діяльність" від 18 лютого 1992 р. [WWW документ]. URL http://www.rada.kiev.ua (10 серпня 2009). ***33.*** *Верховна Рада України (22. 12. 1994). Закон України "Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів" від 22 грудня 1994 р. [WWW документ]. URL http://www.rada.kiev.ua (10 серпня 2009).* ***34.*** *Сергиенко Л. А. Защита персональных данных и Інтернет // Информационное общество. - 2000. - № 4. - С. 44-45.*

УДК 351.9:347.447.52 Б19

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ, ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНФОРМАЦІЙНО ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Олександр Бакалинський, Олександр Богданов, Володимир Мохор

Інститут спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Анотація: **Розглянуто питання відповідальності за порушення законодавства в сфері захисту інформації.**

*Summary:***The question of responsibility for violating the law in protection of information.**

Ключові слова: **Інформація, інформаційна безпека, захист інформації, юридична відповідальність.**

Вступ

Захист інформаційних ресурсів є одним із пріоритетних завдань національної безпеки України. Інформація як результат інтелектуальної творчої діяльності має колосальний потенціал забезпечення ефективного державного управління, розвитку громадянського суспільства та впливу на свідомість, підсвідомість і поведінку людини. Інформаційна сфера в сучасних умовах перетворилась на арену боротьби за світове лідерство та інформаційні впливи на відповідні країни і регіони. В основі цієї боротьби знаходиться добування достовірної і повної інформації про конкурентів і супротивників та країн, що віднесені до інтересів лідерів у сфері інформаційних технологій. Все це підносить інформацію як соціальну зброю, породжує проблеми захисту інформаційних ресурсів та інформації у сфері її обігу [1].

Основна частина

У процесі будівництва суверенної і незалежної держави йде пошук шляхів створення і вдосконалення науково обґрунтованої, економічно доцільної системи захисту інформації, в тому числі в процесі міжнародного співробітництва. Базою державної внутрішньої і зовнішньої політики у сфері захисту інформації мають виступати демократичні правові цінності: ідеї прав і свобод людини і громадянина, верховенство права, повага до інтересів і прав суверенних і незалежних держав тощо.

В інформаційній сфері, особливо пов'язаної із захистом інформації, залишаються нерозв'язаними проблеми щодо створення загальної системи захисту інформації; між чинними актами інформаційного законодавства існують суттєві суперечності, що порушують системність законодавства та не сприяють забезпеченню законності в інформаційній діяльності; мають місце непоодинокі факти порушення прав і свобод громадян підзаконними актами; організаційна структура державних органів, спеціальних підрозділів і служб не забезпечує формування і стале функціонування комплексної системи інформаційної безпеки та всіх складових захисту інформації. Крім того, в існуючому законодавстві існує ряд прогалин.

Європейське спрямування розвитку України, входження її до Світової організації торгівлі, проблеми електронного урядування країною диктують необхідність впровадження норм міжнародного права в національну правову систему. З метою забезпечення надійного захисту інформації та організації управління інформаційною безпекою в Україні ведеться робота над націоналізацією міжнародного стандарту ISO/IEC 27001:2005 "Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги" [2], який дозволить не тільки будувати Систему управління інформаційною безпекою (далі – СУІБ) будь-якої організації, але й проводити сертифікацію відповідності цієї системи. Історія цього стандарту почалась з 1995 року виходом британського стандарту BS 7799-1:1995. Протягом багатьох років цей стандарт вбирав в себе найкращі практики в сфері захисту інформації, побудови та розвитку СУІБ та став першим у серії лінійки міжнародних стандартів ISO/IEC 27000. Враховуючи на те, що у 2009 році очікується прийняття цього стандарту як національного, це породжує багато питань. Пункт А.15 додатку А цього стандарту рекомендує при побудові СУІБ складати в організації перелік всього законодавства, в правовому полі якого організація

спрямовує свою діяльність. Крім того, при розробці посадових обов'язків, враховувати всю, відповідну кожній посаді в організації, відповідальність за безпеку (п. А.8.1), визначати відповідальності за порушення вимог захисту інформації задля включення їх до договорів з партнерами, клієнтами. З метою прозорості в питаннях дисциплінарної практики та правового інформування підлеглих необхідно розробляти дисциплінарні заходи, які мають бути залежними від ваги скоєних порушень. Таким чином, стало актуальним розібратися з питаннями визначення відповідальності за порушення встановленого порядку захисту інформації, дослідивши українське законодавство в цій підгалузі інформаційного права.

З 1 січня 2006 року набрав чинності Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [3] (далі – Закон), який регулює відносини в сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – системах). Він був прийнятий на зміну Закону України «Про захист інформації в автоматизованих системах», який був морально застарілий і не відповідав вимогам сьогодення. Весь Закон коментувати не будемо, а звернемо увагу на статтю 11, в якій сказано, що: «Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно з законом» [3]. Приблизно таке ж саме формулювання зустрічаємо в Положенні про порядок здійснення криптографічного захисту інформації в Україні [4], стаття 14 якого каже про те, що: «У разі порушення вимог щодо порядку здійснення криптографічного захисту інформації суб'єкти підприємницької діяльності, установи, організації, посадові особи та громадяни несуть відповідальність згідно з законодавством України». В Положенні про технічний захист інформації в Україні [8] (стаття 22) теж сказано, що: «У разі порушення вимог щодо забезпечення технічного захисту інформації посадові особи та громадяни несуть відповідальність згідно з законодавством України». Такий же вигляд має і стаття 11 проекту Закону України «Про захист інформації» [5], яка визначає відповідальність за порушення законодавства про захист інформації наступним чином: «Юридичні та фізичні особи, винні в порушенні законодавства про захист інформації, несуть дисциплінарну, цивільну, адміністративну чи кримінальну відповідальність згідно з законодавством». В цьому законопроекті більш чітко визначається, що відповідальність повинні нести: «Юридичні та фізичні особи». Як видно, ця норма носить бланкетний характер і відсилає до норм чинного законодавства, що аж ніяк не сприяє визначеності правового регулювання в сфері захисту інформації. Хочеться зауважити, що в українському законодавстві юридичні особи кримінальну та адміністративну відповідальність не несуть, хоча необхідно відзначити, що в науковій літературі та в кодексах деяких держав (наприклад, Росії) існують розбіжності щодо питання про те, чи можуть юридичні особи нарівні з фізичними бути суб'єктами адміністративної відповідальності. Одні автори вважають, що три види юридичної відповідальності – кримінальна, адміністративна, дисциплінарна – настають виключно за винні діяння і розраховані за самою своєю сутністю лише на фізичних осіб. Інші вимагають встановлення адміністративної відповідальності за протиправні або за протиправні винні діяння фізичних і юридичних осіб. Треті, з огляду на першу позицію – адміністративної відповідальності лише фізичних осіб, доповнюють її відносно юридичних осіб у такий спосіб: для юридичних осіб у сфері державного управління має передбачуватися фінансова відповідальність, супроводжувана адміністративною, дисциплінарною чи кримінальною відповідальністю посадових осіб, конкретно особистої відповідальності винних у вчиненні відповідного правопорушення – проступку або злочину [6]. На наш погляд третій варіант є найбільш доречним.

Між тим, бачимо, що таке формулювання щодо необхідності встановлення відповідальності за порушення в сфері захисту інформації породжує ряд питань.

1. Які саме діяння і за яких обставин є порушенням законодавства про захист інформації в системах?
2. Які саме особи і в якому порядку можуть бути визнані винними в порушенні законодавства щодо захисту інформації в системі?
3. Яку саме відповідальність і в якому порядку несуть ці особи?

Спробуємо розібратись. Які саме діяння і за яких обставин є порушенням законодавства про захист інформації в системах? На наш порушенням законодавства може вважатись декілька діянь.

1. Порушення умов:
   - 1.1 визначених власником системи на підставі його договорів з власником інформації, відповідно до яких користувач отримав можливість виконання однієї або кількох операцій з інформацією, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання;
   - 1.2 договору власником системи щодо забезпечення захисту інформації в системі, укладеного з власником інформації;
   - 1.3 виконання однієї або кількох операцій з інформацією, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання без застосування в системі комплексної системи захисту інформації, або з застосуванням такої системи з не підтвердженою відповідністю;

1.4 створення власником системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, служби захисту інформації, або не призначення осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

2. Порушення правил обробки інформації, тобто правил, згідно з якими виконується одна або кілька операцій з інформацією: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Таким чином, правопорушенням буде вважатись як порушення умов, так і порушення правил, або порушення і умов, і правил одночасно. Крім того, необхідно зауважити, що до складу комплексної системи захисту інформації входять комплекс засобів криптографічного захисту та комплекс засобів технічного захисту інформації [7], тому порушення вимог Положення про порядок здійснення криптографічного захисту інформації в Україні [4] та Положення про технічний захист інформації в Україні [8] також може вважатися порушенням законодавства про захист інформації в системі.

В Положенні про державний контроль за станом технічного захисту інформації [9] (далі – ТЗІ) визначено кваліфікацію порушень з ТЗІ: п. 5.1. Порушення вимог з ТЗІ поділяються на три категорії, які визначають можливість реалізації загроз безпеці інформації:

- перша категорія – невиконання вимог нормативно-правових актів та нормативних документів з ТЗІ, внаслідок чого створюється реальна можливість порушення конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами, цілісності й доступності інформації;
- друга категорія – невиконання вимог нормативно-правових актів та нормативних документів з ТЗІ, внаслідок чого створюються передумови до порушення конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами, цілісності й доступності інформації;
- третя категорія – невиконання інших вимог з ТЗІ.

В тому ж Положенні [9] визначаються і кваліфікаційні ознаки порушень з технічного захисту інформації (п. 5.2). Ознаками порушень першої категорії є:

- встановлення факту циркуляції інформації з обмеженим доступом на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умов підтвердження інструментально-розрахунковими методами наявності технічного каналу поширення інформації з обмеженим доступом;
- встановлення факту обробки інформації з обмеженим доступом в інформаційних або інформаційно-телекомунікаційних системах, які мають вихід незахищеними каналами зв'язку за межі контрольованої зони, за умов відсутності атестата відповідності на комплексну систему захисту інформації;
- встановлення факту обробки інформації з обмеженим доступом в інформаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умов доступу до їх інформаційних ресурсів користувачів, які мають різні повноваження (права доступу до інформації), та відсутності атестата відповідності на комплексну систему захисту інформації;
- встановлення факту несанкціонованого доступу користувачів інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем до інформації з обмеженим доступом шляхом порушення встановлених правил розмежування доступу або подолання заходів захисту.

Ознаки порушень другої категорії:

- встановлення факту циркуляції інформації з обмеженим доступом на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умов відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;
- встановлення факту обробки інформації з обмеженим доступом в інформаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умов відсутності атестата відповідності на комплексну систему захисту інформації.

Невиконання вимог нормативно-правових актів щодо впровадження організаційних заходів з ТЗІ, а також інших норм та вимог у сфері захисту інформації, які не призводять до порушень першої або другої категорії, кваліфікується як порушення третьої категорії.

В Положенні про порядок здійснення криптографічного захисту інформації в Україні [4] так чітко, як в попередньому документі, не визначено кваліфікацію порушень, але також можна зробити висновок, що невиконання вимог цього Положення тягне за собою негативні наслідки для осіб, які його порушують. Це може бути проведення діяльності, яка пов'язана з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації без отримання ліцензії Держспецзв'язку, використання для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, криптосистем і засобів криптографічного захисту, які не допущені до експлуатації, використання для криптографічного захисту конфіденційної інформації криптосистем і засобів криптографічного захисту, які не мають сертифікату відповідності та інше. Можливо цей перелік можна і продовжувати: тут буде відповідальність за

порушення при використанні електронного цифрового підпису (ст. 15) [10], електронного документообігу (ст. 18) [11], можливість вигадувати види правопорушень, тому що вони прямо не вказані. І ось тут і виникають складнощі в застосуванні такого поняття як юридична відповідальність за порушення в сфері захисту інформації. Чому? Тому що юридична відповідальність – це передбачені законом вид і міра державно-владного примусового (у формі каральних і правовідновлюючих чи або компенсаційних способів) зазнання особою втрат благ особистого, організаційного та майнового характеру за вчинене правопорушення, а підставами юридичної відповідальності є склад правопорушення, деліктоздатність (осудність, дієздатність) суб'єкта, його вік і наявність законодавства [1]. А ми маємо проблеми з повним переліком правопорушень в цій сфері, а відповідно до цього і з визначенням складу правопорушення та складнощі з визначенням повного переліку законодавства, яке визначає ці правопорушення. Звідси випливає необхідність кодифікації взагалі всього інформаційного законодавства, про що мова йде вже більше 10 років [12]. Це спростило би відповідним органам державної влади виконання функцій, покладених на них державою, а також впорядкувало б правозастосовчу діяльність.

Для відповіді на питання: «Які саме особи і в якому порядку можуть бути визнані винними у порушенні законодавства щодо захисту інформації в системі» необхідно розглянути види юридичної відповідальності залежно від галузевої структури права. Це дозволить одночасно відповісти і на питання: «Яку саме відповідальність і в якому порядку несуть ці особи». Розрізняють такі види юридичної відповідальності: кримінальну, адміністративну, цивільно-правову, дисциплінарну, матеріальну [6]. Існує ще конституційна відповідальність, але вона лежить за межами нашого дослідження.

Кримінальна відповідальність має юридичною підставою Кримінально-процесуальний кодекс України [13] та настає за вчинення злочинів, вичерпний перелік яких міститься в Кримінальному кодексі [14], тобто встановлюється лише законом, настає з моменту офіційного обвинувачення, реалізується виключно в судовому порядку. Заходи кримінальної відповідальності застосовуються лише в судовому порядку. Правозастосовний акт – вирок. Застосовується тільки до фізичних осіб.

Адміністративна відповідальність має юридичною підставою Кодекс України про адміністративні правопорушення [15] та накладається за адміністративні правопорушення органами державного управління (органами так званої адміністративної юрисдикції) та адміністративними судами до осіб, що не підпорядковані їм по службі. Правозастосовним актом є рішення. Згідно галузевому кодексу застосовується до фізичних осіб, але за практикою останніх років та відповідно до деяких Законів України [16] може застосовуватись і до юридичних осіб.

Дисциплінарна відповідальність має юридичною підставою Кодекс законів про працю [17] та накладається адміністрацією підприємств, установ, організацій (особою, що має розпорядчо-дисциплінарну владу над конкретним працівником) внаслідок вчинення дисциплінарних проступків: 1) відповідно до правил внутрішнього трудового розпорядку; 2) в порядку підпорядкованості; 3) відповідно до дисциплінарних статутів і положень. Реалізується виключно в рамках службової підпорядкованості. Правозастосовний акт – наказ. Застосовується до фізичної особи.

Матеріальна (юридична підстава – Кодекс законів про працю [17]) настає за вчинене майнове правопорушення, шкоду, заподіяну підприємству, установі, організації робітниками та службовцями (фізична особа) при виконанні ними своїх трудових обов'язків. Притягає до відповідальності адміністрація підприємства. Правозастосовний акт – наказ.

Цивільна відповідальність має юридичною підставою Цивільно-процесуальний кодекс [18] та настає з моменту правопорушення – невиконання договірного зобов'язання майнового характеру у встановлений строк або виконання неналежним чином, заподіяння позадоговірної шкоди (цивільно-правового проступку) або здоров'ю чи майну особи, її особливість полягає у добровільному виконанні правопорушником відповідальності без застосування примусових заходів. Державний примус використовується у разі виникнення конфлікту між учасниками цивільних правовідносин. Питання про притягнення суб'єкта (фізичної або юридичної особи) до цивільно-правової відповідальності вирішується судом, арбітражним судом або адміністративними органами держави за заявою учасника правовідносини або потерпілого. Правозастосовний акт – постанова.

Таким чином, ми встановили, що залежно від ступеня тяжкості скоєного правопорушення проти встановленого порядку захисту інформації та негативних наслідків, які наступили внаслідок цього правопорушення, можуть наступати різні види юридичної відповідальності, або навіть їх комбінації, виходячи з вимог ст. 61 Конституції України [19]: "Ніхто не може бути двічі притягнений до юридичної відповідальності одного виду за одне й те саме правопорушення".

Що стосується самої особи – суб'єкта правопорушення, то на підставі аналізу чинного законодавства можна зробити висновок, що суб'єктами вчинення протиправних діянь проти встановленого порядку захисту інформації (а відповідно до цього, проти встановленого порядку управління) є фізичні особи, більше того – це посадові особи (спеціальний суб'єкт). Вік настання відповідальності становить 16 років. Також фізичних осіб може торкнутися дисциплінарна, матеріальна та цивільно-правова відповідальність. На підставі п. 6, 7 ст. 17 Закону України "Про Державну службу спеціального зв'язку та захисту

інформації України" [16] від 23 лютого 2006 року можемо зробити висновок, що адміністративну відповідальність за правопорушення в сфері захисті інформації можуть нести і юридичні особи шляхом зупинення дії, або скасування ліцензій (Стаття 17. Права Державної служби спеціального зв'язку та захисту інформації України…).

6) зупиняти дію або скасовувати в установленому порядку ліцензії на провадження господарської діяльності у сфері криптографічного та технічного захисту інформації, а також дозволів на проведення робіт з технічного захисту інформації для власних потреб органам державної влади;

7) порушувати в установленому порядку питання про припинення інформаційної діяльності з використанням інформаційно-телекомунікаційних систем в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності у разі порушення ними вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та/або технічного захисту інформації…).

Також юридичні особи можуть нести і цивільно-правову відповідальність.

У зв'язку з тим, що юридична відповідальність – один із специфічних проявів загальносоціальної відповідальності, який відповідно до особливостей права прямо виражає його державно-владну природу і, не перекриваючись іншими правовими явищами (правосвідомістю, законністю), торкається головним чином наслідків за неправомірну, безвідповідальну з точки зору закону, поведінку [20], хотілося б торкнутись безпосередньо питання, яке пов'язане з настанням негативних наслідків порушення законодавства про захист інформації. Як було відмічено раніше, вид юридичної відповідальності має визначатися виходячи із ступеню соціальної небезпеки скоєного правопорушення та важкості негативних наслідків. Таким чином, якщо неправомірне діяння є злочином, то застосовуються жорсткі заходи кримінального покарання, які впливають на особу винного.

Наприклад, внаслідок невиконання або порушення вимог Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3], можуть бути створені умови для скоєння злочинів, які передбачені Кримінальним кодексом України [14]. Можемо перерахувати тільки деякі з них.

Стаття 111. Державна зрада (у формі шпигунства).

Стаття 114. Шпигунство.

Стаття 328. Розголошення державної таємниці

1. …карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого;

2. те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від п'яти до восьми років.

Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, – карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Ці злочини можуть бути скоєнні, наприклад, при порушенні вимог статті 4 Закону [3], яка визначає порядок організації доступу до інформації в системі.

Крім того, посадові особи, яким прямо вказано на необхідність проводити роботи з захисту інформації (в їх посадових обов'язках), у разі невиконання своїх обов'язків, що заподіює істотну шкоду охоронюваним законом правам, свободам та інтересам окремих громадян, або державним чи громадським інтересам, або інтересам окремих юридичних осіб, можуть бути притягнуті до кримінальної відповідальності за статтями 364 (Зловживання владою або службовим становищем) або 367 (Службова недбалість) [14]. Такими посадовими особами можуть бути і власники системи, на яких статтею 9 Закону [3] покладається відповідальність за забезпечення захисту інформації в системі.

Адміністративна відповідальність за недодержання вимог законодавства щодо захисту інформації в системах може наступати відповідно до статті 188-31 Кодексу України про адміністративні правопорушення [15]: «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про

криптографічний та технічний захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, та законодавства у сфері надання послуг електронного цифрового підпису, а також створення інших перешкод для виконання покладених на них обов'язків, – тягнуть за собою накладення штрафу на посадових осіб від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян. Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, – тягнуть за собою накладення штрафу на посадових осіб від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян». Доречи, ця стаття є новелою українського законодавства та прикладом закриття прогалин в законодавстві.

Крім того, в Кодексі України про адміністративні правопорушення [15] стаття 212-2 визначає відповідальність за порушення законодавства про державну таємницю, а саме: ...

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності, – тягне за собою накладення штрафу на громадян від одного до трьох неоподатковуваних мінімумів доходів громадян і на посадових осіб – від трьох до десяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на громадян від трьох до восьми неоподатковуваних мінімумів доходів громадян і на посадових осіб – від п'яти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян.

До юридичних осіб адміністративна відповідальність застосовується на підставі розглянутої вище п. 6, 7 ст. 17 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" [16] та ст. 3 Положення про державний контроль за станом технічного захисту інформації [9], в якій сказано, що посадові особи Держспецзв'язку, які здійснюють перевірки стану ТЗІ, мають право: «порушувати в установленому порядку питання щодо зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов'язаної з державною таємницею, у разі виявлення порушень з технічного захисту секретної інформації; складати протоколи про адміністративні правопорушення та надавати до суду на розгляд справи про адміністративні правопорушення».

Засоби дисциплінарної, матеріальної відповідальності встановлюються на підприємстві, в організації, установі залежно від вимог Кодексу законів про працю, види стягнень там перераховані вичерпно. Заходи цивільно-правової відповідальності – відшкодування майнових втрат, скасування незаконних угод, штраф, пеня та інші міри, які полягають у примушуванні особи нести негативні майнові наслідки, повинні застосовуватись на підставі рішення суду, який і має визначати ту міру відповідальності, яка відповідає скоєному правопорушенню.

Висновки

Значним недоліком чинного українського законодавства, зокрема в інформаційній сфері (а також і в сфері захисту інформації в системах), є його неконкретність, певна розмитість формулювань. Фактично відсутні формулювання правопорушень у сфері захисту інформації, визначення конкретних механізмів притягнення до відповідальності осіб, які повинні у вчинені правопорушень проти встановленого порядку захисту інформації, а відповідно і проти встановленого порядку управління. Чинна законодавча та нормативна база не встановлює відповідальності за порушення норм в систематизованому вигляді, всі норми знаходяться в різних Кодексах. Можливо привести висловлювання доктора Бернарда Шлоера, експерту програми TACIC відносно оцінки деяких законодавчих актів України: «Законодавство про інформацію має ознаки того, що межі його ясного і зрозумілого сприйняття ось-ось залишаться позаду» [20], зробленого ще в кінці 90-х років. З тих пір суттєвих змін не сталося. Не зважаючи на більш ніж десятирічну дискусію з приводу необхідності кодифікації інформаційного законодавства, досі такого нормативно-правового акту не прийнято. Тому вважаємо за необхідне створення такого Кодексу.

З метою гармонізації українського законодавства з міжнародним, необхідно як найшвидше прийняти міжнародний стандарт ISO/IEC 27001:2005 як національний, залучивши до експертизи української версії фахівців Держспецзв'язку.

Недостатня увага до проблем захисту інформаційної інфраструктури та інформаційних ресурсів ускладнює діяльність держави щодо забезпечення національної безпеки і обороноздатності держави [20]. Важливим напрямом інформаційної безпеки залишається забезпечення технічного захисту інформації в міністерствах і відомствах та насамперед в інформаційно-телекомунікаційних системах, які забезпечують виконання цими органами функцій держави. Основною причиною подібного стану є нехтування керівництвом державних установ вимогами захисту інформації, що виявляється у відсутності відповідальних за захист інформації осіб, відповідних відомчих нормативних документів, а також чітко не встановленою мірою відповідальності. Таким чином, необхідно розробити певний перелік правопорушень та відповідні до правопорушень міри відповідальності.

На наш погляд, має сенс криміналізувати діяння, які спрямовані проти встановленого порядку захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах, тому що в наслідок таких діянь можуть бути скоєні злочини, які описані в будь-якому розділі Кримінального кодексу.

Необхідно провести дослідження напрямків удосконалення процесу державного управління в сфері захисту інформації, організації, взаємодії та координації діяльності всіх органів державної влади та інших суб'єктів відносин, пов'язаних із захистом інформації в системах.

*Література:**1**. Курс інформатизації управління в ОВС / Під заг. ред. професора Я. Ю Кондратьєва, www.naiau.kiev.ua/biblio/books/inform_OVS. **2**. Міжнародний стандарт ISO/IEC 27001:2005 "Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою - Вимоги". **3**. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5.06.1994 р., чинний від 1.01.2006 р., www.rada.gov.ua. **4**. Положенні про порядок здійснення криптографічного захисту інформації в Україні, яке затверджено Указом Президента України від 22.05.1998 р., www.rada.gov.ua.**5**. Проект Закону України «Про захист інформації», www.dstszi.gov.ua. **6**. Скакун О. Ф. Теорія держави і права, http/topical.in/book/tgp/skakun. **7**. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджено наказом ДСТСЗІ СБ України від 28.04.99 р., № 22, чинний від 01.07.1999 р., dstszi.gov.ua. **8**. Положення про технічний захист інформації в Україні, затверджено Указом Президента України від 27.09.99 р. № 1229, www.rada.gov.ua. **9**. Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації ДССЗЗІ України №87 від 16.05.2007 р., www.rada.gov.ua. **10**. Закон України «Про електронний цифровий підпис» від 22.05.2003 р., www.rada.gov.ua. **11**. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р., www.rada.gov.ua. **12**. Очиченко О. Захист конфіденційної інформації в інформаційно-телекомунікаційних системах, Юридичний радник №4(18), серпень 2007. **13**. Кримінально-процесуальний кодекс України від 28.12.60 р., www.rada.gov.ua. **14**. Кримінальний кодекс України від 5.04.2001 р., www.rada.gov.ua. **15**. Кодекс України про адміністративні правопорушення, від 7 грудня 1984 р., www.rada.gov.ua. **16**. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23.02.2006 р., www.rada.gov.ua. **17**. Кодекс законів про працю України від 10.12.71 р., www.rada.gov.ua. **18**. Цивільний процесуальний кодекс України від 18.03.2004 р., www.rada.gov.ua. **19**. Конституція України // Закони України, Т. 10. – К., 1997. **20**. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України: дис. канд. юрид. наук: 12.00.07 / Інститут законодавства Верховної Ради України. - К., 2006 р. – С 201. **21**. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 р., №1126, www.rada.gov.ua.*

УДК 621.317

АНАЛІЗ ВИМІРЮВАЛЬНИХ РІВНЯНЬ ПРИ ВИКОНАННІ ФУНЦІЙ ЗБЕРЕЖЕННЯ, ВІДТВОРЕННЯ ТА ПЕРЕДАЧІ ОДИНИЦІ ВИМІРЮВАННЯ ДЕРЖАВНИМИ ЕТАЛОНАМИ

Олександр Шевченко
Держспоживстандарт України

Анотація: **Наведені вимірювальні рівняння для трьох державних еталонів для випадків відтворення, зберігання та передачі одиниць вимірювань.**
Summary: **Measuring equation for three state standards suitable reproduction keeping transfer of units are considered.**
Ключові слова: **Вимірювальне рівняння, державний еталон, функції відтворення, зберігання та передача одиниці вимірювання.**

Вступ

Зазвичай вимірювальні рівняння пишуться для випадків проведення вимірювань фізичних величин. Для випадку аналізу вимірювань у держаних первинних еталонах (ДЕ), які мають відтворювати, зберігати та передавати одинцю вимірювань, ці питання досліджено недостатньо. Для задач технічного захисту інформації (ТЗІ) ці питання можуть знайти свої застосування для проведення прецизійних калібрувань засобів вимірювальної техніки, що використовуються під час випробувань з ТЗІ.

І Державний первинний еталон одиниці потужності електромагнітних коливань в коаксіальних трактах у діапазоні частот від 0,03 ГГц до 18 ГГц. ДЕТУ 09-06-05

У ДЕТУ 09-06-05 та відповідному стандарті [1] описано склад державного еталона**.** Найважливішими елементами еталона є еталонні ватметри [1 – 6]. В основу роботи еталонних ватметрів покладено закон збереження енергії (перетворення вимірюваної потужності надвисокої частоти (НВЧ) в тепло, а потім перетворення зміни температури в електричний сигнал) і метод заміщення потужності НВЧ відомою потужністю постійного струму. Як еталони напруги та опору використовуються високоточні цифрові