3 2015 (231)

ПІДПРИЄМНИЦТВО, ГОСПОДАРСТВО І ПРАВО

Щомісячний науково-практичний
юридичний журнал
видається з 1 січня 1996 р.

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПРИВАТНОГО ПРАВА І ПІДПРИЄМНИЦТВА
ІМ. АКАДЕМІКА Ф. Г. БУРЧАКА НАПрН УКРАЇНИ

На першій сторінці обкладинки – пам'ятник Магдебурзькому праву в м. Києві

Співзасновники:
Науково-дослідний інститут приватного права і підприємництва ім. академіка Ф. Г. Бурчака Національної Академії правових наук України,
ТОВ «Гарантія»

Видавець: ТОВ «Гарантія»

Свідоцтво про державну реєстрацію друкованого засобу масової інформації серія КВ № 15779-4251ПР від 02.11.2009 р.

Журнал рекомендовано до друку вченою радою Науково-дослідного інституту приватного права і підприємництва ім. академіка Ф. Г. Бурчака НАПрН України (протокол № 2 від 25.02.2015 р.)

Підписано до друку 20.03.2015. Формат 70×108 1/16. Папір офсетний. Друк офсетний. Ум. друк. арк. 7,35. Обл.-вид. арк. 9,9. Умовн. фарбовідбитків 8,22. Тираж 235. Замовлення № 15-085. Надруковано з готових форм у ТОВ «Друкарня Бізнесполіграф», 02094, м. Київ, вул. Віскозна, 8.

Свідоцтво про державну реєстрацію друкованого засобу масової інформації серія КВ № 15779-4251 ПР від 02.11.2009 р.
Поштова адреса редакції: 01133, м. Київ-133, а/с 23.
Тел./факс (044) 513-33-16.

УДК 347.77

Анфіса Нашинець-Наумова,
канд. юрид. наук,
доцент кафедри правознавства
Інституту суспільства
Київського університету ім. Бориса Грінченка

ТЕОРЕТИЧНІ АСПЕКТИ ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЙ

У статті розглядаються основні завдання та функції системи забезпечення інформаційної безпеки корпорацій.

Ключові слова: інформаційна безпека корпорацій, моніторинг стану інформаційної безпеки корпорацій, елементи системи забезпечення інформаційної безпеки корпорацій, загрози та небезпеки.

На сучасному етапі в економічній та юридичній науках корпорація є одним із найважливіших об'єктів дослідження. Така ситуація виникла не випадково, оскільки корпорації за останні півтори століття стрімко розвивались, активно та постійно трансформувалися, поширювалися. Вони завоювали панівне становище у світовій ринковій економічній системі.

Сутність поняття «корпорація» науковці трактують по-різному. У найзагальнішому вигляді *корпорація* – це організаційна структура, що об'єднує необхідні ресурси для виробництва товарів і надання послуг населенню. Ця форма організації поширена в усіх країнах, оскільки вона [1, с. 13–14]:

- обмежує фінансовий ризик акціонерів унаслідок виключення за чинним законодавством їх відповідальності перед кредиторами товариства за межами капіталу, що розміщений в акціях;
- робить можливим залучення капіталу за рахунок випуску додаткової кількості акцій та емісії інших цінних паперів;
- продовжує діяльність навіть після зміни складу акціонерів;
- сприяє отриманню інвестицій на вигідних умовах;
- дає змогу власникам корпорацій успішно реалізовувати стратегічні плани на засадах колективних інтересів;
- пропонує працівникам участь у розподілі прибутків і капіталу;
- створює механізм повернення вкладених у статутний капітал коштів шляхом продажу акцій;
- забезпечує контроль за діяльністю управлінського апарату тощо.

Вагомою теоретико-методологічною базою дослідження функціонування системи інформаційної безпеки корпорацій є праці таких зарубіжних учених, як Л. Абалкін, В. Абрамова, Ю. Алтухова, Дж. Барбер, Л. Бирки, В. Богомолова, Г. Вечканова, А. Горбунов, К. Гудвіл, К. Девіс, П. Друкер, Р. Леонард, Т. Лоурі, Ф. Найт, П. Самуельсон, А. Сміт, У. Семюелс, Ф. Хайєк та інших. Проблеми інформаційної безпеки юридичних осіб досліджуються і в роботах вітчизняних учених – В. Артемов, О. Баранов, І. Бачило, В. Брижка, В. Гавловського, А. Гевлича, Р. Калюжного, Б. Кормича, А. Марущака, В. Селіванова, В. Цимбалюк, М. Швець та інших, які не тільки розвивають, а й суттєво оновлюють традиційні наукові уявлення в цій галузі. Тому не буде перебільшенням стверджувати, що сьогодні без урахування й аналітичного розгляду їх наукового внеску не може обійтися жодна серйозна праця з методології інформаційно-правової науки.

Мета цієї статті полягає у визначенні суті поняття «інформаційна безпека корпорацій», у формулюванні теоретико-правових аспектів системи інформаційної безпеки корпорацій.

Враховуючи історичний і сучасний досвід розвитку корпорацій в Україні, необхідно зробити акцент на правовому аспекті функціонування системи інформаційної безпеки в корпораціях. Визначальним елементом цієї системи є її мета. Забезпечення інформаційної безпеки корпорацій досягається у процесі свідомої цілеспрямованої діяльності керівних органів корпорації щодо запобігання можливого порушення її звичайного функціонування в результаті дії загроз і небезпек.

Метою забезпечення інформаційної безпеки корпорацій є створення реальних умов

діяльності самої корпорації, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки.

Ефективність системи управління інформаційними ресурсами корпорації й її захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі та функціонуванні корпорації призводять до непоправних збитків у самій корпорації. Слід враховувати, що побудова системи інформаційної безпеки в корпорації неминуче наштовхується на різні протистояння, які необхідно врегульовувати в установленому в корпорації порядку з урахуванням норм чинного законодавства. Існують типові алгоритми локалізації загроз і етапи формування системи інформаційної безпеки, які застосовуються при створенні будь-якої системи безпеки. Так, цілісна система інформаційної безпеки повинна передбачати як профілактичну, так і внутрішню оперативну роботу. *Профілактична робота* допускає використання технічних методів і способів контролю, однак можливість їх проведення стосовно співробітників повинна бути в обов'язковому порядку закріплена письмовою згодою самого працівника. *Внутрішня оперативна робота* – це процес виявлення інформації небезпечного характеру.

До основних етапів формування системи інформаційної безпеки корпорацій можна віднести такі: ідентифікація джерел загроз і ризиків для бізнесу; оцінка ступеня серйозності загрози; вибір і застосування оптимального алгоритму локалізації загроз (побудова системи захисту) з урахуванням виділеного на це бюджету [2, с. 115]. Слід зазначити, що повсякденна практика недержавних об'єктів свідчить про їх підвищену (порівняно з державними структурами) вразливість від протиправних та інших посягань із боку різного роду кримінальних структур, а також окремих осіб.

Власність зобов'язує корпорації займатися діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є підґрунтям функціонування недержавних об'єктів. Отже, охорона корпорацій і забезпечення інформаційної безпеки корпоративної діяльності – стрижнева проблема, що охоплює комплекс організаційно-правових, техніко-технологічних, інформаційних, адміністративних, виховних, фінансових і спеціальних заходів, спрямованих на виявлення, попередження та припинення загроз і зазіхань на стабільність функціонування та розвитку корпорацій. Цей процес передбачає безпеку інформації, охорону приватної власності корпорацій і фізичний захист його персоналу. До власності відносять, *по-перше,* основне матеріальне майно (приміщення, земельна ділянка, парк техніки, сировина й інвентар), а також допоміжне устаткування, призначене для збереження, переробки та перевезення вантажів; *по-друге,* інтелектуальну власність, що складає інформацію, яка є активом компанії, а також знання та досвід співробітників корпорацій, їх професійні секрети, винаходи.

Корпорації, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення як необґрунтовано високі, оскільки життя та репутація цінується набагато вище. Проблемою корпорацій є те, що, заробивши великі гроші, вони не хочуть усвідомлювати, що багатство неминуче переводить їх у «групу ризику». Як свідчить сумний досвід, наші корпорації починають здійснювати суттєві кроки із забезпечення власної безпеки, безпеки інформації лише після того, як у них сталися неприємності [2, с. 120].

Зрозуміло, що без конкретних завдань щодо забезпечення інформаційної безпеки корпорацій неможливо уявити майбутнє цього сектора економіки. Отже, основним завданням системи забезпечення інформаційної безпеки корпорацій є створення умов для організації управління системою інформаційної безпеки.

Основними завданнями системи забезпечення інформаційної безпеки корпорацій є:

- забезпечення інформаційної безпеки корпорацій на всіх рівнях;
- моніторинг (спостереження, оцінка та прогноз) стану інформаційної безпеки корпорацій у зв'язку із впливом загроз і небезпек як зсередини, так і ззовні;
- протидія технічному проникненню до інформаційної системи корпорацій з метою вчинення злочинів;
- забезпечення збереження комерційної таємниці.

З огляду на завдання, які постають перед системою забезпечення інформаційної безпеки корпорацій, доцільно визначити її функції. Під такими ми розуміємо здійснення керівними органами організаційної діяльності із створення умов для оптимального управління системою інформаційної безпеки корпорацій.

До основних функцій системи забезпечення інформаційної безпеки корпорацій слід віднести:

створення та забезпечення діяльності елементів системи забезпечення інформаційної безпеки корпорацій, що включає розроблення правових засад для побудови та функціонування системи інформаційної безпеки корпорацій; системне забезпечення діяльності елементів системи (аналітичне, інформаційне, правове, матеріально-технічне, кадрове, ресурсне забезпечення); розроблення та прийняття управлінських рішень щодо забезпечення системи управління інформаційними

ресурсами корпорацій та вдосконалення механізмів реалізації правових норм щодо них;

управління системою інформаційної безпеки корпорацій (здійснення свідомого цілеспрямованого впливу корпорацій на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки): розроблення на підставі концепції інформаційної безпеки корпорацій конкретних планів і технологій забезпечення інформаційної безпеки відповідно до потреб кожного підрозділу корпорацій; прогнозування, планування, організація, регулювання та контроль усією системою інформаційної безпеки й окремими її елементами; оцінка результативності дій і витрат на проведення заходів щодо забезпечення інформаційної безпеки корпорацій; оптимізація внутрішніх документів корпорацій щодо забезпечення науково-технічних, виробничо-технологічних, організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування розвитку й ефективного використання інформаційних ресурсів корпорації;

здійснення планової й оперативної діяльності щодо забезпечення інформаційної безпеки корпорацій: визначення інтересів кожного підрозділу корпорацій в інформаційній сфері й їх пріоритетності відповідно до цілей корпорації; діагнозування загроз і небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків; визначення та здійснення повноважень корпорацій щодо оперативного управління (володіння, розпорядження, користування) інформаційними ресурсами; забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів корпорації;

здійснення організаційних і матеріально-технічних заходів забезпечення інформаційної безпеки корпорацій [3, с. 118]: розроблення та реалізація фінансово-економічних засад регулювання процесів формування і використання інформаційних ресурсів корпорації; забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності корпорацій; введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності корпорації; забезпечення захисту системи корпорацій від хибної, спотвореної та недостовірної інформації; інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами корпорації; кадрове забезпечення; забезпечення розробки та застосування організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів корпорації (інформаційних технологій, засобів обробки інформації й інформаційних послуг);

здійснення контрольно-наглядової діяльності щодо забезпечення інформаційної безпеки корпорації: забезпечення ефективного використання інформаційних ресурсів у корпорації; контроль за встановленим порядком і правилами формування, розвитку та використання інформаційних ресурсів корпорації; нагляд за додержанням законодавства у сфері формування, розвитку та використання інформаційних ресурсів корпорації.

Враховуючи викладені підходи щодо поняття системи забезпечення інформаційної безпеки корпорацій, засад її формування та функціонування, захисту і призначення, мети, завдань, функцій, а також з урахуванням напрацювань з даних та інших споріднених питань, структура системи повинна мати такий вигляд:

стратегічний рівень:

- Верховна Рада України визначає засади зовнішньої та внутрішньої політики держави в інформаційній сфері; здійснює законодавче регулювання політики національної безпеки України в інформаційній сфері (нормативно закріплює права та свободи людини і громадянина в інформаційній сфері, гарантії цих прав і свобод, основні обов'язки громадянина; закріплює основи національної безпеки, засади цивільно-правової відповідальності; визначає діяння, які є злочинами, адміністративними або дисциплінарними правопорушеннями, та відповідальність за них); створює правові засади функціонування системи забезпечення національної безпеки в інформаційній сфері; затверджує загальнодержавні програми у цій сфері та контролює хід їх виконання; затверджує бюджетні асигнування для фінансування діяльності із забезпечення національної безпеки в інформаційній сфері; визначає порядок створення та повноваження Ради національної безпеки і оборони України; призначає за поданням Президента України Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, Голови Служби безпеки України; призначає на посади та звільняє половину складу Національної ради України з питань телебачення і радіомовлення;
- Президент України здійснює загальне керівництво у сфері інформаційної безпеки України, а саме: очолює Раду національної безпеки і оборони України; здійснює керівництво в інформаційній та інших сферах національної безпеки та оборони України; здійснює контроль і координацію діяльності державних органів у забезпеченні національної безпеки в інформаційній та інших сферах; вживає оперативні заходи з метою нейтралізації загроз національним інтересам України в межах компетенції, визначеної Конституцією; один раз на рік на сесії Верховної Ради звітує перед народом України про стан національної безпеки України; забезпечує взаємодію всіх гілок державної влади між собою,

а також із недержавною складовою системи забезпечення національної безпеки в інформаційній сфері; видає нормативно-правові акти з питань забезпечення національної безпеки в інформаційній сфері; визначає реальні та потенційні загрози та небезпеки для національної безпеки в інформаційній сфері та вживає необхідних заходів з її забезпечення;

тактичний рівень:

• міністерства й інші центральні органи виконавчої влади в межах своїх повноважень: забезпечують реалізацію законів України, указів і розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління у сфері інформаційної безпеки; забезпечують створення, підтримку в готовності та застосування сил і засобів забезпечення інформаційної безпеки, а також управління їх діяльністю; у межах своєї компетенції розробляють нормативні правові акти в інформаційній сфері та представляють їх Президентові України та Кабінету Міністрів України; вносять в органи виконавчої влади пропозиції з удосконалення функціонування системи забезпечення інформаційної безпеки України; керують діяльністю підвідомчих організацій із планування та проведення заходів із забезпечення інформаційної безпеки; забезпечують дотримання прав і законних інтересів громадян, організацій і держави, законів та інших нормативно-правових актів в інформаційній сфері; притягають до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють умови або безпосередню загрозу інформаційній безпеці України;

• органи місцевого самоврядування та місцеві державні адміністрації забезпечують вирішення питань у сфері інформаційної безпеки України у відповідних адміністративно-територіальних одиницях: забезпечують виконання Конституції та законів України, рішень Конституційного Суду України, актів Президента України, Кабінету Міністрів України, інших органів державної влади у сфері забезпечення інформаційної безпеки; забезпечують здійснення заходів щодо охорони громадської безпеки, громадського порядку, боротьби із злочинністю в інформаційній сфері; здійснюють заходи щодо організації правового інформування й інформаційного виховання населення; проводять роботу, пов'язану з розробленням і здійсненням заходів щодо інформаційного забезпечення біженців, а також депортованих осіб, які добровільно повертаються в регіони їх колишнього проживання; забезпечують виконання законодавства щодо національних меншин і міграції, про свободу думки і слова, свободу світогляду, віросповідання; оголошують у разі стихійного лиха, аварій, катастроф, епідемій, епізоотій, пожеж, інших надзвичайних подій зони надзвичайної ситуації; здійснюють передбачені законодавством заходи, пов'язані із забезпеченням інформаційної безпеки, захистом інформаційних прав особи; забезпечують своєчасне інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій під час проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних Сил України, інших військових формувань і правоохоронних органів із використанням озброєння та військової техніки;

оперативний рівень:

• діяльність МВС України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про міліцію», «Про оперативно-розшукову діяльність», «Про боротьбу з тероризмом», «Про боротьбу з корупцією», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про очищення влади», у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України.

Відповідно до п. 3 Указу Президента України «Про Положення про Міністерство внутрішніх справ України» основними завданнями МВС України є: організація та координація діяльності органів внутрішніх справ щодо захисту прав і свобод громадян, інтересів суспільства та держави в інформаційній сфері від протиправних посягань на них, охорони громадського порядку і забезпечення громадської безпеки в інформаційній сфері; участь у розробленні та реалізації державної політики щодо боротьби із кіберзлочинністю та кібертероризмом; забезпечення запобігання злочинам в інформаційній сфері, їх припинення, розкриття і розслідування, розшуку осіб, які вчинили злочини, вжиття заходів, спрямованих на усунення причин і умов, що сприяють вчиненню правопорушень; організація охорони й оборони внутрішніми військами особливо важливих державних об'єктів, зокрема об'єктів критичної інфраструктури держави тощо;

• діяльність Служби безпеки України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про Службу безпеки України», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про боротьбу з тероризмом», «Про боротьбу з корупцією», «Про організаційно-правові основи боротьби з організованою злочинністю», у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України, визначеним у ст. 7 Закону України «Про основи національної безпеки України».

Це, передусім, постійний моніторинг впливу на національну безпеку процесів, що відбуваються, перш за все, в інформаційній, політичній, соціальній, економічній, екологічній, науково-технологічній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці; систематичне спостереження за станом і проявами міжнародного й інших видів тероризму (зокрема, кібертероризму); прогнозування, виявлення й оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин і умов їх виникнення та наслідків прояву; комплексне інформаційно-аналітичне забезпечення діяльності вищих органів державної влади й інших суб'єктів забезпечення національної безпеки України в інформаційній сфері; розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень із метою захисту національних інтересів України; запобігання та нейтралізація впливу загроз і дестабілізуючих чинників на національну безпеку та національні інтереси в інформаційній сфері; локалізація, деескалація та врегулювання конфліктів, ліквідація їх негативних наслідків або впливу дестабілізуючих чинників; оцінка результативності дій щодо забезпечення національної безпеки в інформаційній сфері та визначення витрат на ці цілі; участь у двосторонньому та багатосторонньому співробітництві в галузі інформаційної безпеки, якщо це відповідає національним інтересам України; спільне проведення планових та оперативних заходів з компетентними структурами іноземних держав у рамках міжнародних організацій та договорів у галузі безпеки.

Реалізація окремих положень щодо збереження інформації в корпораціях особливим чином передбачена в Законі України «Про акціонерні товариства» (на прикладі реалізації норм оприлюднення інформації). Забезпечення безпеки інформації в корпораціях закріплене в Законі України «Про інформацію» (статті 9, 10), Законі України «Про акціонерні товариства» (щодо права акціонера на інформацію про діяльність акціонерного товариства) (статті 25, 26), Законі ПАТ (статті 77, 78).

Надання інформаційних послуг корпораціями через мережу Інтернет має супроводжуватися постійним моніторингом загроз і небезпек, які можуть вплинути на безперебійне функціонування веб-сайтів. Одна з вимог вказаної норми полягає в тому, що інформація, розміщена на веб-сайтах корпорацій, повинна мати захист від несанкціонованої модифікації [4, с. 238].

Передбачається, що інформаційне наповнення, захист інформації від несанкціонованої модифікації та технічне забезпечення функціонування веб-сайтів корпорації здійснюють самостійно. У свою чергу, контроль за дотриманням вимог щодо захисту інформації, доступної через Веб-портал, здійснюється Департаментом спеціальної телекомунікаційної системи та захисту інформації СБУ.

Висновки

Основним завданням системи забезпечення інформаційної безпеки корпорацій є створення умов для організації управління цією системою. Під основними функціями системи забезпечення інформаційної безпеки корпорацій ми розуміємо здійснення керівними органами організаційної діяльності із створення умов для оптимального управління системою інформаційної безпеки корпорацій. Це, перш за все, створення та забезпечення діяльності елементів системи забезпечення інформаційної безпеки корпорацій; управління системою інформаційної безпеки корпорацій; здійснення планової й оперативної діяльності щодо забезпечення інформаційної безпеки корпорацій; здійснення організаційних і матеріально-технічних заходів забезпечення інформаційної безпеки корпорацій; здійснення контрольно-наглядової діяльності щодо забезпечення інформаційної безпеки корпорації.

Список використаних джерел

1. *Нашинець-Наумова А. Ю.* Адміністративно-правове регулювання діяльності корпорацій в Україні: дис. ... канд. юрид. наук. – К., 2011. – 224 с.

2. *Логінов О. В.* Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. ... канд. юрид. наук. – К., 2005. – 236 с.

3. *Нашинець-Наумова А. Ю., Романська А. В.* Інститут неправдивої інформації в інформаційному праві // Тенденції розвитку юридичної науки в XXI столітті: Всеукр. наук.-практ. конф. до Дня науки, 22 травня 2014 р. – К., 2014. – С. 117–120.

4. *Нашинец-Наумова А. Ю.* Организационно-правовые структуры системы обеспечения информационной безопасности корпораций // Современные вопросы государства, права, юридического образования: Сборник научных трудов по материалам X Междунар. науч.-практ. конф., 22 декабря 2013 г. – Тамбов, 2014. – С. 236–241.

Стаття надійшла до редакції 22.01.2015 р.

In the article discusses the basic tasks and functions of information security corporations.

В статье рассматриваются основные задачи и функции системы обеспечения информационной безопасности корпораций.