

## Основні складові інформаційної безпеки держави

*Анна Турчак, Інститут підготовки кадрів державної служби зайнятості України*

У статті з'ясовані основні складові інформаційної безпеки держави. Встановлено, що інтереси будь-якої країни значною мірою залежать від збереження інформаційної безпеки. Створити розвинене і захищене інформаційне середовище – неодмінне завдання для суспільного та державного розвитку. Продовж останнього часу світ зазнав якісних змін щодо процесів управління, зумовлених тим, що інтенсивно впроваджуються сучасні інформаційні технології. Водночас стає більш імовірним несанкціоноване втручання в робочий процес будь-якої інформаційної системи, і значення наслідків від цієї небезпеки значно зросло. В результаті багато країн все більшу увагу приділяє проблемним питанням, пов'язаним із захистом інформації та пошукам відповідних рішень. Доведено, що дослідження питань державної інформаційної безпеки дає змогу говорити, що забезпечування інформаційної безпеки базується на інформаційній організації країни. Ця організація має надавати гарантію інформаційної безпеки держави та її суб'єктів під час глобалізаційних процесів та підвищення загрози, яку становить міжнародний тероризм. На жаль, в Україні є дуже багато чинників, які стають перешкодами при створенні такої інформаційної організації, тут грає не останню роль неузгодження роботи державних владних органів щодо забезпечування інформаційної безпеки. Таким чином, науковий аналіз ряду проблемних питань щодо розробки та втілення державної політики в межах інформаційної сфери сьогодні має особливе значення, адже їх розв'язання дасть змогу розвиватися суспільству, що має інформаційний характер, і у такий спосіб забезпечить національну та інформаційну безпеку України.

**Ключові слова:** державна політика, інформація, інформаційна безпека, інформаційна політика, інформаційне середовище, національна безпека, складові, суспільство

## Main composition of information security of the state

*Anna Turchak, Institute of Personnel Training of the State Employment Service of Ukraine*

The article clarifies the main components of state information security. It has been established that the interests of any country depend to a large extent on the preservation of information security. Create a well-developed and secure information environment - an indispensable task for public and state development. The world has undergone qualitative changes in recent management processes due to the intensive implementation of modern information technologies. At the same time, unauthorized interference with the workflow of any information system becomes more likely, and the significance of the consequences of this danger has increased significantly. As a result, many countries are paying more attention to the problem of information protection and the search for appropriate solutions. It was discovered that the phenomenon of "information security" involves the high-quality informing of people and free access to various information bases, but there should also be control actions for non-dissemination of classified information, maintenance of the society in a state of integrity, protection against any negative informational influence, etc. Solving this complex problem issue will enable both the protection of public and state interests, as well as the promotion of the rights of the citizen to comprehensive and high-quality information. It has been proved that the study of issues of state information security makes it possible to say that information security is based on the information organization of the country. This organization should provide a guarantee of informational security of the state and its subjects during the globalization processes and increasing the threat posed by international terrorism. Unfortunately, Ukraine has a lot of factors that hinder the creation of such an information organization; the role of non-coordination of the work of state authorities in providing information security plays a role here. Thus, the scientific analysis of a number of problematic issues regarding the development and implementation of state policy within the information sphere is of particular importance today, since their solution will enable for the development of a society that is informational in nature and thus will ensure the national and informational security of Ukraine.

**Keywords:** state policy, information, information security, information policy, information environment, national security, components, society

## Основные составляющие информационной безопасности государства

Анна Турчак, Институт подготовки кадров государственной службы занятости Украины

В статье выяснены основные составляющие информационной безопасности государства. Установлено, что интересы любой страны в значительной степени зависят от сохранения информационной безопасности. Создать развитую и защищенную информационную среду – непереносимые задачи для общественного и государственного развития. В течение последнего времени мир претерпел качественные изменения относительно процессов управления, обусловленных тем, что интенсивно внедряются современные информационные технологии. В то же время становится более вероятным несанкционированное вмешательство в рабочий процесс любой информационной системы, и значение последствий этой опасности значительно возросло. В результате многие страны все больше внимания уделяют проблемным вопросам, связанным с защитой информации и поиском соответствующих решений. Доказано, что исследование вопросов государственной информационной безопасности позволяет говорить, что обеспечение информационной безопасности базируется на информационной организации страны. Эта организация должна предоставлять гарантию информационной безопасности государства и его субъектов при глобализационных процессах и повышении угрозы, которую представляет международный терроризм. К сожалению, в Украине имеется очень много факторов, которые становятся препятствиями при создании такой информационной организации, здесь играет не последнюю роль несогласование работы государственных органов власти по обеспечению информационной безопасности. Таким образом, научный анализ ряда проблемных вопросов по разработке и реализации государственной политики в пределах информационной сферы сегодня имеет особое значение, ведь их решение позволит развиваться обществу, которое носит информационный характер, и таким образом обеспечит национальную и информационную безопасность Украины.

**Ключевые слова:** государственная политика, информация, информационная безопасность, информационная политика, информационная среда, национальная безопасность, составляющие, общество

### Постановка проблеми.

Інтереси будь-якої країни значною мірою залежать від збереження інформаційної безпеки. Створити розвинене і захищене інформаційне середовище – неодмінне завдання для суспільного та державного розвитку. Продовж останнього часу світ зазнав якісних змін щодо процесів управління, зумовлених тим, що інтенсивно впроваджуються сучасні інформаційні технології. Водночас стає більш імовірним несанкціоноване втручання в робочий процес будь-якої інформаційної системи, і значення наслідків від цієї небезпеки значно зросло. В результаті багато країн все більшу увагу приділяє проблемним питанням, пов'язаним із захистом інформації, та пошукам відповідних рішень.

Питанням складових інформаційної безпеки держави присвячували свої праці такі провідні науковці, як Гнатцов О. Г., Деремо В. Н., Деремо В. Н., Морозов О. Л.,

Соснін О. В. та інші. Проте, станом на сьогодні актуалізується необхідність дослідження основних складових інформаційної безпеки держави, що зумовило вибір теми даної статті.

### Мета дослідження.

У статті поставлено за мету з'ясувати основні складові інформаційної безпеки держави.

### Виклад основного матеріалу.

Держави, котрі не здатні до забезпечення власної інформаційної безпеки, перетворюються на неконкурентоспроможні і, як підсумок, втрачають змогу боротися за ринки та ресурси. Можемо підкреслити, що великі держави зникли частково через нездатність ефективно управляти на власних територіях та інформаційну структуру, що не могла дієво функціонувати в нових умовах існування. Тому не можна заперечувати те, що будь-яка розвинена країна повинна мати систему, що забезпечувала б інформаційну безпеку, а перелік закріплених

відповідними державними органами функцій та повноважень повинен бути закріплений в законодавстві.

Явище «інформаційна безпека» передбачає якісне інформування людей та вільний доступ до різноманітних інформаційних баз, однак повинні бути ще й контролюючі дії щодо нерозповсюдження секретної інформації, підтримання соціуму у цілісному стані, захист від будь-якого негативного інформаційного впливу таке ін. Вирішення такого комплексного проблемного питання дасть можливість як захисту суспільних і державних інтересів, так і сприяння утвердженню прав громадянина на всебічну та якісну інформацію.

Щоб ефективно забезпечувати інформаційну безпеку в країні, необхідно вирішити такі масштабні завдання: розробити теоретичні основи по забезпеченню захисту інформації; створити систему структур, які б відповідали за збереження інформаційної безпеки; вирішити питання щодо захисту інформації і налагодити її автоматизацію; створити нормативно-правову базу, що регламентувала б вирішення всіх завдань, пов'язаних із забезпеченням інформаційного захисту; почати виробляти засоби інформаційної безпеки; організувати підготовку спеціалістів відповідного фаху тощо.

Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни [10].

Контекст нацбезпеки передбачає вивчення двох аспектів поняття «інформаційна безпека». Згідно з першим воно вважається самостійним елементом нацбезпеки у будь-якій країні, а згідно з другим – інтегрованою складовою будь-якого іншого виду безпеки, такого як, наприклад, військова, економічна, політична тощо.

Одне з найповніших тлумачень терміну «інформаційна безпека» розглядає її в якості стану, за якого життєво-важливі особистісні, суспільні і державні інтереси є захищеними, мінімізуються збитки, спричинені неповнотою, невчасністю і недостовірністю інформації, негативним інформаційним впливом, негативними наслідками функціонування технологій в інформаційній сфері, а також несанкціонованим поширенням даних. Це трактування так чи інакше об'єднує фактично усі галузі інформаційної взаємодії, в якій перебувають державні суб'єкти.

Інформаційна безпека як невід'ємна складова національної безпеки вперше була присутньо описана у Законі «Про основи національної безпеки України».

Інформаційний суверенітет країни і система його захисту дуже пов'язані із інформаційною безпекою, яку можна розглянути, як стан захищеності внутрішніх інформаційних масивів як таких, тобто захищеності якісного рівня інформації, ступінь її надійності, захищеності різних інформаційних сфер від розголосу, а також захищеності інформаційно-ресурсної бази. З іншої точки зору, інформаційну безпеку можна вважати контролем інформаційних потоків, обмеженням у використанні провокативної, агресивної до суспільства інформації, регулюванням рекламної інформації; механізмом, за допомогою якого захищають національний інформаційний простір від зовнішнього інформаційного загарбання.

Серед головних складових інформаційної безпеки держави виділяють: обсяг інформаційного продукту, що виробляється в державі і державою; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них [5].

Потребу забезпечити інформаційну безпеку зумовлюють багато факторів: необхідність підтримати національну

безпеку Української держави загалом; наявність небезпек, що загрожують інформаційному середовищу держави і можуть нести шкоду для загальних національних інтересів; можливість шляхом інформаційного впливу частково керувати свідомістю і поведінкою громадян. Інформаційна безпека України має перед собою головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Також така ціль передбачає потребу створити систему протистояння будь-якій інформаційній загрозі та оборону власних інформаційних ресурсів, середовища та інфраструктурної складової країни.

Враховуючи те, що національному інформаційному ресурсу нині відводиться роль одного з основних чинників, на якому базується економічна потужність країни та її суб'єктів, необхідно формулювати державні інтереси, фактори і загрози для інформаційної сфери, аналізувати ефективність наявної системи захисту та можливості її покращення. Державна інформаційна політика створює контекст для того, щоб обговорення стосувалося не лише прав людей, юридичних осіб і країни в інформаційній галузі, але і потреби захистити інтелектуальну власність, державні інформаційні ресурси та конфіденційну інформацію.

Окрім того, можна виділити ряд основних положень держполітики забезпечення інформаційної безпеки: скорочення доступності інформації є винятком із загальних засад про відкритість інформаційних джерел і реалізується лише на законодавчій підставі; необхідність персоніфікації відповідальності за те, що інформацію зберігали, засекретили чи розсекретили; надання та вилучення доступу до інформаційних ресурсів реалізується на підставі законодавчо затвердженого права власності на цю інформацію; державою формується нормативно-правова база, що здійснюватиме регулювання прав, обов'язків і відповідальності всіх суб'єктів

в інформаційному просторі; наявність правової відповідальності юридичних і фізичних осіб, що займаються збором, нагромадженням і обробкою персональних даних і конфіденційної інформації, за її збереження і використання; країна законним чином захищає суспільство від помилкових, перекручених і недостовірних відомостей, що надходять через ЗМІ; влада контролює створення і використання будь-якого засобу інформаційного захисту, в обов'язковому порядку сертифікуючи такий і ліцензуючи діяльність у галузі інформаційної безпеки; протекціоністська політика з боку держави, що означає підтримку вітчизняного виробника, що виготовляє засоби інформатизації і захисту інформації, і здійснення заходів для того, щоб захистити внутрішній ринок від появи на ньому неякісного інформаційного продукту; держава робить світові інформаційні ресурси, глобальні інформаційні мережі доступнішими для громадян; країна намагається відмовитися використовувати закордонні інформаційні технології для інформатизації державних владних і управлінських структур і віддати перевагу конкурентоздатним вітчизняним аналогам; в державі формується програма інформаційної безпеки, в якій консоліднують свої сили державні організації і комерційні структури задля того, щоб створити єдину систему інформаційної безпеки; країна активно протидіє інформаційному вторгненню з боку решти держав, сприяє тому, щоб глобальні інформаційні мережі й системи інтернаціоналізувалися.

Згідно з вищезазначеними принципами і положеннями забезпечити інформаційну безпеку країни можна, зробивши ряд важливих кроків: розвинути науково-практичні основи інформаційної безпеки у відповідності до сучасної геополітичної ситуації та умов, продиктованих політичним і соціально-економічним розвитком; формувати законодавчу і нормативно-правову бази, щоб забезпечити інформаційну безпеку, зокрема розробити реєстр інформаційних ресурсів, регламентувати інформаційний обмін між органами держави, підприємствами,



нормативно закріпити відповідальність посадовців і пересічних українців за відповідність критеріям інформаційної безпеки; розробити механізми втілення права громадянина на інформацію; формувати систему інформаційного захисту, що є складником загального механізму нацбезпеки України; розробити сучасні методи і технічні засоби, що забезпечували б комплексний підхід до вирішення завдань інформаційного захисту; розробити критерії і методи, за якими оцінюватимуться системи і засоби інформаційної безпеки з точки зору ефективності і їх сертифікації; дослідити форми і можливості державі цивілізовано впливати на суспільну свідомість; комплексно дослідити діяльність кадрів в інформаційних системах, зокрема методи мотивування, посилити морально-психологічну стійкість і соціальну захищеність фахівців, що мають справу із секретними і конфіденційними даними.

Інформаційну безпеку країни в загальнонаціональних масштабах визначають як систему заходів, що мають на меті не допустити несанкціонований доступ до інформаційних ресурсів, їхню модифікацію та руйнацію. Вона передбачає втілення таких цілей: захистити політичні, державні і громадські інтереси; захистити моральні цінності; заборонити інформацію, яка пропагує агресивну війну, насилля, дискримінацію та порушення прав громадянина.

Національні інтереси Української держави мають певні пріоритети, визначені в «Законі України Про основи національної безпеки України». Серед них є такі, що стосуються інформаційної сфери: гарантувати конституційні права і свободи людини і громадянина; зберегти та зміцнити науково-технологічний потенціал, утвердити інноваційну модель розвитку; забезпечити розвиток і реалізацію функцій, які покликана виконувати українська мова як державна в кожній сфері життя суспільства по всій Україні, гарантувати вільний розвиток, застосування і захист усіх мов нацменшин в Україні; розвивати духовність, моральні

засади, інтелектуальний потенціал Української нації.

Важливою проблемою безпеки у сфері інформації, як уже зазначалося, є забезпечування захисту і моніторинг національної інформаційної бази та розповсюдження інформації про державу у межах світового інформаційного простору. Інформаційний простір слід розуміти як середовище, у межах якого відбувається створення, збір, зберігання, обробка і поширення інформаційних даних, яке підлягає державній юрисдикції.

Слід підкреслити, що будь-які інформаційні технології складаються із: формування інформаційних даних, їх оброблення, зберігання та передачі (засвоєння). Задля безпеки слід подбати про надійну роботу усіх складників такої системи. Аналізуючи проблему з цього ракурсу, можна виокремити головну ціль діяльності у сфері інформації – створення повноцінної відкритої інформаційної бази.

Відсутні відомості, їх повністю чи в більшості негативний характер щодо сучасного світу чинить вплив на рівень зовнішньополітичної і економічної діяльності як на державному рівні загалом, так і на окремих представників населення та їх об'єднань. Це зумовлює загальнодержавне значення цієї проблеми, а при її нехтуванні стає загрозою для національної безпеки. Саме через це створюються належні умови для розширювання інформаційної присутності у межах світового інформаційного простору, що є найважливішим завданням держполітики у такій сфері, як інформаційна безпека.

Одним із основних елементів реалізації державної політики в інформаційній сфері є інформаційна інфраструктура, що є невід'ємною частиною стратегічних інформаційних ресурсів і має велике значення для обороноздатності держави і її інформаційного ринку. За Законом України „Про Концепцію національної програми інформатизації” до інформаційної інфраструктури входять: міжнародні та міжміські телекомунікаційні та комп'ютерні мережі; системи

інформаційно-аналітичних центрів; інформаційні ресурси; інформаційні технології; системи науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформації; система підготовки кваліфікованих фахівців у сфері інформатизації [8]. Інформаційною інфраструктурою є єдність таких компонентів, як: система виробництва продуктів інформаційної сфери, доставка їх до споживачів, система вироблення інформаційної продукції та її доставка, система вироблення інформаційних технологічних засобів, система накопичування і зберігання інформаційних продуктів або інформаційних ресурсів, тобто системи сервісних послуг, що надаються об'єктам інфраструктури, і система підготовки спеціалістів.

Вдосконалення суспільних відносин великою мірою залежить від розвитку інформаційних ресурсів, які є базовими для створення ефективних моделей державного управління. Отже, цей вид ресурсів є водночас об'єктом управління і предметом діяльності державної влади та її інститутів. Інформаційні ресурси – це інформаційна інфраструктура та циркулююча в ній продукція інформаційної діяльності, яка дає змогу вирішувати відповідні завдання [1]. Найважливіше тут зрозуміти те, що ці два елементи інформаційного ресурсу взаємодоповнюють один одного і не можуть використовуватися окремо.

Першою складовою системи забезпечується оперативне керування країною, друга зосереджена на оперативному рівні, а третьою здійснюється планування стратегічного характеру, спрямоване на зовнішньополітичну діяльність.

Розглядаючи проблему інформаційної безпеки, важливо виділити загрози для інформаційної безпеки та проаналізувати шляхи захисту від цих небезпек. Загрози інформаційній безпеці – явища, дії факторів, що мають негативний характер або процеси, що зумовлюють: часткове або повне втрачання можливості забезпечити власні інтереси в межах

інформаційної сфери соціальними об'єктами, що підлягають інформаційній безпеці; порушення нормальної життєдіяльності, здійснення руйнації або стримування розвитку об'єктів технічного інформаційного спрямування у сфері безпеки.

Як правило, виділяють такі типи інформаційних загроз: політичні; економічні; суспільні; військові та науково-технічні [10]. В політичній сфері це: система державного управління; системи підготовки прийняття політичних рішень; виборчі системи; телекомунікаційні системи спеціального призначення. В економічній: система прийняття рішень; банківська інфраструктура; управління економічним станом в умовах надзвичайних ситуацій; система управління державними комунікаціями, які мають економічний характер; корпоративні війни і промисловий шпіднаж. В суспільній: загрози для системи формування громадської думки; системи ЗМК; структури політичних партій, громадських рухів, релігійних організацій; структури забезпечення основних прав і свобод людини. У військовій: інформаційні ресурси збройних сил; системи управління військами; системи постійного контролю і спостереження; канали надходження інформації стратегічного, оперативного і розвідувального характеру. В науково-технічній: системи накопичення ноу-хау; об'єкти інтелектуальної власності; структури фундаментальних і прикладних досліджень; структури аналізу та прогнозування тенденцій в науково-технічній сфері; бази і банки даних конфіденційного характеру.

Закон України “Про національну безпеку України” визначає наступні загрози національним інтересам і національній безпеці України в інформаційній сфері: 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 [9].

Вітчизняні експерти [7], як правило, загрози інформаційній безпеці України за своєю загальною спрямованістю, поділяють на такі види: загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; загрози інформаційному забезпеченню державної політики України; загрози розвитку вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку; загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються.

Загрозами для інформаційного забезпечення української державної політики вважають: монополізацію інформаційної вітчизняної ринкової системи, її певних сфер, що підтримують вітчизняні і закордонні інформаційні структури; блокування роботи державних ЗМІ щодо поінформування українських і закордонних мас населення; наявність низької ефективності інформаційного забезпечення, спрямоване на державну політику через дефіцит фахівців, відсутню систему створення і втілення державної політики у сфері інформації.

До загроз розвитку української інформаційної галузі можна віднести: протидію доступу української держави до новітнього інформаційно-технологічного забезпечення, взаємовигідній і рівноправній участі української промисловості у світовому поділі праці в індустрії інформаційної сфери, інструменти, що передбачає інформатизація, телекомунікація і зв'язок, інформаційні продукти та сприяння поглибленню технологічної залежності

України у сфері новітніх технологій в інформаційній сфері; закупка державною владою засобів інформатизації з-за кордону, телекомунікаційних засобів і засобів зв'язку при наявності українських відповідників, що не поступаються параметрами закордонному виробництву; витіснення з вітчизняного ринкового простору українського виробництва вищезгаданих засобів; від'їзд за межі держави висококваліфікованих спеціалістів.

Загрозами для безпеки інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються, можуть бути: протиправні збирання та використання інформації; порушення технології обробки інформації; впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби; розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації; знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку; вплив на пароліно-ключові системи захисту автоматизованих систем обробки і передачі інформації; компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах; впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності; знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації; перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікацій і зв'язку під час створення й розвитку

української інформаційної інфраструктури; несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації [7].

Найбільше вражає те, що одна з основних загроз інформаційної безпеки міститься у сфері роботи органів державної влади: невиконання або неналежне виконання державними владними органами власних повноважень у межах інформаційної сфери. Хоч, згідно з Конституцією України, інформаційна безпека – один із пріоритетів країни та справа усіх українців.

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз [4]. Внутрішні джерела – це відсутність історичних, політичних та соціальних практичних навичок проживання на території правової держави, що зачіпає процес практичного втілення конституційних прав і свобод населення, зокрема, в межах інформаційної сфери та примноження організованих правопорушень та ріст числа правопорушень комп'ютерного спрямування, зменшення частки числа освіченого населення, що сильно утруднює підготовку трудового ресурсу для застосування новітнього технологічного забезпечення, зокрема, інформаційного. Недостатня координація роботи такого органу, як вище державне керівництво, владних структур та угруповань військового характеру у втіленні єдиної державної політики забезпечення нацбезпеки теж можна зарахувати до таких джерел. Тут же і відставання нашої держави від розвинених країн за інформатизацією посадовців, юридично-фінансових, промислових структур та побутовими умовами населення. Серед джерел зовнішнього характеру є іноземні політичні, військові, економічні та розвідувальні структури інформаційної сфери; політика домінування певних держав в інформаційній сфері; робота міжнародних терористичних угруповань; розробка різними структурами концепції

війн інформаційного характеру; культурне захоплення конкретних країн.

В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів, дезорганізації державного управління тощо. Розгляд питань інформаційної безпеки дозволяє виділити чотири групи інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу. Першу групу пов'язують зі стрімким розвитком нової зброї інформаційного характеру, що здатна результативно впливати на людську психіку і інформаційно-технологічні державні структури. Аналіз досліджень сьогодення в цій галузі дає змогу говорити про ефективні результати програмування, спрямованого на поведінку окремих особин, що піддаються впливу, на комп'ютерну систему банків даних знань і інформаційні ресурси. Другою групою передбачається наявність нового вигляду правопорушень соціального спрямування, що базуються на досягненнях новітнього інформаційно-технологічного забезпечення: махінації з операціями банку; хуліганство у комп'ютерній сфері; протизаконне копіювання технологічних рішень тощо. Як вважають провідні дослідники цієї галузі, комп'ютерні технології стають провідними знаряддями злочинів. Третьою групою є електронний контроль життя, настроїв, планів населення та організацій політичного характеру, тотальний комп'ютерний контроль за суспільством держави. Інформаційними технологіями дозволяється накопичення, зберігання і використання величезних масивів інформації про здоров'я, активність соціального плану, політичні настрої, відносини, фінансове забезпечення громадян. Четвертою групою є використання інформаційних технологічних засобів у політичній боротьбі. Підвищення впливу ЗМІ на політичні процеси, роботи владного



механізму – одна з головних тенденцій розвитку суспільства у наш час.

Далі з'ясуємо, якими ж засобами користується інформаційний захист від перелічених небезпек. Кожна загроза безпеці різних галузей інформаційної життєдіяльності має відповідні напрямки, методологію та систему заходів по забезпеченню інформаційної безпеки. Так, Закон України «Про національну безпеку України» серед основних напрямів державної політики з питань національної безпеки в інформаційній сфері виділяє: 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 [9].

Головним завданням заходів із забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [6].

Загалом основні напрямки діяльності по забезпеченню інформаційної безпеки

держави являють собою величезний комплекс заходів, до яких відносяться: розвиток науково-практичних основ інформаційної безпеки; розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки; розробка нормативно-правових і організаційно-методичних документів; розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів; формування правового статусу суб'єктів системи інформаційної безпеки; розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці; відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці; розвиток сучасних методів забезпечення інформаційної безпеки [3].

Розвитком науково-практичної бази, що має інформаційна безпека, зумовлюються: розроблення стратегії забезпечення інформаційної безпеки держави; обґрунтування державної політики за умови глобалізаційних інформаційних явищ, створення інформаційних мереж світового значення, бажання певних країн мати найкращий розвиток і застосовувати світовий інформаційний простір; розроблення науково-практичної бази створення і провадження державної політики у такій сфері, як інформаційна безпека; обґрунтування пріоритетних завдань нацбезпеки, що містять довгостроковий інтерес, відповідний суспільному розвитку.

Розвиток законодавчих і нормативно-правових основ забезпечення інформаційної безпеки передбачає окреслення почерговості розроблення актів законодавчого і нормативно-правового характеру та механізмів практичного втілення чинної законодавчої системи.

Розроблення нормативно-правового і організаційно-методичного переліку документів містить створення документації, що регламентує: роботу в

галузі інформаційної безпеки державних владних структур; взаємовідносини суб'єктів інформаційної діяльності для забезпечування інформаційної безпеки; врегулювання державними органами процесів роботи і розвитку, що здійснює ринок засобів інформації, розвиток інформаційних продуктів і послуг; інформаційних відносин в соціумі і на державному рівні, зважаючи на ринкову економіку та ін.

Правовий статус для суб'єктів інформаційної безпеки потребує забезпечення такого статусу для користувачів інформаційного і телекомунікаційного напрямку; вимагає визначити їхню відповідальність за забезпечування процедури втілення законодавчих норм і актів до суб'єктів, на які поширюється інформаційна безпека, які вчинили злочин, працюючи із закритими даними, та злочин, що передбачає застосування незахищеного засобу інформації; розробити склад злочинів, враховуючи специфіку відповідальності кримінального, цивільного, адміністративного, дисциплінарного характеру.

Покращення організації, спрямованої на форми і методи уникнення і усунення загроз інформаційній безпеці, включає: розроблення нормативно-правових основ життєдіяльності системи інформаційної безпеки, розрізнення повноважень державних владних структур, що повинні забезпечувати інформаційну безпеку; розроблення моніторингової системи, що аналізує інформаційну безпеку на предмет її стану; розроблення ідей по створенню позитивних факторів, щоб подолати критичний стан промислових сфер України, у галузі, що поширюється на інформатизацію і захист інформації; аналізування техніко-економічного показника українського та іноземного програмно-технічного забезпечення, спрямованого на інформаційну безпеку і обрання ефективних напрямів розвитку українського технічного забезпечення; розроблення системи даних економічного і статистичного характеру, що показують результативність роботи, проробленої системою забезпечування такої галузі, як інформаційна безпека;

досліджування критеріїв і методології оцінювання результативності інформаційної безпеки та ін.

Розвиток новітніх методів інформаційної безпеки – це розробка форм і інструментів, що сприяють цивілізованому впливові держав на формування колективної свідомості суспільства і практичних рекомендацій із реалізації у практичному застосуванні; розроблення методології комплексних досліджень роботи працівників інформаційної системи, разом з тим і методів підвищування мотиваційного рівня, морально-психологічної стабільності і соціального захисту осіб, що провадять роботу із секретними і конфіденційними даними; розробка практичних рекомендацій зі збереженням і зміцненням суспільної політичної рівноваги; забезпечення прав і свобод населення; зміцнення таких понять як законність і правопорядок методологією, що має інформаційна безпека; створення шляхів і інструментів для забезпечування органів державної влади, фірм і осіб достовірними, повними і своєчасними даними; розроблення головних діяльнісних напрямів по запобіганню негативного інформаційного впливу на настрої індивідуальної, групової і суспільної свідомості; розроблення цивілізованої, демократичної форми і методології впливу на ЗМІ; розроблення механізмів розвитку, що мають інформаційні відносини у підприємницькій сфері і зарахування інформаційних ресурсів до господарських відносин; досліджування головних методів зниження криміногенних обставин, зменшення кількості злочинів комп'ютерного характеру, насамперед, у межах кредитно-фінансової сфери; розроблення методології і практичної рекомендації із контролем над експортними операціями щодо вітчизняного наукомісткого технологічного забезпечення; обґрунтування напрямів протистояння засобам, що вважаються інформаційною зброєю; вдосконалення видів контролювання персоналу у рамках захищених систем інформаційної сфери.

Одна з головних передумов, що сприяє національній безпеці держави – наявність її економічного потенціалу, тобто

комплекс потужностей матеріального і духовного спрямування громадськості та здатність держави задіяти ці потужності, щоб забезпечити свою безпеку. В свій час інформацією охоплюються усі сфери функціонування людини і підвищується рівень економічного потенціалу держави, сприяючи зростанню матеріального і духовного суспільного потенціалу, створювати передумови координації та мобілізації. Окрім цього, вона формує матеріальний і інтелектуальний ресурс країни для того, щоб забезпечити ефективний захист від агресивних в інформаційному плані країн.

З вищесказаного очевидно, що державна політика в сфері формування інформаційних ресурсів і інформатизації повинна бути спрямована на створення умов для ефективного і якісного інформаційного забезпечення рішення задач соціально-економічного розвитку країни. Серед основних напрямків державної політики в сфері інформатизації виділяють: забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси; формування і захист державних інформаційних ресурсів; створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі; створення умов для якісного й ефективного інформаційного забезпечення громадян, органів державної влади, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення національної безпеки в сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної і промислової політики в сфері інформатизації з обліком сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення й удосконалювання системи залучення інвестицій і механізму стимулювання розробки і реалізації проектів інформатизації;

розвиток законодавства в сфері інформаційних процесів, інформатизації і захисту інформації [2].

Слід відразу зазначити, що ніякі окремо взяті засоби захисту не мають змоги стати запорукою адекватної безпеки. Наявність надійного захисту, що можливий тільки за умов створення механізмів комплексного забезпечення безпеки. Як правило, виділяють три головні складники такої комплексної діяльності: нормативно-правовий; технічний; засоби організації.

Нормативно-правовий інструментарій захисту визначають державні законодавчі акти, що врегульовують правила застосування, оброблення та передавання інформаційних даних, що мають обмежений доступ та визначають рівень відповідальності за їх порушення. Ст. 34 Конституції України розглядає право українських громадян на інформацію, забезпечування процесів інформаційного характеру. Ця та решта статей Конституції повинні виступати як основа розвитку законодавства інформаційної сфери. Невідповідний характер діючого законодавства України вимогам, що ставить інформаційний прогрес – одна з головних проблем про захист інформації, що за наявних в державі потужних науково-технічних ресурсів може спричинити особливо тяжкі наслідки.

Увесь комплекс технічних засобів поділяють на фізичні та апаратно-програмні, що включають прилади електричного, механічного, електромеханічного та електронного типу. Фізичним засобам притаманне втілення як автономних пристроїв та систем, що здійснюють функції загального захисту об'єктів, які обробляють на них інформацію. Розміщення апаратних технічних засобів відбувається власне в обчислювальній техніці, в телекомунікаційних апаратах чи в приладах, що зв'язуються з такою апаратурою стандартним інтерфейсом. Програмним засобам співвідносне поняття програмного забезпечення, що забезпечує функції захисту інформаційних даних.

Організаційні засоби захисту поділяють на ті, що мають організаційно-технічний

характер та ті, що мають організаційно-правовий, який використовують при створенні та функціонуванні будь-яких структур. Іншими словами, лише на нормативно-правовій базі та за наявності апаратно-програмного забезпечення можливо ефективно керувати за широкого впровадження новітніх інформаційного технологічного забезпечення. Ці питання часто недооцінюють керівники різноманітних організацій.

Усе це дає змогу підсумувати, що достатній рівень інформаційної державної безпеки забезпечує цілий комплекс заходів політичного, економічного, організаційного та решти характеристик, що дають змогу реалізувати інформаційні права та інтереси країни і її суб'єктів.

#### **Висновки.**

Дослідження питань державної інформаційної безпеки дає змогу говорити, що забезпечування

інформаційної безпеки базується на інформаційній організації країни. Ця організація має надавати гарантію інформаційної безпеки держави та її суб'єктів під час глобалізаційних процесів та підвищення загрози, яку становить міжнародний тероризм. На жаль, Україна має дуже багато чинників, які стають перешкодами при створенні такої інформаційної організації, тут грає не останню роль неузгодження роботи державних владних органів щодо забезпечування інформаційної безпеки. Таким чином, науковий аналіз ряду проблемних питань щодо розробки та втілення державної політики в межах інформаційної сфери сьогодні має особливе значення, адже їх розв'язання дасть змогу розвиватися суспільству, що має інформаційний характер, і у такий спосіб забезпечить національну та інформаційну безпеку України.

#### **БІБЛІОГРАФІЧНІ ПОСИЛАННЯ:**

1. Гнатцов О. Г. Інформаційні ресурси в системі забезпечення державної безпеки / О. Г. Гнатцов. – Режим доступу: <http://www.niisp.gov.ua/vydanna/panorama>
2. Дерекко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Н. Дерекко // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2. – С. 16-22.
3. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту / В. В. Домарев. – Режим доступу: <http://domarev.kiev.ua>
4. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби. – Режим доступу: <http://www.ngo.dn.ua/doc/concept.doc>
5. Інформаційна потужність держави, як складова національної безпеки. – Режим доступу: <http://propolis.com.ua>
6. Концепція інформаційної безпеки держав-учасників Співдружності Незалежних Держав у військовій сфері. – Режим доступу: <http://www.ngo.dn.ua>
7. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О. Л. Морозов. – Режим доступу: <http://www.viche.info>
8. Про Концепцію Національної програми інформатизації. Закону України від 4 лютого 1998 р. № 75/98-ВР // Відомості Верховної Ради. – 1998. – № 27-28. – С. 182.
9. Про національну безпеку України Закон України від 21.06.2018 № 2469-VIII // Відомості Верховної Ради. – 2018. – № 31. – Ст. 241.
10. Соснін О. В. Інформаційна політика України: проблеми розбудови / О. В. Соснін. – Режим доступу: <http://www.niisp.gov.ua/vydanna/panorama>

#### **REFERENCES**

1. Hnattsov, O.H. *Informatsiini resursy v systemi zabezpechennia derzhavnoi bezpeky* [Information resources in the system of state security]. Retrieved from: <http://www.niisp.gov.ua/vydanna/panorama> [in Ukrainian].
2. Dereko, V.N. (2015). *Teoretyko-metodolohichni zasady klasyfikatsii zahroz ob'ektam informatsiinoi bezpeky* [Theoretical and methodological principles of classification of threats to objects of information security]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, 2, 16-22 [in Ukrainian].
3. Domarev, V.V. *Bezpeka informatsiinykh tekhnolohii. Metodolohiia stvorennia system zakhystu* [Information technology security. Methodology for creating security systems]. Retrieved from: <http://domarev.kiev.ua> [in Ukrainian].



4. *Informatsiina bezpeka suspilstva i derzhavy. Stratehichni tsili i zadachi informatsiinoi borotby* [Information security of the society and the state. Strategic goals and objectives of information struggle]. Retrieved from: <http://www.ngo.dn.ua/doc/concept.doc> [in Ukrainian].
5. *Informatsiina potuzhnist derzhavy, yak skladova natsionalnoi bezpeky* [Information power of the state as a component of national security]. Retrieved from: <http://propolis.com.ua> [in Ukrainian].
6. *Kontseptsiiia informatsiinoi bezpeky derzhav-uchasnykiv Spivdruzhnosti Nezaleznykh Derzhav u viiskovii sferi* [The concept of information security of the states-members of the Commonwealth of Independent States in the military sphere]. Retrieved from: <http://www.ngo.dn.ua> [in Ukrainian].
7. Morozov, O.L. *Informatsiina bezpeka v umovakh suchasnoho stanu i perspektyv rozvytku derzhavnosti* [Information security in the conditions of the current state and prospects of statehood development]. Retrieved from: <http://www.viche.info> [in Ukrainian].
8. Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii Zakonu Ukrainy vid 4 liutoho 1998 r. № 75/98-VR [About the Concept of the National Program of Informatization]. (1998). *Vidomosti Verkhovnoi Rady*, 27-28, 182 [in Ukrainian].
9. Pro natsionalnu bezpeku Ukrainy Zakon Ukrainy vid 21.06.2018 № 2469-VIII [On National Security of Ukraine]. (2018). *Vidomosti Verkhovnoi Rady*, 31, 241 [in Ukrainian].
10. Sosnin, O.V. *Informatsiina polityka Ukrainy: problemy rozbudovy* [Information Policy of Ukraine: Problems of Building.]. Retrieved from: <http://www.niisp.gov.ua/vvdanna/panorama> [in Ukrainian].

**Турчак Анна Василівна**

Аспірант

Інститут підготовки кадрів державної служби  
зайнятості України  
03038, м. Київ, вул. Нововокзальна, 17.

**Turchak Anna**

PhD Student

Ukrainian State Employment Service Training  
Institute  
17, Novovokzalna Str., Kyiv, 03038, Ukraine

Email: [Avturchak@gmail.com](mailto:Avturchak@gmail.com)

Цитування: Турчак А. В. Основні складові інформаційної безпеки держави /А. В. Турчак// Аспекти публічного управління. – 2019. – Т. 7 – № 5. – С. 44-56

Citation: Turchak A.V. (2019). Osnovni skladovi informatsiinoi bezpeky derzhavy [Main composition of information security of the state]. *Public administration aspects*, 7 (5), 44-56

Стаття надійшла / Article arrived: 14.04.2019

Схвалено до друку / Accepted: 16.05.2019