УДК 004.056

С.О. Гахов

ЗАСТОСУВАННЯ МЕТОДІВ ПРАВОВОГО РЕГУЛЮВАННЯ ПІД ЧАС ЗДІЙСНЕННЯ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЩОДО КІБЕРНЕТИЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ, УСТАНОВ ТА ОРГАНІЗАЦІЙ

У статті досліджуються питання організації кібернетичного захисту інформаційних систем підприємств, установ та організацій. Розглянуто методи правового регулювання та на їх основі запропонована методика розроблення організаційних документів щодо кібернетичного захисту інформаційних систем підприємств, установ та організацій.

Ключові слова: кібернетична безпека, кібернетичний захист, кібернетичне право.

Постановка проблеми. У грудні 2015 року ми стали свідками остаточних результатів складної, цілеспрямованої та довготривалої кібернетичної атаки на вітчизняні енергетичні об'єкти, зокрема на "Прикарпаттяобленерго" і інші підприємства, внаслідок чого без електроенергії залишилися 80 тис. споживачів на досить тривалий термін. На завершальному етапі даної кібернетичної атаки було уражено автоматизовану систему контролю та управління енергообладнанням [1].

Робоча комісія з розслідування інциденту прийшла до висновку, що основною причиною вдалої кібернетичної атаки на вітчизняні енергетичні об'єкти стали "відсутність загальних обов'язкових вимог до енергетичних компаній у гарантуванні IT-безпеки систем автоматизації виробництва, недостатня обізнаність та підготовка технічного персоналу з приводу кібербезпеки і відсутність внутрішніх структур контролю кібербезпеки, незалежних від системних адміністраторів" [2].

Основні причини вдалої кібернетичної атаки на вітчизняні енергетичні об'єкти знаходяться в площині правового та організаційного забезпечення їх кібернетичної безпеки, що спонукає до пошуку шляхів методологічного забезпечення організаційної діяльності керівників підприємств, установ та організацій та відповідних фахівців щодо кібернетичного захисту інформаційних систем.

Аналіз останніх досліджень і публікацій за темою статті. Проблеми розбудови системи кібернетичної безпеки України розглядали В.П. Шеломенцев, В.М. Бутузов, В.Д. Гавловський, Д.В. Дубов, Н.А. Ожеван, В.Л. Бурячок, О.Г. Корченко, В.О. Хорошко та інші науковці.

Проведений аналіз наукових джерел показав необхідність подальшого дослідження питань організаційного забезпечення як складової частини кібернетичного захисту, зокрема методологічного забезпечення організаційної діяльності керівників підприємств, установ та організацій та відповідних фахівців щодо кібернетичного захисту інформаційних систем.

Постановка завдання. Якість правових, адміністративних, організаційних, технічних та інших заходів кібернетичного захисту інформаційних систем визначає захищеність життєво важливих інтересів людини, суспільства, держави у кібернетичному просторі. З розвитком інформаційного суспільства посилюється вплив ефективності кібернетичного захисту інформаційних систем на безпеку людей та суспільства в цілому.

Метою статті є: встановити зв'язок між правовими, адміністративними та організаційними заходами кібернетичного захисту інформаційних систем підприємств, установ та організацій; визначити можливість та доцільність застосування методів права в здійсненні організаційної діяльності відповідних керівників та фахівців щодо забезпечення кібернетичної безпеки на локальному рівні; запропонувати методологічний підхід у застосуванні методів кібернетичного права в організаційній діяльності, що розглядається.

Основний матеріалу дослідження. Розглянемо сутність організаційних заходів кібернетичного захисту інформаційних систем підприємств, установ та організацій.

Д.В. Дубов, М.А. Ожеван під *кібернетичною безпекою* пропонують розуміти "стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику

стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним інтересам" [3, 4].

В.П. Шеломенцев розглядає *систему кібернетичної безпеки* в загальному випадку "як сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються" [5].

Основою існування бізнес-процесів сучасного підприємства (установи, організації) є *інформаційна інфраструктура* (системи типу ERP, BI, бухгалтерський облік, системи обліку HP тощо), яка створюється і підтримується власними силами підприємства (силами департаменту (відділу) IT, службою захисту інформації тощо) або силами компанії-аутсорсера. З одного боку, застосування інформаційних технологій якісно змінює бізнес-процеси сучасного підприємства (установи, організації), створює умови для ведення більш ефективнішого бізнесу та отримання прибутку. З іншого боку, існування бізнес-процесів підприємства (установи, організації) в кіберпросторі створює умови та можливості стороннього впливу на них.

Необхідно відмітити, що суб'єкти малого та середнього підприємництва все частіше стають основними цілями кіберзлочинців оскільки:

підприємці та їхні працівники часто елементарно не обізнані в питаннях інформаційної та кібернетичної безпеки;

підприємці не можуть собі дозволити наймати фахівців в галузі інформаційної та кібернетичної безпеки;

підприємці не можуть собі дозволити закупівлю та застосування засобів захисту інформації тощо.

Тому, часто невеликі компанії виявляються нездатними повністю відновитися від наслідків кібернетичних атак. Забезпечення кібернетичної безпеки стає діяльністю, яка направлена на виживання підприємств, установ, організацій в умовах конкурентної боротьби і є справою від генерального директора до пересічного працівника підприємства.

Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" відповідальність за забезпечення захисту інформації в інформаційній системі покладається на власника системи [6], але коло учасників, які можуть впливати на кібернетичну безпеку підприємств, установ, організацій досить широке: власники істотної участі; управлінський персонал та працівники; особи, які здійснюють зовнішній аудит; представники державних органів, які відповідно до своїх посадових обов'язків здійснюють контроль за діяльністю; представники компаній-партнерів по бізнесу та компаній аутсорсерів тощо.

Кібернетична безпека підприємства, установи, організації є результатом організаційних, контролюючих, виконавчих, інженерно-технічних заходів, застосовуваних засобів і методів захисту інформації в інформаційних системах тощо.

Метою організаційних заходів кібернетичного захисту інформаційних систем підприємств, установ та організацій є створення і реалізація захищеної інформаційної технології, регламентація роботи працівників з інформаційною системою та використання інформаційних ресурсів, створення і функціонування дієвої системи контролю тощо. При цьому розробляється система документів локального рівня: положення, інструкції, правила тощо, які визначають і формують завдання, структуру, функції, повноваження служби захисту (відповідальних за захист інформації), визначають порядок застосування інформаційних систем та захисту інформації в них тощо.

Документи локального рівня (рівня підприємства, установи та організації), які регламентують процеси забезпечення кібернетичної безпеки відповідних інформаційних систем, мають розроблятися у відповідності з законодавством держави, нормами інформаційного та кібернетичного права. Дані документи затверджуються або вводяться в дію

наказами та розпорядженнями керівників підприємств, установ та організацій.

Встановимо можливість та доцільність застосування методів права в здійсненні організаційної діяльності відповідних керівників та фахівців щодо забезпечення кібернетичної безпеки на локальному рівні.

О.А. Барановим запропонована класифікація суспільних відносин в інформаційній сфері [7], яка зображена на рис. 1.

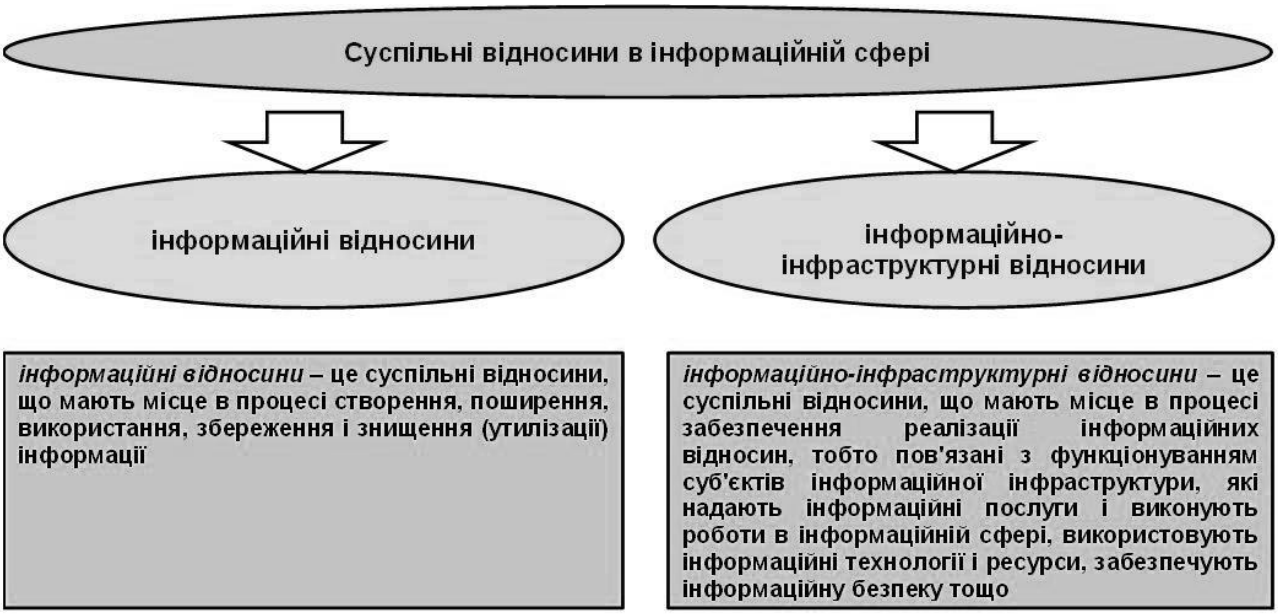

Рис. 1. Класифікація суспільних відносин в інформаційній сфері

Інформаційно-інфраструктурні відносини потребують відповідного правового регулювання, яке “може бути охарактеризоване як здійснюваний за допомогою юридичних засобів процес упорядкування суспільних відносин з метою забезпечення певної сукупності соціальних інтересів, які вимагають правового гарантування” [7].

Саме інформаційно-інфраструктурні відносини, які відображають норми поведінки суб’єктів в кібернетичному просторі, становлять предмет *кібернетичного права*.

Відомо, що право, яке є сукупністю норм, що створюються і охороняються державою, являє собою узгоджену, цілісну систему. Ця система є складною взаємозалежною ієрархічною структурою. Прийнято розрізняти наступні структурні елементи системи права в їх ієрархічній послідовності: галузь права; підгалузь права; інститут права; субінститут права, норма права [7].

Кібернетичне право є підгалуззю інформаційного права (співвідношення інформаційного та кібернетичного прав показано на рис. 2) і має містити інститути права, які регулюють суспільні відносини щодо інформації в кіберпросторі, інформаційних систем і технологій, у тому числі й кібербезпеки. Інформаційно-інфраструктурні відносини тісно пов’язані з іншими видами суспільних відносин, що визначає органічний зв’язок кібернетичного права з іншими галузями вітчизняного законодавства.

Кібернетичне право як система норм, що регламентують суспільні інформаційно-інфраструктурні відносини, повинна мати свій метод їх застосування.

Виділяються два основних загально правових методи регулювання суспільних (у тому числі інформаційних) відносин: *імперативний і диспозитивний*.

Якщо в правовому регулюванні перевага віддається встановленню обов’язків, обмежується ініціатива суб’єктів права з конкретизації положень юридичних приписів, що визначають їх поведінку, серед юридичних фактів переважають акти одностороннього волевиявлення (наприклад, адміністративні накази), а правова регламентація має суцільний, всеохоплюючий характер, то правове регулювання базується на імперативному методі [8].

Наприклад, в статті 8 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” сказано, що “державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю” [6].

Рис. 2. Співвідношення інформаційного та кібернетичного прав

Якщо в правовому регулюванні ширше, ніж зобов’язання та заборони, застосовуються дозволи, сторони відносин, що їх регулює право, мають змогу відступати від зазначених у правових нормах варіантів поведінки та вільні самі ухвалювати рішення щодо участі в цих відносинах (зокрема, через укладення між собою різноманітних правочинів), а право визначає лише найбільш важливі аспекти їх взаємодії, то правове регулювання засновується на диспозитивному методі [8]. Наприклад, в статті 8 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” сказано, що “умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством” [6].

Стає можливим запропонувати методику розроблення проектів організаційних документів локального рівня (положень, інструкцій, правил тощо), яка складається з таких етапів та застосовуваних методів:

визначення сфери суспільних відносин та відповідних галузі, підгалузі, інституту та субінституту права;

визначення переліку нормативно-правових документів та сукупності норм, які регулюють певну сферу суспільних відносин;

аналіз та визначення характеру виділеної сукупності норм на предмет застосовуваного методу правового регулювання (імперативний, диспозитивний тощо);

реалізація функції перетворення виділених норм права в положення документів організаційного характеру із застосуванням імперативного і диспозитивного методів правового регулювання;

перевірка повноти реалізації норм права в положеннях розробленого проекту документа організаційного характеру шляхом застосування методу семантичного аналізу;

подання розробленого проекту документа на затвердження (або введення в дію шляхом видання відповідного наказу керівника підприємства, установи, організації).

Необхідно відзначити, що запропоновану методику можливо застосовувати під час розроблення будь-яких проектів організаційних документів (положень, інструкцій, правил тощо) підприємств, установ, організацій. При цьому висуваються вимоги до законодавця щодо забезпечення повноти охоплення нормами правового регулювання суспільних відносин в інформаційній сфері, які на практиці не завжди виконуються.

Висновки

Система норм, що регламентують суспільні інформаційно-інфраструктурні відносини становлять кібернетичне право.

Організаційні заходи кібернетичного захисту інформаційних систем підприємств, установ та організацій створюють умови та забезпечують їх кібернетичну безпеку як досягнення відповідного стану.

Під час розроблення проектів організаційних документів підприємств, установ та організацій відповідальні особи реалізують перетворюючу функцію: норми законодавства, нормативно-правових документів відображаються в регламенти локального рівня з урахуванням характеру та особливостей відповідних бізнес-процесів. Під час реалізації даної функції рекомендується застосовувати методи правового регулювання суспільних відносин (імперативний, диспозитивний тощо) та метод семантичного аналізу.

Перспективні дослідження з окресленої тематики мають торкнутися обґрунтування рекомендацій суб'єктам малого та середнього підприємництва, які є найбільш вразливими по відношенню до сторонніх кібернетичних впливів, щодо забезпечення їх кібернетичної безпеки.

Література

1. Президент: Має бути негайно відпрацьована Національна система кібербезпеки. [Електронний ресурс] – Режим доступу: http://www.president.gov.ua/news/prezident-maye-buti-negajno-vidpracovana-nacionalna-sistema-36667.

2. Міненерговугілля оприлюднило звіт про російську кібератаку на обленерго. [Електронний ресурс] – Режим доступу: http://ukr.lb.ua/news/2016/02/12/327779_minenergovugillya_oprilyudnilo_zvit.html.

3. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України [Електронний ресурс] / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 31 с. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015.– 288 с.

5. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення [Електронний ресурс] / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2. – С. 299-309. – Режим доступу: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

6. Про захист інформації в інформаційно-телекомунікаційних системах. Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР. [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр.

7. Баранов О.А. Інститути інформаційного права / О.А. Баранов // Правова інформатика. – 2006. – № 3 (11). – С. 39-45.

8. Загальна теорія держави і права: [Підр. для студентів юрид. вищих навчальних закладів] / М.В. Цвік, О.В. Петришин, Л.В. Авраменко та ін.; За ред. д-ра юрид. наук, проф., акад. АПрН України М.В. Цвіка, д-ра юрид. наук, проф., акад. АПрН України О.В. Петришина. – Харків: Право, 2011. – 584 с.

Надійшла 03.08.2016 р. Рецензент: д.т.н., проф. Толубко В. Б.