АКТУАЛЬНІ ПРОБЛЕМИ МІЖНАРОДНОГО ПРАВА, МІЖНАРОДНИХ ВІДНОСИН, БЕЗПЕКИ ТА ГЛОБАЛІСТИКИ

Кормич Б. А., НУ "ОЮА"

ПРАВОВІ ВАЖЕЛІ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ: МІЖНАРОДНИЙ І ВІТЧИЗНЯНИЙ ДОСВІД

В статье анализируются формы и виды угроз в информационной сфере. Рассмотрены основные аспекты международного и национального правового регулирования информационной безопасности.

The article provides the analyses of the forms and types of the threats in the informational sphere. The main aspects of the international and national level of legal regulation of the informational security are also reviewed.

Інформаційна безпека для сучасного цивілізаційного періоду стала однією з важливих проблем, що стосується як окремої людини, так і держави та суспільства в цілому.

Тому ця проблематика досліджується фахівцями різних галузей науки, зокрема правознавцями. Ряд конкретних питань аналізували такі вітчизняні і зарубіжні фахівці як І. Арістова, І. Бачило, В. Копилов, В. Лопатин, В. Ярочкін та інші [1 – 5].

Але багато аспектів залишаються недостатньо вивченими, що потребує подальшої наукової розробки. В даній статті вирішується завдання узагальнити підходи до розуміння існуючих інформаційних загроз, визначені сучасним міжнародним та національним законодавством.

Ще одним аспектом, на який необхідно звернути увагу, є проблема інформаційних війн та інформаційного тероризму, яка небезпідставно вважається однією з найактуальніших та найнебезпечніших загроз, яку несе в собі розвиток інформаційних технологій. Попри існування багатьох спільних ознак між інформаційними війнами та інформаційним тероризмом (адже і в тому і в іншому випадку відбувається несанкціоноване, протиправне втручання в інформаційні процеси), а різниця, насамперед, полягає у суб'єкті цих дій (держава або кримінальні чи терористичні угруповання), питання інформаційного тероризму набуло більш широкого визнання на міжнародному рівні, в той час, як питання інформаційних війн та інформаційної зброї дуже часто залишалося за рамками обговорень.

Так, ще у 1996 р. в Резолюції Організації Об'єднаних Націй 51/210 "Заходи щодо ліквідації міжнародного тероризму" (п 3. (с)) державам пропонувалось, здійснюючи заходи по боротьбі з тероризмом, в тому числі створюючи відповідне законодавство, "звернути увагу на ризик використання терористами електронних або дротових комунікацій для вчинення кримінальних дій і необхідність знайти засоби, погоджені з національним законодавством, для попередження подібної злочинності розвитку відповідної співпраці" [6].

Навпаки, правові проблеми інформаційної війни та регулювання застосування інформаційної зброї досить довгий час у сфері відкритої інформації виступали лише предметом наукових дискусій. З ініціативи Російської Федерації цю проблему було офіційно визнано на міжнародному рівні, коли 4 січня 1999 р. на 53 сесії Генеральної Асамблеї ООН було прийнято резолюцію 53/70 "Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки" [7]. В цій Резолюції було висловлено стурбованість тим, що новітні інформаційні технології і засоби телекомунікації можуть бути використані в цілях, несумісних із завданнями забезпечення міжнародної стабільності і безпеки, і можуть негативно вплинути на безпеку держав, відзначено необхідність попередити неправомірне використання або використання інформаційних ресурсів або технологій у злочинних або терористичних цілях, і у зв'язку з цим держави-члени ООН були закликані сприяти розгляду на багатосторонньому рівні існуючих і потенційних загроз в сфері інформаційної безпеки.

Специфікою інформаційної зброї є те, що об'єктом її застосування може бути будь-який з трьох типів елементів інформаційної сфери: "Засоби і лінії зв'язку – матеріальна основа світової інформаційної інфраструктури (до неї входять не лише засоби, поєднані між собою різноманітними каналами зв'язку, але й вся апаратура, призначена для обробки інформації); інформація в чистому вигляді і її потоки; безпосередньо сама людина" [8]. Таким чином застосування інформаційної зброї охоплює:

– деструктивний вплив на матеріальні об'єкти інформаційної сфери;

– знищення, спотворення або зміну інформації;

– цілеспрямований вплив на нервову систему, психіку та свідомість людини.

При цьому застосування такої зброї може носити як відкритий характер в умовах відкритого збройного конфлікту, так і латентний характер в рамках інформаційного протиборства в мирний час.

Значним кроком у створенні міжнародно-правових засад захисту інформаційної безпеки стало підписання в рамках Ради Європи Конвенції про кіберзлочинність, яке відбулося в Будапешті 23 листопада 2001 р. Україна ратифікувала цю Конвенцію у 2005 р. [9] Особливістю цього міжнародно-правового акта є те, що він встановлює певну систему правил, щодо видів правопорушень з використанням інформаційних та телекомунікаційних технологій, які країни-сторони даної Конвенції зобов'язані імплементувати в національне законодавство. Аналізуючи структуру Конвенції можна виділити декілька груп правопорушень в цій сфері. Так, всі "кібернетичні" правопорушення класифікуються на групи, в рамках яких виділяються окремі їх види.

Перша група носить назву "Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем". До неї входять такі дії, як: незаконний доступ, нелегальне перехоплення; втручання у дані, втручання у систему, зловживання пристроями.

Другу групу складають "правопорушення, пов'язані з комп'ютерами", що яких відносять: підробку, пов'язану з комп'ютерами та шахрайство, пов'язане з комп'ютерами (мається на увазі створення або підміна даних із злочинною метою).

Третя група – "правопорушення, пов'язані зі змістом" до якої відносяться правопорушення, пов'язані з дитячою порнографією.

Нарешті, четверту групу складають "правопорушення, пов'язані з порушенням авторських та суміжних прав".

Таким чином, можна говорити про поступовий розвиток міжнародно-правових стандартів в галузі інформаційної безпеки, які мають важливе значення для інформаційної безпеки національних держав, враховуючи сучасні тенденції глобалізації та інформатизації. Існує нагальна необхідність більш ширкого сприйняття Україною цих стандартів, зокрема створених в рамках програм та планів Європейського Союзу з формування Єдиного європейьского інформаційного простору.

Залучення міжнародного та зарубіжного досвіду при формуванні національного державно-правового механізму інформаційної безпеки дозволить уникнути так популярного в нашій країні процесу "винаходження велосипеду", оскільки в світі існує досить багато країн з більш високим рівнем інформатизації, які раніше зіткнулися з тими проблемами, які постають перед Україною сьогодні. Найбільш прийнятні організаційно-правові підходи до проблеми реалізовані законодавством Сполучених Штатів Америки, Канади, країн-членів Європейського Союзу, Російської Федерації. При цьому йдеться як про запозичення конструктивного досвіду, так і про відмову від кроків, що призвели до негативних наслідків в інформаційній сфері.

Виходячи з цього слід зазначити, що певною мірою міжнародний досвід впливає на формування національного законодавства та на процеси створення дієвого механізму інформаційної безпеки.

Закон України "Про основи національної безпеки" (ч. 2 ст. 5) визначає, що "національна безпека України забезпечується шляхом проведення виваженої державної політики" [10]. Таким чином, саме політика називається головним "інструментом" досягнення необхідних безпечних умов суспільного і державного життя. До того ж акцент робиться саме на державній політиці, тобто такій, яка проводиться від імені держави її владними органами. І це не дивно, адже саме в арсеналі державних засобів проведення політики є всім відомий інструмент державного примусу, який найчастіше і асоціюється із такими термінами, як "захист", "безпека" тощо.

Ця ж норма зазначає, що дана державна політика щодо забезпечення національної безпеки проводиться "відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах".

Серед таких програмних документів найважливішими є Стратегія національної безпеки України і Воєнна доктрина України, які є обов'язковими для виконання і основою для розробки конкретних програм за складовими державної політики національної безпеки. Дані документи розробляються на основі Закону України "Про основи національної безпеки" та затверджуються Президентом України.

Безпосердньо ж вибір конкретних засобів і шляхів забезпечення національної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Крім того, політика національної, та відповідно інформаційної безпеки повинна проводитися лише у тих формах і тими методами і засобами, які є притаманними і прийнятними у демократичній правовій державі. Тобто, базуватися на принципах демократії і верховенства права.

Як вже зазначалося, офіційна українська концепція безпеки побудована на позиціях визначення можливих загроз національним інтересам та встановлення адекватних відповідних заходів. Базові положення щодо визначення таких загроз і заходів містяться безпосередньо в Законі України "Про основи національної безпеки", на основі якого розробляються інші, більш деталізовані програмні документи щодо захисту окремих напрямків національної безпеки. Слід відзначити, що норми даного Закону носять в більшій мірі декларативний характер. Разом з тим вони можуть надати уявлення про конкретні сфери та напрямки реалізації державної політики в цій сфері.

Закон України "Про основи національної безпеки України" виділяє дві ключові категорії, якими обумволюється зміст та спрямованість державної політики в сфері інформаційної безпеки.

По-перше, це "***загрози національним інтересам і національній безпеці України в інформаційній сфері***" (ст. 7), до яких віднесено:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

По-друге, це така категорія, як "***основні напрями державної політики з питань національної безпеки в інформаційній сфері***" (ст. 8), які включають:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Розглядаючи питання напрямків державної політики в сфері інформаційної безпеки, необхідно назвати ще один законодавчий акт, який, хоч і не стосується загальних питань інформаційної політики держави, також визначає перспективні завдання в галузі інформаційної безпеки. Цим актом є Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [11], нормами якого, як вже згадувалося, дається найбільш повне визначення інформаційної безпеки.

В п. 13 даного Закону визначаються основні шляхи вирішення проблеми інформаційної безпеки, до яких віднесено такі, як:

– створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

– вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Як вже зазначалося, Закон України "Про основи національної безпеки України" передбачає розробку декількох програмних документів, які повинні визначати конкрентні напрямки проведення державної політики щодо безпеки в різних сферах.

Одним з таких ключових документів в сфері інформаційної безпеки є, затверджена Указом Президента України, *Стратегія національної безпеки України* [12]. Цей документ визначає принципи, пріоритетні цілі, завдання та механізми забезпечення життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз. Дана Стратегія є базою для розробки конкретних програм, проектів та планів заходів за складовими державної політики національної безпеки та механізмів їх реалізації і розрахована на період досягнення визначених нею цілей.

В якості головної мети цієї Стратегії визначається завдання забезпечити такий рівень національної безпеки, який би гарантував поступальний розвиток України, її конкурентоспроможність, забезпечення прав і свобод людини і громадянина, подальше зміцнення міжнародних позицій та авторитету Української держави у сучасному світі. Однією із складових даної мети є і забезпечення інформаційної безпеки.

Окремо відзначається, що державна політика національної безпеки України формується і реалізується за умов, коли у сучасному світі нівелюється різниця між внутрішніми та зовнішніми аспектами безпеки, зростає вага несилових (політичних, економічних, соціальних, енергетичних, екологічних, *інформаційних* складових її забезпечення.

Механізм реалізації державної політики інформаційної безпеки, відповідно до положень Стратегії національної безпеки, повинен складатися з трьох елементів: системи управління інформаційною безпекою, ресурсного забезпечення інформаційної безпеки та механізмів державного та громадського контролю за реалізацією цієї Стратегії.

Основним програмим документом, що визначає напрямки діяльності держави щодо захисту національної безпеки у військовій сфері та прийняття якого знову ж таки прямо передбачено законодавством є *Воєнна доктрина України* [13]. Воєнна доктрина представляє собою сукупність керівних принципів, воєнно-політичних, воєнно-стратегічних, воєнно-економічних і військово-технічних поглядів на забезпечення воєнної безпеки держави. В рамках цих поглядів та принципів значної уваги приділяється і питанням інформаційної безпеки та інформаційного забезпечення оборонної діяльності.

Зокрема, до основних завдань Збройних Сил України в мирний час, зокерма, віднесено

– здійснення розвідувальної та інформаційно-аналітичної діяльності в інтересах оборони держави;

– здійснення заходів щодо забезпечення інформаційної безпеки (п. 23);

Таким чином, ми можемо побачити, що у вітчизняному законодавстві існує цілий ряд нормативно-правових актів, які містять норми щодо визначення цілей та принципів забезпечення інформаційної безпеки. Разом з тим відповідні положення досить часто є неузгодженими та виражені в нормах-деклараціях або нормах-цілях, що не передбачають конкретних механізмів реалізації.

В світовій практиці питання формування поглядів та підходів на вирішення актуальних питань державного життя, в тому числі й інформаційної безпеки, традиційно вирішуються в форматі так званих Зелених та Білих книг, які створюються як державними так і недержавними інституціями. "Зелена книга" представляє собою зібрання конкретних проблемних питань, які потребують вирішення і виносяться на обговорення чи то в рамках органів державної влади, чи то в суспільстві в цілому. В свою чергу, за результатами такого обговорення формується "Біла книга", яка містить конкретні рекомендації щодо шляхів та способів розв'язання зазначених проблем.

В цьому аспекті цікавим є досвід Державної служби спеціального зв'язку та захисту інформації України, яка підготувала аналогічний проект під назвою "Біла книга з питань інформаційної безпеки". В рамках даної Білої книги висвітлюються стан та перспективи вирішення всього комплексу питань, пов'язаних з інформаційною безпекою України.

Зокрема, в Білій книзі запроваджена класифікація основних складових інформаційної безпеки, та конкретних завдань щодо їх захисту. Основними об'єктами захисту в рамках інформаційної безпеки в даній класифікації виступають інформаційний простір, інформація з обмеженим доступом та інформаційні ресурси. Відповідно виділяються основні системоутворюючі складові інформаційної безпеки, до яких належать:

1) захист інформаційного простору;

2) захист інформації з обмеженим доступом;

3) захист інформаційних ресурсів.

Політика інформаційної безпеки реалізується як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких входить вирішення питань щодо створення безпечних умов функціонування і розвитку інформаційної сфери.

Література:

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти / І. В. Арістова. – Харків: УВС, 2000.
2. Бачило И. Л. Информационное право / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. – СПб., 2001.
3. Копылов В. А. Информационное право / В. А. Копылов. – М.: Юристъ, 2002.
4. Кормич Б. А. Інформаційне право / Б. А. Кормич. – Харків: Бурун і К, 2011.
5. Ярочкин В. И. Информационная безопасность: Учебник / В. И. Ярочкин. – М.: Фонд "Мир", 2003.
6. United Nations. A/RES/51/210. "Measures to eliminate international terrorism" Resolution Adopted By The General Assembly. 17 December 1996.
7. United Nations. A/RES/53/70 "Developments in the field of information and telecommunications in the context of international security" Resolution Adopted By The General Assembly. 4 January 1999.
8. Петров В. От информационных войн к управляемому информационному сотрудничеству / В. Петров, И. Рабинович // Власть. – 2001. – № 1. – С. 21 – 22.
9. Конвенція про кіберзлочинність. Рада Європи. Будапешт 23 листопада 2001 р. (Ратифіковано Законом України "Про ратифікацію Конвенції про кіберзлочинність" від 7 вересня 2005 р. № 2824-IV).

10. Про основи національної безпеки України :Закон України від 19 червня 2003 р. № 964 – IV // Офіційний вісник України. – № 29. – С. 38. – Ст. 1433.
11. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
12. Про Стратегію національної безпеки України : Указ Президента України від 12 лютого 2007 р. № 105/2007.
13. Про Воєнну доктрину України : Указ Президента України від 15 червня 2004 р. № 648/2004.

Трюхан О. А., НУ "ОЮА"

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ПРАВОВОГО РЕГУЛЮВАННЯ ПРАЦЕВЛАШТУВАННЯ МОЛОДІ

Статья посвящена исследованию особенностей правового регулирования труда молодежи. В работе анализируются международно-правовые акты и некоторые нормы трудового законодательства Украины. Рассматривается право молодежи на труд в системе прав и свобод человека. Исследуются особенности правового регулирования условий труда молодых работников.

This article is devoted to the research of the peculiarities of the legal regulation of the youth work. The paper analyzes the international legal acts and some labor laws of Ukraine. The paper deals with the right of young people to work in the system of human rights and freedoms. Peculiarities of the legal regulation of the working conditions of the young workers are also studied

Найбільш уразливою та соціально незахищеною категорією населення є молодь. Через відсутність достатнього практичного досвіду, правових та професійних знань, а часто і моральної непідготовленості до конкуренції на ринку праці, реалізувати своє право на працю молодим громадянам сьогодні складно. Різниця між рівнем домагань молодої людини високого життєвого рівня та можливостями його досягнення, між особистими сподіваннями та труднощами часто призводить до дезадаптації індивідуума, що в остаточному підсумку може призвести до поведінки протиправного характеру, тобто до злочинності, алкоголізму, наркоманії тощо.