ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2019.4(46)
Issue 4(46) 2019

ІНФОРМАЦІЙНЕ ПРАВО. ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

УДК 342.951(477)

Онопрієнко Станіслав Григорович,
кандидат юридичних наук,
старший викладач кафедри
Військового інституту Київського
національного університету імені Тараса Шевченка,
м. Київ, Україна
ORCID ID 0000-0002-5524-1798

ПРОТИДІЯ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В ІНФОРМАЦІЙНІЙ СФЕРІ: ПРАВОВИЙ АСПЕКТ

Стаття містить аналіз тенденцій у сфері протидії загрозам національної безпеки. Автор обґрунтовує, що особливістю сучасного суспільства є розвиток інформаційних технологій, які дозволяють значно швидше здійснювати виробничі операції, що займали велику кількість часу та зусиль.

Зроблено висновок, що зазначений закон є більш досконалим, ніж попередній законодавчий акт, водночас у ньому залишилась велика кількість прогалин, пов'язаних із визначенням особливостей забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека, національна безпека, сектор безпеки і оборони, інформаційне законодавство, правовий механізм, інформаційні технології.*

Проблеми забезпечення інформаційної безпеки є сьогодні надзвичайно важливими, оскільки Україна – це держава, яка потерпає від агресії Російської Федерації, у тому числі в інформаційній сфері. Інформаційні війни, які ведуться сьогодні, прийшли на зміну класичній збройній агресії, а боротьба за свідомість та можливість управляти поведінкою окремих людей, великих соціальних груп, представників державних органів є більш вагомою, ніж можливість спричиняти безпосередню шкоду життю та здоров'ю військовослужбовців та об'єктам критичної інфраструктури. Тому інформаційна безпека сьогодні постає як найбільш важлива мета організації суспільних відносин, до втілення якої прагнуть і науковці, і політики, і представники громадянського суспільства.

Водночас, незважаючи на те що питання інформаційної безпеки знаходили своє відображення в роботах І.В. Арістової, К.І. Бєлякова, О.О. Золотар, Д.О. Красікова, Б.А. Кормича, О.В. Олійника та інших авторів, питання протидії загрозам національній безпеці в інформаційній сфері досліджено ще недостатньо.

Метою написання статті є визначення особливостей правових аспектів протидії загрозам національній безпеці в інформаційній сфері.

Особливістю сучасного суспільства є розвиток інформаційних технологій, які дозволяють здійснювати ті виробничі операції, які займали велику кількість часу та зусиль, значно швидше, заощаджуючи людські, часові та інші матеріальні

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).45

ресурси. Разом з тим, інформатизація багатьох процесів як у сфері суспільного виробництва, освіти, так і в інших сферах, сприяла виникненню явища надмірної залежності людини від інструментів, за допомогою яких вона має сьогодні змогу виконувати свої функціональні обов'язки, приймати інформовані рішення у всіх сферах життєдіяльності, реалізувати свою електоральну та іншу політичну активність. На жаль, інформатизація сьогодні породжує певну залежність людини від способів здійснення тих операцій, які раніше доводилося робити самостійно, а сьогодні їх виконання миттєво реалізується за допомогою шаблонних алгоритмів. Як справедливо вказує В.О. Кір'ян, інформаційне суспільство призвело до експоненційного збільшення зв'язків між елементами нових соціальних систем, що, у свою чергу, поєднане із процесами нелінійності культури, трансформацією звичайних соціальних систем, глобалізацією та етнізацією соціальних процесів, призводить до збільшення не тільки кількості, а й якості загроз. Дедалі зростаюча залежність від інформаційних технологій, які виробляються поза межами України, створює додаткові загрози залежності від чужих інформаційних технологій. Основою сучасних реальних кібернетичних загроз, тобто загроз, створених штучним інтелектом, загроз кібернетичного характеру, в яких людина не бере участь, виступає здатність цих систем до самостійного навчання через накопичення масивів інформації та готових матриць їх вирішення залежно від тих чи інших параметрів, здатності перебудовувати методи вирішення задач, а головне – здатність до самостійного формування таких задач із подальшим визначенням методів і наступним їх вирішенням, тобто здатність до само творення [1, с. 38].

Для того, щоб отримати певну інформацію, людина вже не потребує самостійно застосовувати свої навички аналізу та синтезу, застосовувати вміння моделювати певні варіанти розвитку подій. Засоби програмного забезпечення, які вміє сьогодні використовувати практично будь-яка людина, що займається нефізичною працею, роблять аналітичні операції значно швидше, і, головне, значно якісніше (за умови коректного застосування, безумовно). Як наслідок, виникає відчуження людини від засобів виробництва, працівник перетворюється на пасивний додаток до певних програм, вводячи в них певні відомості та дані, отримуючи та роздруковуючи результати їх аналізу, не розуміючи навіть принципові засади оброблення інформації.

За таких умов підвищується віктимність найбільш вразливої частини будь-якої системи інформаційної безпеки – людини. Достатньо дистанційного коригування програмного забезпечення (а воно, як ми пам'ятаємо, створюється переважно за межами України) – і функціонування атомних електростанцій або повітряний рух зазнають коригування, цілі якого можуть бути далекими від мирних.

Окремо слід сказати про рівень інформаційної культури військовослужбовців. Як справедливо вказують І.М. Коропатнік і І.М. Шопіна, спроможність Збройних Сил України своєчасно відповідати на виклики часу, професіоналізація сил оборони, ефективність виконання військовослужбовцями службово-бойових завдань мають своєю необхідною умовою підвищення рівня інформаційної культури рядового та командного складу на ціннісному, світоглядному та діяльнісному рівнях. Особливу важливість має, на думку авторів, керованість процесом її формування та зміцнення, що вимагає: визначення ключових індикаторів наявного

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).45

рівня інформаційної культури як на індивідуальному, так і на організаційному рівні, систематичного проведення моніторингу з метою визначення динаміки таких індикаторів; а також правового закріплення комплексу заходів щодо розвитку інформаційної культури у Збройних Силах України на рівні довгострокової програми, до виконання якої доцільно залучити, окрім внутрішньовідомчих, ресурси громадянського суспільства, що забезпечить більш об'єктивну оцінку отриманих результатів [2, с. 53]. Повністю погоджуючись з визначеною авторами необхідністю здійснювати роботу щодо формування рівня інформаційної культури військовослужбовців на світоглядному, ціннісному та діяльнісному рівнях, акцентуємо увагу на системності та систематичності такої роботи. Авральні методи на кшталт проведення виїзних лекцій та семінарів мають недостатній рівень ефективності, якщо не супроводжуються у майбутньому певним супервійзійним моніторингом (за встановленими педагогічною наукою закономірностями, якщо знання не пов'язані з практичним засвоєнням, виробленням вмінь та навичок, то в середньому через 6 днів у пам'яті залишається не більш ніж 20% отриманої інформації).

Враховуючи кількість осіб, виконуючих свої функціональні обов'язки в секторі безпеки і оборони, а також особливу важливість відносин, у яких вони беруть участь, для збереження територіальної цілісності, недоторканості та державного суверенітету нашої держави було б логічно уявити, що завдання забезпечення їх особистої інформаційної безпеки знайшло своє відображення у Законі України "Про національну безпеку України", який визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз, яким визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони [3]. Але аналіз цього закону свідчить, що питання особистої інформаційної безпеки представників сектору безпеки і оборони знаходяться поза межами правового регулювання. Така ж ситуація має місце з положеннями Закону України "Про основні засади забезпечення кібербезпеки України", який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [4]. Проте особистість людини вказаним законом не віднесена ні до об'єктів кібербезпеки, ні до об'єктів кіберзахисту. Отже, склалася ситуація, за якої увага держави спрямована переважно на вдосконалення технічних засобів захисту інформації, тоді як найбільш вразлива складова будь-якої системи інформаційної безпеки – людська особистість – навіть не розглядається як цінність, яку держава має захищати, хоча б для того, щоб у

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).45

певний момент не припинити своє суверенне існування (не кажучи вже про загальнолюдські гуманістичні ідеали).

Безумовно, Закон України "Про національну безпеку України" є більш досконалим, ніж попередній законодавчий акт, водночас у ньому залишилась велика кількість прогалин, пов'язаних із визначенням особливостей забезпечення інформаційної безпеки Подолання вказаних вад і прогалин є умовою та необхідним фактором для створення надійного механізму забезпечення інформаційної безпеки в Україні.

На підставі вказаного вище можна зробити такі висновки. По-перше, проблема протидії інформаційним загрозам у сфері національної безпеки є сьогодні найважливішою для забезпечення державного суверенітету, територіальної цілісності та незалежності нашої держави. Отже, на її вирішення мають бути спрямовані зусилля органів державної влади та місцевого самоврядування, науковців, усіх активних суб'єктів громадянського суспільства. По-друге, законодавство, яке регулює питання, пов'язані із забезпеченням національної безпеки в інформаційній сфері, вирізняється суперечливістю, наявністю великої кількості прогалин, що не дозволяє визначити правовий статус, сферу прав, обов'язків та відповідальності суб'єктів, діяльність яких має забезпечувати національну безпеку в інформаційній сфері.

Іншим аспектом цієї проблеми є постійне реформування органів, компетентних у сфері виконання завдань забезпечення інформаційної безпеки. Так, створення, а потім ліквідація Міністерства інформаційної політики України лише сприяло, на нашу думку, марному витрачанню надзвичайно великої кількості державних коштів, але не дозволила створити належний досвід управлінської практики, використання якого могло створювати певні перешкоди для інформаційної агресії Російської Федерації. Створення нових органів публічної влади, компетенція яких стосується забезпечення інформаційної безпеки, на жаль, також не супроводжуються залученням фахівців у цій сфері, зокрема, науковців, які розробили концепцію інформаційної безпеки нашої держави. Сподіваємось, що хаотичності та безсистемності підходу до проблем правового забезпечення інформаційної безпеки сектору безпеки і оборони прийде на зміну виважене та відповідальне ставлення до захисту найбільш цінної складової вказаної сфери – людини і громадянина.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Кір'ян В.О.* Інформаціологічний зміст ідеології безпеки. *Правова інформатика*. 2012. № 33 (1). С. 39–43.

2. *Шопіна І.М., Коропатнік І.М.* Роль інформаційної культури в підвищенні ефективності функціонування Збройних Сил України. *Наука і правоохорона*. 2017. № 2. С. 47–54.

3. Про національну безпеку: Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України* .2017. № 45. Ст. 403.

REFERENCES

1. *Kirian V.O.* (2012) Informatsiolohichnyi zmist ideolohii bezpeky. "Information content of security ideology". Pravova informatyka. No. 33 (1). P. 39–43 [in Ukrainian].

2. *Shopina I.M., Koropatnik I.M.* (2017) Rol informatsiinoi kultury v pidvyshchenni efektyvnosti funktsionuvannia Zbroinykh Cyl Ukrainy. "The role of information culture in improving the functioning of the Armed Forces of Ukraine". Nauka i pravookhorona. No. 2. P. 47–54 [in Ukrainian].

3. Pro natsionalnu bezpeku: Zakon Ukrainy vid 21 chervnia 2018 roku № 2469-VIII. "On National Security": Law of Ukraine of June 21, 2018 No. 2469-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2018. No. 31. Art. 241 [in Ukrainian]
4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. "On the Fundamental Principles of Cybersecurity of Ukraine": Law of Ukraine of October 5, 2017 No. 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2017. No. 45. Art. 403 [in Ukrainian]

UDC 342.951(477)

Onopriienko Stanislav,
Candidate of Technical Sciences, Senior Lecturer,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID 0000-0002-5524-1798

COUNTERING THREATS TO NATIONAL SECURITY IN THE INFORMATION SPHERE: THE LEGAL ASPECT

The article contains an analysis of trends in countering threats to national security. The author substantiates that the peculiarity of modern society is the development of information technologies that allow much faster production operations that previously took a lot of time and effort. Such trends can save human, temporary and other material resources. At the same time, informatization contributed to the emergence of the phenomenon of an excessive dependence of a person on information technology, with the help of which he is now able to fulfill his functional duties. A person becomes alienated from the means of production, the employee turns into a passive application to certain programs, entering certain information and data into them, receiving and printing the results of their analysis, and not understanding even the fundamental principles of information processing.

The author substantiates that under such conditions the victimization of the most vulnerable part of any information security system - the human being - increases.

The article contains an analysis of the provisions of the Law of Ukraine "On National Security of Ukraine". The author claims that the said law is more perfect than the previous legislative act, but at the same time a large number of gaps remained in it related to determining the features of ensuring information security. Overcoming these shortcomings and gaps is a condition and a necessary factor for creating a reliable mechanism for ensuring information security in Ukraine.

The author concludes that the problem of countering information threats in the field of national security is today the most important for ensuring state sovereignty, territorial integrity and independence of our state. The efforts of state authorities and local self-government, scientists, all active subjects of civil society should be aimed at solving this problem. The legislation regulating issues related to ensuring national security in the information sphere is notable for its inconsistency, the presence of a large number of gaps, and it does not allow determining the legal status, scope of rights, duties and responsibilities of entities whose activities should ensure national security in the information sphere.

Keywords: information security, national security, security and defense sector, information legislation, legal mechanism, information technology.

Отримано 25.10.2019