal Affairs of Ukraine.

Key words: information, information security, internal affairs bodies, the technical protection of information.

Здійснений нами науковий аналіз досліджень галузі технічного захисту інформації (далі – ТЗІ) [1-6] та чинної нормативно-правової бази [7-10], дозволяє нам дійти висновку про існування певної послідовності робіт з технічного захисту інформації в окремо взятій організації, установі, на підприємстві.

Незважаючи на значну кількість публікацій, присвячених аналізові змісту, послідовності та порядку проведення робіт на кожному з етапів зазначеного виду діяльності, на сьогодні відсутній єдиний, системний підхід до вирішення аналізованих питань. Причому кількість таких робіт коливається від чотирьох (у дослідженні В.А. Петрова, А.С. Піскарьова, А.В. Шеіна [6]) до десяти (у роботі М.В. Мецатуняна [5]) та навіть сорока (Державний стандарт ДСТУ 3396.1-96 [7]).

Водночас, здійснений нами компаративний аналіз наукових доробків та нормативно-правових актів у сфері ТЗІ, дозволив нам виділити основні тенденції з даного питання.

1. Загальноприйнятою є думка щодо необхідності реалізації функцій захисту інформації через створення та підтримку в робочому стані певної системи. Така система не має однозначної назви. Частина авторів, зокрема В.В. Льовкін, А.А. Малюк, В.А. Петров, А.В. Прєлов [3]; В.А. Матвєєв, С.В. Молотков [4] пропонують послуговуватись терміном “система захисту інформації”, інші (наприклад М.В. Мецатунян [5]) користуються дефініцією “комплексна система захисту інформації”. На наш погляд, найбільш вдалою і такою, що відбиває іманентні даній системі ознаки є термін “система технічного захисту інформації”, тому надалі, абстрагуючись від різноманітних і почасти не досить обґрунтованих авторських суб’єктивованих визначень, для позначення цієї системи ми застосували саме дане поняття.
2. Здійснений нами догматико-юридичний аналіз дозволив виділити чотири етапи проведення робіт з ТЗІ [7-10]:
   - розроблення системи технічного захисту інформації;
   - впровадження системи ТЗІ;
   - дослідження ефективності системи ТЗІ;
   - обслуговування (супроводження) СТЗІ.

Не дивлячись на те, що класифікація заходів за вказаними етапами не завжди використовується в наукових дослідженнях, що стосуються даної проблематики, роботи, які згідно з чинними

нормативними документами пропонується виконати, у сукупності вказані як обов'язкові в більшості наукових досліджень, зокрема В.А. Петрова, А.С. Піскарьова, А.В. Шеіна [3], В.А. Матвєєва, С.В. Молоткова [4], М.В. Мецатуняна [5], Ю.Я. Самохвалова, В.О. Темнікова, В.О. Хорошка [11], Л.І. Северина, С.Л. Северина, А.В. Дудатьєва [12].

Разом із цим, у частині нормативних документів [6-5] згадується ще один етап робіт – дослідження (або аналіз) об'єктів інформаційної діяльності. На даному етапі мають бути проведені [9]: вивчення та аналіз проектної, програмної документації, інформаційних потоків, у тому числі із застосуванням засобів пошукової та вимірювальної техніки, умов функціонування об'єктів інформаційної діяльності, інформаційних систем з метою визначення загрози безпеці інформації щодо її витоку, блокування чи порушення цілісності. Причому етап дослідження має передувати іншим, вказаним вище.

На необхідності проведення дослідження особливостей функціонування об'єкта інформаційної діяльності як початкового етапу в процесі створення системи ТЗІ підприємства зазначено в роботах більшості авторів, що досліджують різноманітні питання у сфері ТЗІ. Такої думки дотримуються Ю.Я. Самохвалов, В.О. Темніков, В.О. Хорошко [11], В.В. Льовкін, А.А. Малюк, В.А. Петров, А.В. Прєлов [3], М.В. Мецатунян [5], Л.І. Северин, С.Л. Северин, А.В. Дудатьєв [12].

3. Наявні в чинній нормативно-правовій базі розходження з питання визначення етапу дослідження об'єктів інформаційної діяльності як обов'язкового в процесі створення системи ТЗІ мають значний негативний вплив на процеси створення та подальшого функціонування систем ТЗІ в організаціях та на підприємствах України, що керуються у своїй діяльності зазначеною базою. Закріплення даного етапу в одних нормативних документах та його відсутність в інших, у процесі створення систем ТЗІ на підприємствах, в установах, організаціях призводить до недооцінки важливості робіт, що мають бути проведені в процесі дослідження об'єктів інформаційної діяльності.

Підсумовуючи викладене, зауважимо, що в органах внутрішніх справ, як складовій системи державних органів, відносно яких здійснюється технічний захист інформації, порядок проведення робіт на етапі дослідження об'єктів інформаційної діяльності залишається і зараз не визначеним чітко. Поряд із детальною регламентацією інших чотирьох етапів проведення робіт з ТЗІ діючою нормативно-правовою базою (у тому числі – відомчими наказами та вказівками), така ситуація дозволяє нам дійти висновку про приділення недостатньої уваги до даного етапу з боку законодавця, а відтак – про необхідність комплексного вивчення даної проблеми в рамках здійснюваного нами дослідження з метою встановлення та обґрунтування потреби його проведення, а також визначення змісту даного етапу відносно об'єктів інформаційної діяльності органів внутрішніх справ.

При цьому під об'єктами інформаційної діяльності (ОІД), відповідно до чинної нормативно-правової бази, ми розуміємо: інженерно-технічні споруди, приміщення з визначеною контрольованою зоною, де здійснюється адміністративна, фінансово-економічна, науково-технічна та інша діяльність, пов'язана з інформацією, що підлягає захисту від витоку технічними каналами та спеціальних впливів.

Для об'єкта інформаційної діяльності кваліфікуючими будуть наступні ознаки:
1) ОІД може бути або приміщенням, або інженерно-технічною спорудою;
2) у такому приміщенні або споруді здійснюється діяльність, пов'язана з інформацією, що підлягає захисту від витоку технічними каналами та спеціальних впливів.

Слід зауважити, що для позначення даного етапу в нормативно-правових актах пропонується декілька назв: етап визначення й аналізу загроз [7], етап проведення обстеження підприємства [8], етап дослідження об'єктів інформаційної діяльності, інформаційних систем щодо безпеки інформації [9, 10].

Поряд із цим, здійснений нами формально-юридичний та герменевтичний аналіз положень нормативних документів, що містять переліки та опис робіт для вказаних вище етапів, дозволяє нам резюмувати: незважаючи на відмінності в найменуваннях, насправді йдеться про один і той же етап проведення робіт із технічного захисту інформації, оскільки перелік робіт, які мають проводитися на даному етапі, включає в себе досить різноманітні напрями. Втім їх спільною

рисою є те, що всі вони спрямовані на отримання та аналіз інформації про особливості функціонування об'єкта, інформація якого підлягає технічному захистові.

Визначити назву даного етапу, яка найбільш повно відображає його зміст, можливо виключно на підставі детального вивчення робіт, що мають бути проведені в процесі його реалізації.

У цьому зв'язку слід зауважити, що нині значна кількість фахівців сфери ТЗІ у своїх дослідженнях, присвячених питанням послідовності та змісту робіт з технічного захисту інформації, намагається визначити перелік робіт, явно недостатню увагу приділяючи встановленню напрямів проведення таких робіт. Така ситуація актуальна і для чинної нині нормативної бази.

Так В.В. Льовкін, А.А. Малюк, В.А. Петров, А.В. Прєлов [3] називають наступні види робіт, що мають бути проведені на першій стадії створення системи ТЗІ: аналіз складу і змісту конфіденційної інформації, визначення її цінності; опис об'єкта захисту, його елементів: робочих місць, приміщень, будинків, території, засобів обробки інформації, зв'язку, сигналізації, наявних засобів захисту інформації; вимірювання характеристик елементів об'єкта захисту. Причому авторами пропонується визначення даного етапу як передпроектної стадії.

В.А. Матвєєв та С.В. Молотков [4] до робіт, що мають бути проведені на даному етапі, включають аналіз уразливих елементів об'єкта; аналіз можливих загроз; оцінку ризику. Однак окремим етапом дана сукупність робіт у дослідженні не визначена, тобто вказані роботи входять до загального переліку дій зі створення системи ТЗІ.

Л. Кєдровська та В. Ярочкін [2] пропонують даний етап вважати етапом аналізу об'єкта захисту з вивченням наступних напрямків: установлення складу інформації, що потребує захисту; визначення найбільш важливих елементів інформації, що захищається; встановлення терміну життя критичної інформації (час, необхідний конкуренту для реалізації добутої інформації); ключових елементів інформації (індикаторів), що відображають характер охоронюваних даних; проведення класифікації індикаторів по функціональних зонах (виробничо-технологічні процеси, система матеріально-технічного забезпечення, підрозділу керування і т.д.).

Згідно з Державним стандартом ДСТУ 3396.0-96 [7] на етапі визначення й аналізу загроз реалізуються: аналіз об'єктів захисту, ситуаційного плану, умов функціонування підприємства; оцінка ймовірності прояву загроз та очікуваної шкоди від їх реалізації; підготовка засадничих даних для побудови окремої моделі загроз. Державний стандарт ДСТУ 3396.1-96 [8] містить більш детальний перелік, який складається з дев'яти видів робіт.

У цій ситуації, ми вважаємо недоцільним ставити собі на меті обрання одного з вказаних переліків як такого, що, за нашим переконанням, включить в себе всі види робіт з технічного захисту інформації першого етапу створення системи ТЗІ. Так само, відсутня необхідність у виробленні власного авторського переліку. Ми переконані, що створення універсального вичерпного переліку робіт неможливе в принципі – адже у кожному випадку створення системи технічного захисту інформації конкретного підприємства можливе проведення й інших заходів, залежно від особливостей його функціонування.

Тоді головним завданням, яке має бути вирішене в процесі дослідження змісту робіт з технічного захисту інформації на початковому етапі створення системи ТЗІ, ми вважаємо визначення напрямів проведення таких робіт. У якості бази такого дослідження нами було обрано Державний стандарт ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт" [8]. Наш вибір обумовлено наступними чинниками.

По-перше, на наше переконання, напрями проведення початкових робіт після свого визначення мають бути закріплені саме у нормативних документах, що регулюють порядок проведення робіт зі створення системи ТЗІ поряд із переліками робіт, які містяться в них на цей час. Причому переліки робіт не мають бути вичерпними, адже в кожному з напрямів можливе проведення й інших заходів, залежно від особливостей функціонування підприємства. Замість цього перелік робіт повинен мати характер мінімально необхідного для створення системи ТЗІ – це дозволить значно розширити можливість використання при їх проведенні останніх наукових доробків.

По-друге, як свідчить проведений нами контент-аналіз чинної нормативно-правової бази, на сьогодні саме обраний нормативний документ слід визнати як такий, що містить найбільш повну сукупність таких робіт. Причому, з урахуванням того факту, що даний Державний стандарт набрав чинності 1997 року, постійно використовується в роботі підрозділів ТЗІ і до цього часу не зазнав змін, маємо підстави зробити аргументований висновок про можливість визнання визначеного ним переліку робіт, як такого, що підтверджений часом.

Таким чином, підбиваючи підсумок, хотіли б запропонувати класифікувати запропоновані в Державному стандарті [8] заходи за об'єктом здійснюваного на етапі їх проведення аналізу наступним чином:

– аналіз місця розташування об'єкта (до даного виду робіт входять заходи щодо аналізу умов функціонування підприємства, його розташування на місцевості (ситуаційного плану), для визначення можливих джерел загроз);

– дослідження технічних умов функціонування об'єкта (дослідження засобів забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території; вивчення схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій; визначення наявності та технічного стану засобів забезпечення ТЗІ; виявлення наявності транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів; визначення технічних засобів і систем, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню; визначення технічних засобів, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ);

– дослідження інформаційних умов функціонування об'єкта (дослідження інформаційних потоків та технологічних процесів оброблення інформації; перевірка наявності на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію та проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує інформаційну діяльність).

Запропонована класифікація дозволить отримати уявлення про напрями діяльності, які пропонується реалізувати на початковому етапі створення системи технічного захисту інформації.

ЛІТЕРАТУРА

1. Давыдовский А.И. Методология построения безопасных процессов обработки информации / А.И. Давыдовский // Безопасность информационных технологий. – 1994. – № 1. – С. 63-65.

2. Кедровская Л. Коммерческая тайна в условиях рыночной экономики / Л. Кедровская, В. Ярочкин // Информационные ресурсы России. – 1992. – № 5-6. – С. 11-15.

3. Проблемы автоматизированной разработки технического задания на проектирование системы защиты информации / [В.В. Левкин, А.А. Малюк, В.А. Петров, А.В. Прелов] // Безопасность информационных технологий. – 1994. – № 1. – С. 40-44.

4. Матвеев В.А. Специфика обеспечения безопасности информационных технологий / В.А. Матвеев, С.В. Молотков // Безопасность информационных технологий. – 1995. – № 1. – С. 43-50.

5. Мецатунян М.В. Некоторые вопросы проектирования комплексных систем защиты информации / М.В. Мецатунян // Безопасность информационных технологий. – 1995. – № 1. – С. 53-54.

6. Петров В.А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах / В.А. Петров, А.С. Пискарев, А.В. Шеин. – М.: МИФИ, 1995. – 48 с.

7. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1997-01-01]. – К.: Держстандарт України, 1997. – 15 с. – (Національний стандарт України).

8. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – [Чинний від 1997-07-01]. – К.: Держстандарт України, 1997. – 11 с. – (Національний стандарт України).

9. 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: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29.12.2000 № 89/67, зареєстрований в Міністерстві юстиції України 20.01.2001 за № 50/5241 / [Електронний ресурс]. – Режим доступу: www.rada.gov.ua.

10. 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 23.02.2002 № 9, зареєстрований в Міністерстві юстиції України 13.03.2002 за № 245/6533 / [Електронний ресурс]. – Режим доступу: www.rada.gov.ua.

11. Самохвалов Ю.Я. Організаційно-технічне забезпечення захисту інформації: [навч. посіб.] / Ю.Я. Самохвалов, В.О. Темніков, В.О. Хорошко ; за ред. В. О. Хорошка. – К.: НАУ, 2002. – 207 с.

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

УДК 351.713(477)

КЛАСИФІКАЦІЯ АДМІНІСТРАТИВНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ОПОДАТКУВАННЯ

Огороднікова І.І., аспірант

Національний університет державної податкової служби України

У статті досліджено та проаналізовано критерії класифікації правопорушень у сфері оподаткування, за які передбачена адміністративна відповідальність.

Ключові слова: класифікація, критерії, адміністративна відповідальність, правопорушення в сфері оподаткування.

Огородникова И.И. КЛАССИФИКАЦИЯ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ НАЛОГООБЛОЖЕНИЯ / Национальный университет государственной налоговой службы Украины, Украина

В статье исследованы и проанализированы критерии классификации правонарушений в сфере налогообложения, за которые предусмотрена административная ответственность.

Ключевые слова: классификация, критерии, административная ответственность, правонарушение в сфере налогообложения.

Ogorodnikova I.I. CLASSIFICATION ADMINISTRATIVE OFFENCES IN THE FIELD OF TAXATION / National university of the state tax service of Ukraine, Ukraine

In the article investigational and analysed criteria of classification of offences in the field of taxation, which administrative responsibility is foreseen for.

Key words: classification, criteria, administrative responsibility, offence in the sphere of taxation.

Останнім часом спостерігається певна динамічність норм українського адміністративного та податкового законодавства, що обумовлено політичними, економічними, правовими, культурологічним чинниками. Певних змін у свою чергу зазнало і законодавство, що регулює інститут адміністративної відповідальності за правопорушення в сфері оподаткування.

Відповідно до змін, несених до Закону України «Про державну податкову службу в Україні» Законом України від 25.03.2005 р. № 2505-IV IV (у редакції Закону № 2154-VI (2154-17) від 27.04.2010 – зміни застосовуються у 2010 році) [1], органам ДПС України надано право застосовувати до платників податків фінансові (штрафні) санкції, стягувати до бюджетів та