

12. Окландер М. А. Логістична система підприємства : [монографія] / М. А. Окландер. – О. : Астропринт, 2004. – 312 с.
13. Крикавський Є. В. Логістика. Для економістів : підручник / Є. В. Крикавський. – Львів : Національний університет "Львівська політехніка", 2004. – 448 с.
14. Pfohl H. Ch. Systemy logistyczne. Biblioteka Logistyke / H. Ch. Pfohl. – Poznan, 1998. – 420 s.
15. Уваров С. А. Логистика : общая концепция, теория и практика / С. А. Уваров. – СПб. : Инвест-НП, 1996. – 232 с.
16. Чернишов М. А. Муниципальная экономика: логистическая концепция. – Ростов-на-Дону : Рост. гос. стрит. ун-т, 1998. – 230 с.
17. Крикавський Є. В. Логістичні системи : навч. посібник / Є. В. Крикавський, Н. В. Чернописька. – Львів : Видавництво Національного університету "Львівська політехніка", 2009. – 264 с.
18. Сток Дж. Р. Стратегическое управление логистикой / Дж. Р. Сток, Д. М. Ламберт ; пер с 4-го англ. изд. – XXXII. – М. : ИНФРА-М, 2005. – 797 с.
19. Сток Дж. Р. Стратегическое управление логистикой / Дж. Р. Сток, Д. М. Ламберт ; пер с 4-го англ. изд. – XXXII. – М. : ИНФРА-М, 2005. – 797 с.
20. Моисеева Н. К. Экономические основы логистики: учебник / Н. К. Моисеева. – М. : ИНФРА-М, 2010. – 528 с.

УДК: 342+35.078.3

Л.Г. Чистоклетов

к. ю. н., доцент

Львівський державний університет внутрішніх справ

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В СФЕРІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В УКРАЇНІ

У даній статті на підставі основних теоретичних та практичних аспектів розглянуті найбільш актуальні питання інформаційно – правової безпеки суб'єктів господарювання в Україні. Виокремлено найбільш сучасні реалії внутрішніх та зовнішніх загроз інформаційної безпеки господарської діяльності. Досліджено та дана кваліфікація інформаційних загроз в сфері адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання.

Ключові слова: інформаційна безпека, адміністративно-правове забезпечення, загрози безпеці діяльності, суб'єкти господарювання, внутрішні загрози, зовнішні загрози.

В данной статье на основании основных теоретических и практических аспектов рассмотрены наиболее актуальные вопросы информационно-правовой безопасности субъектов хозяйствования в Украине. Выделены наиболее современные реалии внутренних и внешних угроз информационной безопасности хозяйственной деятельности. Исследованы и данная квалификация информационных угроз в сфере административно-правового обеспечения безопасности деятельности субъектов хозяйствования.

Ключевые слова: информационная безопасность, административно-правовое обеспечение, угрозы безопасности деятельности, субъекты хозяйствования, внутренние угрозы, внешние угрозы.

In this article the basic theoretical and practical aspects considered most relevant issues of information security -legal businesses in Ukraine. Pointed out in the most modern realities of internal and external threats to information security business. Explored and this qualification in the field of information threats administrative and legal security of business entities, and defines the main tasks of administrative and legal information security entity for the purpose of forecasting and early detection of threats to information security, the causes and conditions that are favorable for the application of financial, material and moral damage. Established that ensure the availability, integrity and confidentiality of information resources is one of the key tasks for effective security of the entity.

Keywords: information security, administrative and legal support, security threats activities, entities, internal threats, external threats.

Постановка проблеми. Першочерговою проблемою адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання в секторі національної економіки є те, що в даній сфері безпекотворення ще не визначилися відповідально підходити до вирішення проблем забезпечення інформаційної безпеки

діяльності і ще не визрів постулат за яким необхідно було б обов'язкове використання у господарській діяльності форм та методів адміністративно-правового інформаційного забезпечення, здатного у ринкових умовах організувати захист інтересів суб'єкта господарювання на всьому організаційно-правовому полі.

З цього приводу, стабільне функціонування та зростання економічного потенціалу суб'єктів господарської діяльності в умовах шаленого розвитку інформаційних відносин багато в чому залежить від наявності надійної системи інформаційної безпеки. Дане і зумовлює **актуальність** наукових пошуків даного напрямку.

Аналіз останніх досліджень. Останнім часом наукові доробки з розв'язання різних проблем інформаційної безпеки в сфері адміністративно-правового забезпечення безпеки діяльності значно активізувались. Дослідженню окремих напрямків інформаційної безпеки присвятили свої праці Ю. Бабенко, О. Беліков, К. Беляков, Ю. Мірошник, А. Марущак, О. Івченко, П. Пригунов, Д. Прокоф'єва та ін. Проте, такі питання як внутрішні та зовнішні загрози інформаційній безпеці діяльності суб'єктів господарювання та шляхи їх попередження в сфері адміністративно-правового забезпечення державними та недержавними органами залишаються мало дослідженні, потребують також подальшого наукового осмислення питання конфіденційного та таємного діловодства на підприємстві як важливої складової системи інформаційної безпеки підприємства.

Мета дослідження. Досягнення поставленої мети реалізовувалось через постановку та послідовне вирішення основних завдань, які пов'язані з дослідженням внутрішніх та зовнішніх загроз інформаційній безпеці суб'єктів господарювання, встановлення каналів витоку конфіденційної інформації і можливі шляхи локалізації таких загроз.

Виклад основного матеріалу. Аналіз стану справ в сфері інформаційної безпеки свідчить, що на сьогоднішній день концепція і структура захисту інформації вже склалася, і її основу становлять:

- досить розвинутий арсенал технічних засобів захисту інформації;
- значна кількість суб'єктів господарювання, що спеціалізуються на вирішенні питань захисту інформації;
- чітко окреслена система поглядів на цю проблему;
- наявність значного практичного досвіду тощо.

Досвід також показує, що:

- забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів та шляхів удосконалювання і розвитку системи захисту, безперервному контролю її стану, виявленні її слабких місць та протиправних дій;
- безпека інформації може бути забезпечена лише за умови комплексного використання всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі засоби, методи і заходи поєднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування системи повинно контролюватися, оновлюватися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов;
- ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки суб'єктів господарювання і дотримання ними усіх установлених правил, спрямованих на її захист.

Пріоритетним напрямком у процесі формування та забезпечення інформаційної безпеки будь-якої господарської діяльності є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Це, природно, вимагає конкретних дій, спрямованих на захист інформації з обмеженим доступом. Як свідчить вітчизняна і закордонна преса, кількість злочинів в інформаційній сфері не тільки не зменшується, але й має досить стійку тенденцію до росту.

Досвід показує, що для боротьби з цією тенденцією необхідна цілеспрямована організація процесу захисту інформаційних ресурсів. Причому в цьому повинні брати активну участь професіонали, адміністрація та співробітники, що і визначає значимість організаційної сторони питання.

Систему захисту інформації в сфері адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання можна, на нашу думку, визначити як сукупність державних та недержавних компетентних органів, які в процесі діяльності застосовують спеціальні засоби, методи і заходи, що забезпечують захист інформації від внутрішніх та зовнішніх загроз в безпеці діяльності суб'єктів господарювання.

Таким чином, зважаючи на важливість та значимість, яку отримує людство від інформаційної сфери, на сьогоднішній політичний, економічний та соціальний розвиток нашого суспільства у більшості залежить від якісного, достовірного та оперативного одержання інформації для прийняття чисельних рішень, що приймаються на різних рівнях – від Верховної Ради України до громадянина. Величезні інформаційні потоки буквально захлипають людей. Обсяг наукових знань, за оцінкою фахівців подвоюється кожні п'ять років. Дане підтверджується й тим, що за даними Всесвітньої інтернет статистики в Європі налічується понад 476 млн. користувачів Інтернет, що становить 58.3% усього населення континенту або 22.7% користувачів світу. Найпотужнішими країнами-користувачами Інтернет є Німеччина, Росія, Велика Британія, Туреччина. Україна посідає 9 місце у списку, маючи понад 15 млн. користувачів [1].

Щоб переконатися, що інформація дійсно має цінність, слід комплексно розглядати користувача та проблему, яку потрібно вирішити. Для цього необхідно, насамперед, відповісти на питання: яка інформація, кому, коли і в якому вигляді повинна бути представлена. Іншими словами, постає проблема визначення та задоволення інформаційних потреб споживача інформації [2, с.443].

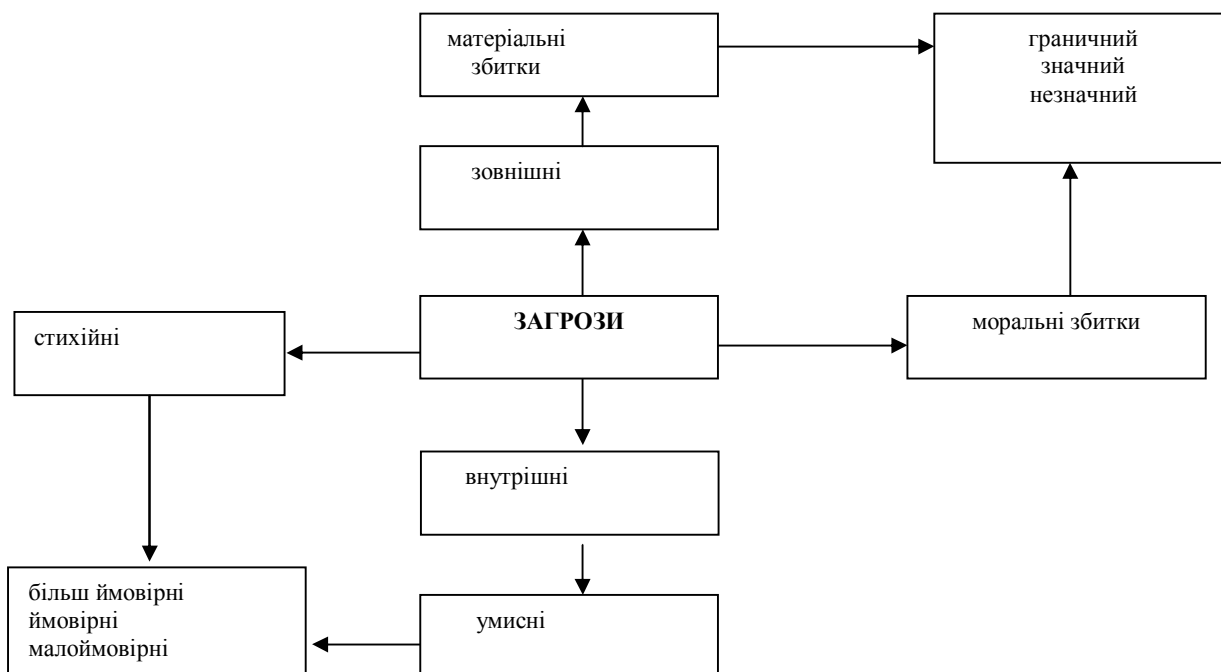
Розглядаючи проблеми адміністративно-правового забезпечення інформаційної безпеки діяльності суб'єктів господарювання, слід детальніше зупинитися на такому важливому аспекті як загрози інформаційної безпеки (далі – ІБ). Адже саме вони є джерелом порушення ІБ.

Р.Б. Тарасенко визначає, що загрози інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері [3]. На нашу думку, під поняттям загрози інформаційній безпеці діяльності суб'єктів господарювання слід розуміти як потенційну можливу подію, дію, процес або явище, яке може призвести до порушення конфіденційності інформації, а також неправомірного її тиражування. Як правило, загрози свідчать про наявність прогалин, тобто слабких місць в ІБ. Проте, не завжди це так. Наприклад, загроза перебою в електроживленні або відключенні електрики існує в силу залежності техніки від якісного електроживлення.

Забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів є одним з ключових завдань для ефективної безпеки діяльності суб'єкта господарювання. До подібних ресурсів можна віднести: контракти і договори; інформацію фінансового і технічного характеру; інформацію про нові проекти, бізнес-плани; інформацію про співробітників; інформацію про нематеріальні активи; дані бухгалтерського обліку; інформацію про поточну діяльність організації.

Уся подібного роду інформація, в основному, зберігається і обробляється за допомогою автоматизованих інформаційних систем, тобто результат діяльності підприємства багато в чому залежить від стійкості і захищеності цих систем від дій зловмисників, конкурентів. Диверсифікація, проникнення на нові ринки, пошук нових клієнтів і постачальників, створення нових підрозділів ведуть до ускладнення структури організації, що вимагає вдосконалення інформаційної системи із застосуванням нових інформаційних технологій. Але з побудовою сучасної автоматизованої системи зростає вірогідність різного роду загроз, спрямованих на підрив ІБ підприємства. Загрози ІБ, як правило, спрямовані на підрив цілісності, конфіденційності, доступності інформації. Результатом цих загроз можуть бути просочування інформації, розголошення, спотворення (модифікація), знищення тощо. На рисунку представлена класифікація загроз адміністративно-правовому забезпеченню інформаційної безпеки діяльності суб'єктів господарювання за декількома критеріями:

- джерело загроз (внутрішні і зовнішні);
- характер завданого збитку (загрози, що спричиняють за собою моральний або матеріальний збиток);
- вірогідність появи;
- причини виникнення.



Види загроз адміністративно-правового забезпечення інформаційної безпеки діяльності суб'єктів господарювання

Джерело: розроблено автором

До *зовнішніх загроз* можна віднести:

- промислове шпигунство;
- атаки на систему захисту з метою крадіжки, знищення, спотворення інформації;
- відсутність на ринку достатньої кількості сертифікованих засобів захисту інформації;
- недосконалість існуючої нормативно-правової бази адміністративно-правового забезпечення ІБ;
- діяльність недобросовісних партнерів, клієнтів.

До *внутрішніх джерел загроз* ми відносимо:

- недосконалість використовуваної системи захисту інформації;
- застарілі програмно-технічні засоби зберігання і обробки даних;
- низьку кваліфікацію співробітників;
- використання «піратського» програмного забезпечення;
- саботаж персоналу;
- недостатню пожежну, технічну безпеку приміщень, будівель організації.

Також до внутрішніх загроз інформації можна віднести підривну діяльність конкуруючих організацій, які здійснюють її шляхом вербування агентів для подальшої дезорганізації конкурента, помста співробітників, які незадоволені заробітною платою або статусом у фірмі та інше. Ми вважаємо, для того щоб ризик таких випадків був мінімальний, необхідно, щоб кожен співробітник в сфері господарської діяльності відповідав, так званого, «статусу благонадійності».

Фахівці вважають, що спостерігається помітне зростання з кожним роком все більш і більш витончених, універсальних і складних вірусних програм, що завдають помітного збитку як корпоративним, так і домашнім користувачам [4].

Як правило, захисту потребують два типи відомостей, які підпадають під категорію конфіденційної інформації або комерційної таємниці:

- інформація, що становить науково-технологічні відомості, пов'язані безпосередньо з конструкторською і технологічною документацією, відомості про використовувані матеріали, а також опис методів і способів виробництва нових виробів, унікальний програмний продукт;
- інформація, що становить ділові відомості про діяльність установи: фінансова документація, перспективні плани розвитку, напряму модернізації виробництва, аналітичні матеріали про дослідження конкурентів і ефективність роботи на ринках товарів і послуг, різні свідчення про партнерів та ін.

Саме ці два типи відомостей стають найчастіше об'єктом комп'ютерних злочинів [5, с. 42]. До речі, професор Р.Калюжний ще в 1992 році наголошував на визначній ролі обчислювальної техніки в роботі органів внутрішньої справ [6, с. 3].

Виходячи із вище зазначеного, вважаємо що, основними завданнями адміністративно-правового забезпечення ІБ будь-якого суб'єкта господарювання є створення стабільної, ефективної торгівельної і виробничої діяльності усіх підрозділів, захист від втрат, крадіжок, спотворення і знищення конфіденційної інформації та комерційної таємниці, розкрадання фінансових коштів відвертання загроз безпеки. Система ІБ потрібна також для підвищення якості послуг, що надаються як гарантія безпеки майнових прав та інтересів клієнтів.

Для досягнення зазначеної мети, у першу чергу, потрібно:

- категорювання інформації на конфіденційну інформацію та комерційну таємницю;
- прогнозування і своєчасне виявлення загроз інформаційної безпеки, причин і умов, які є сприятливими щодо нанесення фінансового, матеріального і морального збитку;
- створення умов діяльності з найменшим ризиком реалізації загроз безпеки інформаційним ресурсам і нанесення різних видів збитку;
- створення механізму і умов для ефективного реагування на загрози ІБ, на основі правових, організаційних і технічних засобів.

Висновок. Постійне зростання темпів розвитку і поширення інформаційних технологій, висока конкуренція та існуюча криміногенна ситуація створюють умови для ефективного реагування на загрози ІБ, а також повинні визначити пріоритетні питання про створення на підприємстві *єдиної системи адміністративно-правового забезпечення інформаційної безпеки діяльності суб'єктів господарювання*. Система ІБ суб'єкта господарювання, на нашу думку, повинна включати правові, інформаційно-аналітичні, організаційні, фізичні, інженерно-технічні та програмні напрями забезпечення захисту інформаційних ресурсів. Для повної оцінки ситуації господарської діяльності за усіма напрямками забезпечення ІБ, на нашу думку, потрібна розробка *Концепції адміністративно-правового забезпечення інформаційної безпеки суб'єкта господарювання*, яка б встановлювала системний підхід до проблеми безпеки інформаційних ресурсів і була систематизованим викладом цілей, завдань, принципів проектування і комплексу заходів щодо адміністративно-правового забезпечення інформаційної безпеки суб'єкта господарювання.

Література

1. *Internet World Stats Електронний ресурс.* – Режим доступу: <http://www.internetworldstats.com/stats4.htm#europe>.

2. Чистоклетов Л.Г. Інформація як визначальний чинник адміністративно-правового забезпечення фінансово-економічної та інформаційної безпеки суб'єктів господарювання / Л.Г.Чистоклетов // Митна справа. – 2011. – № 5, ч. 2. – с. 441–448.

3. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с. – [Електронний ресурс]. – Режим доступу: <http://www.ukr.vipreshebnik.ru/2012-06-25-18-22-00/563-2011-06-18-18-00-40.html>.

4. Лужецький В. А., Войтович О. П., Кожухівський А. Д., Северин Л. І., Трегубенко І. Б. . Основи інформаційної безпеки. – Черкаси : ЧДТУ, 2008. – 1 електрон. опт. диск (CD-ROM) – (Series "Information security").

5. Мотлях О. І. Методика розслідування комп'ютерних злочинів : монографія / О. І. Мотлях. – К. : Освіта України, 2010. – 296 с. с. 42.

6. Калюжний Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореферат дисс. ... д-ра юрид. наук / Р. А. Калюжний. – К. : Институт государства и права им. В. М. Корецкого, 1992. – 23 с. с. 3.

УДК 342:345.01

М.С. Дзюдзь

начальник Управління Державної пенітенціарної служби України у Львівській області

ОРГАНИ ДЕРЖАВНОЇ ПЕНІТЕНЦІАРНОЇ СЛУЖБИ УКРАЇНИ В СИСТЕМІ СУБ'ЄКТІВ ЗАХИСТУ ПРАВ, СВОБОД І ЗАКОННИХ ІНТЕРЕСІВ ГРОМАДЯН У ВИПРАВНИХ УСТАНОВАХ

У статті розглядається діяльність органів Державної пенітенціарної служби України в системі суб'єктів захисту прав, свобод і законних інтересів громадян у виправних установах. Розкриваються особливості адміністративно-правового статусу Державної пенітенціарної служби та механізм правового регулювання діяльності, який становить систему правових засобів і методів.

Ключові слова: органи пенітенціарної служби, права та свободи громадян, механізм правового регулювання, виправні установи.

В статье рассматривается деятельность органов Государственной пенитенциарной службы Украины в системе субъектов защиты прав, свобод и законных интересов граждан в исправительных учреждениях. Раскрываются особенности административно-правового статуса Государственной пенитенциарной службы и механизм правового регулирования деятельности, который составляет систему правовых средств и методов.

Ключевые слова: органы пенитенциарной службы, права и свободы граждан, механизм правового регулирования, исправительные учреждения.

The article deals with the activities of the State Penitentiary Service of Ukraine in the system of protection of rights, freedoms and legitimate interests of citizens in prisons. Peculiarities of administrative and legal status of the State Penitentiary Service and the mechanism of legal regulation of the activity, which constitutes the system of legal remedies and methods, are investigated.

Keywords: penitentiary service, rights and freedoms of citizens, mechanism of legal regulation, correctional institutions.

Постановка проблеми. Реформи у сфері державного управління, проведені в Україні останніми роками, спрямовані на підвищення ефективності діяльності державних органів в інтересах розвитку громадянського суспільства та зміцнення держави, забезпечення прав, свобод і законних інтересів громадян. Нові підходи до державного будівництва викликають об'єктивну потребу переглянути багато уявлень, які склалися в теорії адміністративного права щодо впливу держави (організаційного та регулювального), системи публічної влади й управління, їх контролюючої ролі в різних сферах суспільного життя, зокрема у сфері виконання кримінальних покарань у вигляді позбавлення волі.

Аналіз досліджень даної проблеми. Дослідження діяльності органів Державної пенітенціарної служби України в системі суб'єктів захисту прав, свобод і законних інтересів громадян у виправних установах у різних аспектах проводили українські вчені: О. Бандурка, Н. Бортник, Є. Додін, В. Василенко, В. Колпаков, Р. Калюжний, Л. Коваль, О. Кузьменко, В. Олефір, В. Ортинський, О. Остапенко, В. Петков, Ю. Римаренко, Х. Ярмакі та інші.