

ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351.746:007

Є. О. Архипова

кандидат філософських наук,
доцент кафедри теорії та практики управління
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»

А. В. Черниченко

студент кафедри теорії та практики управління
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ ЯК НАГАЛЬНА ПОТРЕБА СЬОГОДЕННЯ

Стаття присвячена дослідженню інформаційної безпеки в органах державної влади. Підкреслена актуальність зазначеного питання в розрізі викликів сьогодення. Визначено місце інформаційної безпеки в структурі державної безпеки. Розглянуто загрози інформаційній безпеці в органах державної влади, окреслено шляхи їх подолання.

Ключові слова: інформаційна безпека, органи державної влади, загрози інформаційній безпеці, забезпечення інформаційної безпеки, відкритість та прозорість діяльності.

Постановка проблеми у загальному вигляді. Функціонування сучасного соціуму як у рамках окремої соціальної групи, держави чи в межах усього глобалізованого світу ґрунтується на використанні різноманітних інформаційних технологій, які забезпечують пошук, передачу, накопичення, аналіз та обробку інформації. Перехід до моделі електронного урядування, зокрема впровадження дедалі більшої кількості електронних послуг, вимагає від української держави посилення заходів, спрямованих на забезпечення інформаційної безпеки реальних чи потенційних користувачів цих послуг та державних органів. Попередження або мінімізація негативних наслідків від реалізації інформаційних загроз є важливим складником національної безпеки, тому забезпечення належного рівня інформаційної безпеки є для української

держави одним із пріоритетних завдань сьогодення. Водночас слід відзначити, що державні органи України через певні суб'єктивні та об'єктивні причини мають низку проблем у сфері забезпечення інформаційної безпеки.

Аналіз останніх досліджень та публікацій. Проблеми інформаційної безпеки та захисту інформації у своїх роботах висвітлюють Г. Почепцов, О. Литвиненко, О. Соснін, Є. Лук'янчиков, В. Остроухов та інші дослідники. Низка праць присвячена дослідженню інформаційної безпеки в контексті національної безпеки (наприклад, роботи В. Ліпкана, Б. Кормича, С. Домбровської, М. Дмитренка). Різні аспекти розвитку комунікативних механізмів органів державної влади та населення в контексті утвердження нової моделі державного управління вивчають О. Бажинова, Л. Лашкіна, Л. Пашко, Є. Рома-

ненко, С. Чукут, В. Юрченко. Питання інформаційного та технічного забезпечення державного управління досліджують такі автори, як: В. Брижко, М. Дітковська, О. Карпенко, Ю. Уманський. Зазначимо, що потреба ширшого та активнішого використання новітніх ІКТ у державному управлінні та публічному адмініструванні відзначається багатьма авторами, тоді як проблема інформаційної безпеки в органах державної влади залишається практично поза увагою сучасних науковців. З огляду на це метою статті є проблема забезпечення інформаційної безпеки в органах державної влади.

Виклад основного матеріалу статті. Інформаційна безпека нині є одним із ключових понять як у науковому дискурсі, так і в підприємстві, державному управлінні, політичній, економічній, військовій та соціальній сферах.

Світові тенденції засвідчують швидке зростання вагомості інформації у суспільстві та збільшення попиту на використання засобів її передачі та обробки – сучасних інформаційно-комунікаційних технологій (далі – ІКТ), а отже, значною мірою актуалізують питання інформаційної безпеки. Широке застосування ІКТ у всіх сферах людської діяльності є логічною вимогою інформаційно-орієнтованого глобалізованого соціуму, тому очевидною є потреба впроваджувати та розвивати передові ІКТ і в органах державної влади. Використання ІКТ державними відомствами та організаціями збільшує ефективність перебігу внутрішніх інформаційних процесів, зокрема тих, що забезпечують прийняття рішень, а також покращує процедури надання різноманітних послуг громадянам та юридичним особам, робить державну владу прозорішою та більш відкритою. Громадяни дедалі частіше виявляють бажання не лише отримувати інформацію, що поширюється органами державної влади та місцевого самоврядування, але й впливати на прийняття рішень, визначення пріоритетних напрямів розвитку, формування програми дій в межах компетенції цих органів [3]. Така активність громадян відображає необхідність впровадження ефективних та безпечних засобів комунікації, які зроблять можливим ведення повноцінного діалогу органів державної влади та суспільства.

З огляду на це забезпечення належної інформаційної безпеки органів державної влади посідає чільне місце у системі інформаційної безпеки особи, суспільства і держави, а отже, і у забезпеченні національної безпеки України

загалом. Перед українською державою стоїть важливе завдання – зайняття міцних позицій в інформаційній сфері, зокрема вихід на принципово новий рівень якості надання послуг із використанням інформаційних технологій.

Слід відзначити, що у забезпеченні інформаційної безпеки суспільства провідну роль виконує держава, що є одним з її головних обов'язків та пріоритетів, особливо, з огляду на складні суспільно-політичні обставини, що склалися в нашій країні останніми роками. Дослідники зазначають, що рівень розвитку та безпека інформаційного середовища є одними з найвагоміших факторів державної безпеки. Справді, такі складники інформаційної безпеки, як кібербезпека, безпека інформації та захист від деструктивних інформаційних впливів, справляють значний вплив на стан воєнної, соціальної, економічної, політичної, енергетичної, екологічної та інших елементів національної безпеки України. Розвиток національного інформаційного середовища має супроводжуватися захистом від реальних та потенційних інформаційних загроз, зокрема інформаційної агресії, маніпулювання індивідуальною та масовою свідомістю, підміни ціннісних орієнтирів тощо.

Забезпечення інформаційної безпеки є досить складним процесом, а дії державних органів можуть як підвищувати її рівень, так і зменшувати. Наприклад, розробка та реалізація програм, спрямованих на підвищення рівня інформаційної культури та критичного мислення населення, активне пропагування «свідомого» споживання інформації та дотримання принаймні елементарних норм інформаційної безпеки у повсякденному житті сприятиме підвищенню загального рівня інформаційної безпеки. І навпаки, невважені рішення державної влади в інформаційній сфері, не завжди високий рівень технічного забезпечення послуг, які мають надаватися державними установами та службами, недостатній рівень компетентності державних службовців на місцях тощо спроможне знизити рівень інформаційної безпеки громадян, суспільства та держави, а отже, і національної безпеки загалом. Та й самі органи державної влади можуть потерпати від ведення несприятливої інформаційної політики іншими суб'єктами інформаційних відносин, що дестабілізує управлінські процеси та спричиняє розбалансованість комунікацій між державою і громадськістю.

Залежно від причин виникнення дослідники [5] виділяють такі види інформаційних загроз у державі:

- небезпеки, що є результатом спланованих та усвідомлених дій державної влади з метою створення авторитарного та іншого режиму;
- загрози, що можуть виникати через діяльність еліти в інтересах тільки вузького кола осіб;
- небезпеки, що є наслідком надмірної закритості органів влади від громадськості;
- небезпеки, що є наслідком взаємодії державного апарату з представниками кримінальних кіл, яка призводить до проникнення кримінальних авторитетів до структур державної влади тощо.

Також доцільно зазначити, що головним завданням усіх заходів, які спрямовані на формування та підтримання на визначеному рівні інформаційної безпеки, є мінімізація загроз через такі фактори, як недостовірність, неповнота та несвоєчасність інформації, її отримання та поширення незаконним шляхом.

Проаналізувавши діяльність державних органів, виокремлюємо дії, що мають здійснюватися ними в сфері забезпечення інформаційної безпеки:

- забезпечення та охорона прав громадян в інформаційній сфері, що закріплені в Конституції, державних та міжнародних правових актах;
- розробка і реалізація державної інформаційної політики;
- розвиток та узгодження нормативно-правової бази у сфері інформаційної безпеки;
- формування і розвиток закладів та інституцій, сферою відповідальності яких є інформаційно-психологічна безпека;
- забезпечення інформаційного суверенітету України;
- захист державних таємниць.
- сприяння розвитку національного інформаційного простору [1; 2].

Отже, організація діяльності державних структур в інформаційній сфері – це процес, що ніколи не зупиняється, а головною його спрямованістю є розвиток нормативно-правової бази та організаційно-технічного складника. Забезпечення інформаційної безпеки – це вектор цілої програми для України, що має проводитись відповідно до норм міжнародного права та чинного законодавства.

Інформаційний простір України на державному рівні має бути сформований органами державної влади так, аби сприяти розвитку

та вдосконаленню інформаційно-аналітичних ресурсів для ефективного здійснення управлінської діяльності на всіх структурних рівнях, починаючи із загальнонаціонального та закінчуючи органами місцевого самоврядування.

В українському законодавстві окреслені контури системи забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня – Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів, інших відомчих нормативних актах.

Проте ми не можемо не погодитися з позицією С. Домбровської [7], що перманентний процес реорганізації державних органів унеможливорює нормальне їх функціонування, зокрема формування та реалізацію державної інформаційної політики. Несвоєчасна розробка інформаційних та інформаційно-комунікаційних систем, «доведення» та виправлення помилок у програмному забезпеченні вже на етапі його широкого використання, неузгодженість інформаційних систем різних відділів, органів та установ, відсутність багатофункціональних, інтегрованих в єдину інформаційну систему, захищених баз даних ускладнює роботу державних органів – це далеко не повний перелік специфічних проблем державних органів у сфері інформаційної безпеки. Недосконалість та нестача інформаційно-комунікаційного забезпечення, неприйняття змін та подекуди просто низький рівень комп'ютерної грамотності держслужбовців вимагає більших часових, фінансових та матеріальних витрат на обслуговування громадян і юридичних осіб, спричиняє різні конфліктні ситуації, зокрема між працівниками державних установ, ускладнює процес прийняття рішень на всіх рівнях.

Загрозу інформаційній безпеці суспільства несе незаконне приховування відкритої інформації, її несанкціонована модифікація та знищення, що може призвести до посилення корупції, економічних злочинів, маніпулювання свідомістю, нав'язування штучно створених образів з метою зміни суспільних настроїв, пріоритетів, цінностей тощо [3; 4; 6].

Протиправні втручання в кібернетичні системи державних органів призводять до блокування інформаційних ресурсів, несанкціонованих змін в управлінських процесах, порушення інформаційних прав та свобод громадян. Зокрема, можна виділити такі загрози інформаційній безпеці,

як розголошення персональних даних через випадкові або навмисні дії співробітників, підкуп чи шантаж їхніх родичів або інших наближених осіб, несанкціонований доступ до елементів державної системи обробки даних без або зі зміною структури її компонентів, зняття інформації з державних ліній зв'язку за допомогою спеціальної радіоперехоплюючої апаратури, модернізація програмного забезпечення тощо.

Висновки і пропозиції. Таким чином, забезпечення інформаційної безпеки в органах державної влади є важливим елементом забезпечення державної безпеки загалом. Ця діяльність є досить динамічним процесом, що ніколи не зупиняється.

З метою посилення рівня інформаційної безпеки в органах державної влади необхідно якісно підвищити захищеність вітчизняних мереж зв'язку та інформаційних ресурсів, насамперед тих, що використовують державні структури, прагнути виключити незаконне втручання в їх роботу, а також витік конфіденційної та персональної інформації. Так, потрібно мінімізувати використання іноземного програмного забезпечення та апаратури, сприяти підготовці вітчизняних фахівців у цій сфері. Розвиток вітчизняних технологій, техніки та інформаційних продуктів необхідно поєднувати зі стимулюванням їх використання держструктурами та приватними компаніями. Також необхідне розширення співпраці в сфері забезпечення міжнародної ІБ з глобальними та регіональними організаціями.

У процесі забезпечення інформаційної безпеки доцільною є взаємодія зі ЗМІ та імплементація основних принципів створення системи інформаційної безпеки відповідно до наявних

ресурсів. Крім того, з огляду на складну ситуацію на Сході України одним із надзвичайно важливих викликів українській державності є забезпечення переваги у медіа-інформаційному просторі, що також є одним зі складників інформаційної безпеки держави.

Список використаної літератури:

1. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. URL: <http://zakon5.rada.gov.ua/laws/show/47/2017>
2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 р. URL: <http://zakon.rada.gov.ua/laws/show/287/2015>
3. Архипова Є.О., Дмитренко Н.О. Ефективна комунікація між органами державної влади та громадськістю як умова розвитку демократичного суспільства. Інвестиції: практика та досвід. 2016. №1. С. 92–96.
4. Архипова Є.О. Механізми управління свідомістю людини в інформаційному суспільстві Мультиверсум. Філософський альманах / Гол. ред. В.В. Лях. Вип. 4(92). 2010. С. 3–13
5. Баранов А. Информационный суверенитет или информационная безопасность? Національна безпека і оборона. 2001. № 1. С. 70–76.
6. Дмитренко М. Проблеми інформаційної безпеки України. URL: <http://social-science.com.ua/article/807>
7. Домбровська С.М. Механізми забезпечення інформаційної безпеки як складника державної безпеки України. Зовнішня політика та національна безпека. URL: <http://www.kbuara.kharkov.ua/e-book/tpdu/2015-1/doc/5/01.pdf>

Архипова Е. А., Черныченко А. В. Обеспечение информационной безопасности в органах государственной власти как насущная потребность сегодня

Статья посвящена исследованию информационной безопасности в органах государственной власти. Подчеркнута актуальность данного вопроса в разрезе вызовов современности. Определено место информационной безопасности в государственной безопасности. Рассмотрены угрозы информационной безопасности в органах государственной власти, определены пути их преодоления.

Ключевые слова: *информационная безопасность, органы государственной власти, угрозы информационной безопасности, обеспечение информационной безопасности, открытость и прозрачность деятельности.*

Arkhylova Ye. O., Chernychenko A. V. Providing information security in public authorities as the general needs of today

The article is devoted to the study of information security in state authorities. The relevance of this issue in the context of present-day challenges is emphasized. The place of information security in the structure of state security is determined. The threats to information security in state authorities are considered, ways of overcoming them are outlined.

Key words: *information security, state authorities, threats to information security, information security, openness and transparency of activity.*