УДК 343.3

*ЧЕРНУХІН Ігор Олександрович*

# ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

**Постановка проблеми.** Перехід України до інформаційного суспільства зумовлює впровадження новітніх інформаційних технологій в усі сфери життя, зокрема державне управління. За останні 15 років застосування органами державної влади та місцевого самоврядування інформаційно-телекомунікаційних систем набуло вражаючих масштабів. Інформаційні системи використовуються для оброблення та зберігання статистичної, економічної, політичної, науково-технічної, екологічної інформації, підготовки відповідних документів, ведення баз даних та ін. Водночас автоматизації піддаються не лише процеси підготовки, обліку, передавання, зберігання документів, а й системи прийняття рішень.

Близько п’яти років спостерігається тенденція впровадження в органах місцевого самоврядування України новітніх систем електронного голосування, які передбачають фіксацію та оброблення результатів волевиявлення депутатів під час прийняття рішень. Оскільки системи переважно будуються з використанням поширених у світі операційних систем та засобів обчислювальної техніки, вони можуть стати об’єктом злочинних посягань зловмисників. Порушення штатної роботи систем електронного голосування зумовлює фальсифікацію результатів волевиявлення депутатів, що не сприятиме вирішенню загальнодержавних чи місцевих проблем соціально-економічного, екологічного характеру, справедливого розподілу ресурсів (земельні, водні, корисні копалини тощо) територіальних громад.

Ця проблема потребує проведення на державному рівні комплексу організаційних, правових, технічних заходів й варта поглибленого наукового дослідження.

**Аналіз останніх досліджень та публікацій** у сфері захисту інформації у системах електронного голосування свідчить про недостатнє дослідження цієї тематики. Більшість наукових доробків В.Бутузова, М.Галамби, А.Гуза, Г.Гулака, Д.Дубова, В.Зубарєва, В.Конах, С.Мельника, М.Ожевана, В.Хланя, В.Хлевицького, В.Шеломенцева, О. Юрченка із захисту інформації торкається питань забезпечення безпеки функціонування систем, в яких обробляється інформація з обмеженим доступом або захист якої визначений законом. Деякі праці О.Довганя, О.Єрменчука, В.Нідільніченко, П.Скурського торкаються тематики захисту інформаційних систем технологічного управління об’єктами промисловості, енергетики, транспорту (так званої “критичної інфраструктури”). Водночас на системному рівні питання захисту інформації у системах електронного голосування не вивчалися.

**Метою статті** є дослідження організаційно-правових аспектів захисту систем

електронного голосування представницьких органів України від несанкціонованого втручання, а завданнями – класифікація наявних в Україні систем електронного голосування, визначення загроз безпеці інформації, що в них циркулює, а також недоліків законодавства України у цій сфері, обґрунтування пропозицій щодо законодавчого регламентування захисту систем електронного голосування від злочинних посягань.

**Виклад основного матеріалу.** На сьогодні в Україні в представницьких владних органах створено та функціонує 47 систем електронного голосування, з них одна експлуатується у Верховній Раді, 46 – в органах місцевого самоврядування різних рівнів (1 – Верховної Ради АР Крим, 22 – обласних рад, 23 – міських рад). Залежно від виду кінцевого обладнання депутатів (засобів голосування) та інтерфейсу з'єднувальних ліній класифікуємо такі системи на три типи (див. рис. 1):

*Тип 1* – система традиційного голосування (руками) з використанням електронно-обчислювального засобу (засобів) для уведення, документування результатів волевиявлення та виведення їх на табло.

*Тип 2* – система електронного голосування, яка використовує як кінцеве обладнання пульти голосування з обмеженим набором функцій (кнопки "за", "проти", "утримався", "реєстрація") з їх апаратною реалізацією (унеможливлює зміну програми). У системах цього типу електронно-обчислювальний засіб (засоби) застосовуються для підрахунку, документування результатів волевиявлення та виведення їх на табло. Прикладом такої системи є система голосування Верховної Ради України "Рада-3".

*Тип 3* – система електронного голосування, яка використовує як кінцеве обладнання електронно-обчислювальні засоби (ПЕОМ, планшети, ноутбуки тощо). При цьому з'єднання кінцевого обладнання із сервером може здійснюватися за проводовою (тип 3а) чи радіотехнологією (тип 3б).

Аналізуючи таку типологію систем електронного голосування можливо виділити їх спільну особливість – обов'язкову наявність електронно-обчислювальної техніки (комп'ютерів), які використовують поширені у світі операційні системи Windows, Linux, Android. Уразливість таких систем до кібернетичних атак зумовлюють загрози інформації, що циркулює у системах електронного голосування, а саме:

– несанкціоноване зовнішнє втручання з інтернету (в разі підключення елементів системи голосування до глобальної мережі), що може призвести до блокування роботи системи чи модифікації (знищення) інформації в ній (для систем типу 1, 2, 3). Такі дії можуть бути спричинені проведенням кібератаки або в реальному масштабі часу, або внаслідок застосування шкідливого програмного забезпечення з настанням небезпечних наслідків через певний час. При цьому у системі типу 3б зовнішнє втручання можливо не лише до серверів, а й до кінцевого обладнання;

– інсайдерське втручання в роботу системи, що може бути спричинене насамперед неправомірними (некваліфікованими) діями обслуговуючого персоналу, зокрема неумисним зараженням серверів шкідливим програмним забезпеченням (для систем типу 1, 2, 3). Для систем типу 3 зберігається загроза зараження кінцевого обладнання для голосування шкідливим програмним забезпеченням самим користувачем (депутатом);

– несанкціонований доступ до кінцевого обладнання голосування з боку сторонніх осіб у разі його винесення депутатом із контрольованої зони (для систем типу 3б). Наприклад, в одній із обласних рад України кінцеве обладнання виконано на базі планшета, який завжди знаходиться в користувача;

– блокування роботи системи електронного голосування шляхом поставлення радіозавад на частоті обміну інформацією між елементами системи (для систем типу 3б).

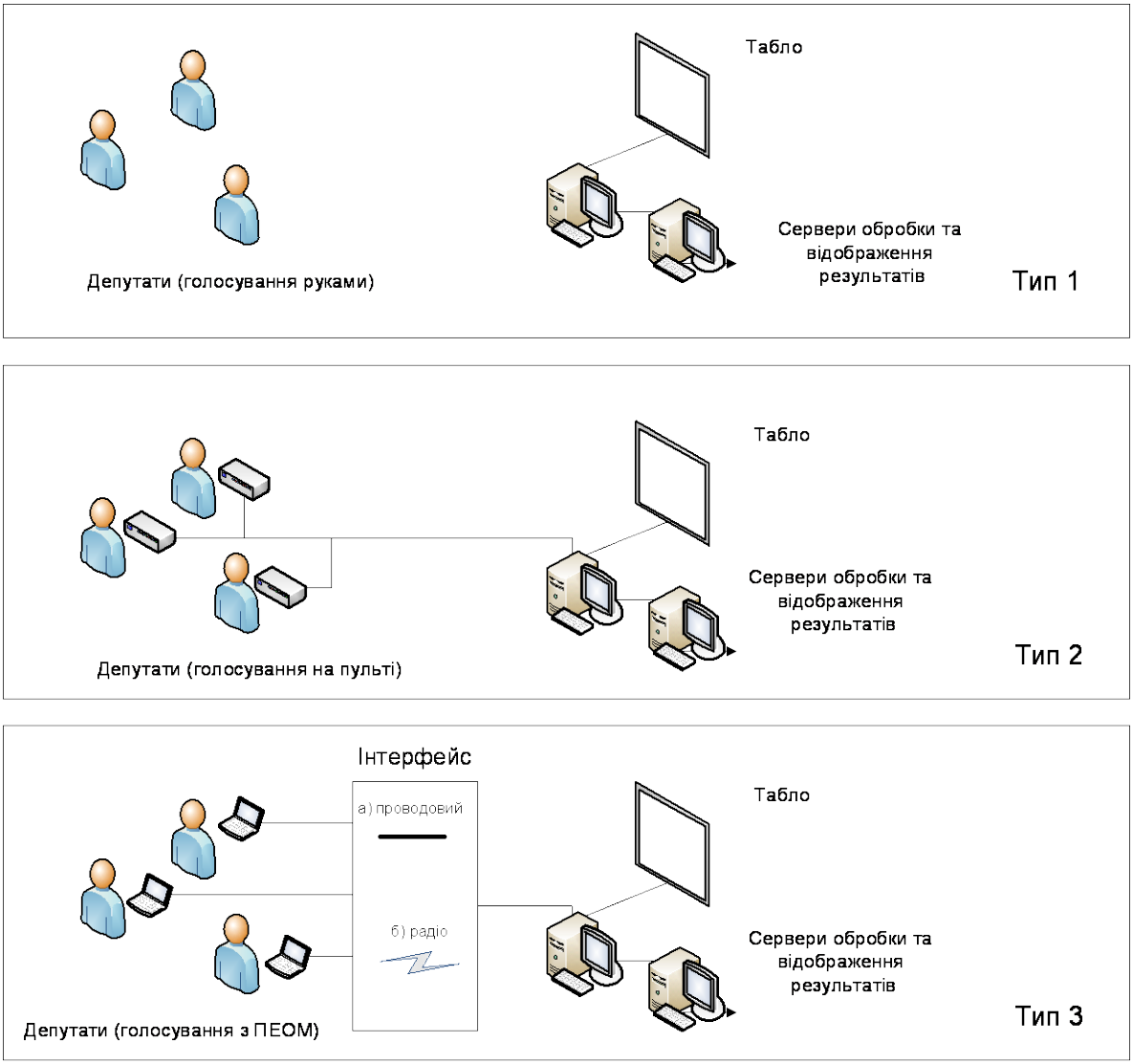


Рис. 1. Типи систем електронного голосування

Крім того, можливий несанкціонований витік інформації під час закритих засідань місцевих рад, проведення яких регламентовано статтею 46 Закону України "Про місцеве самоврядування в Україні" [1].

На нашу думку, наведені загрози свідчать про необхідність створення комплексів захисту інформації у системах електронного голосування. Враховуючи тотожність термінів "електронно-обчислювальна машина" ("комп'ютер") та "інформаційна система", що було досліджено в минулих працях [2], правові основи захисту інформації в системах електронного голосування доцільно досліджувати, спираючись на чинне законодавство України у цій сфері.

Так, відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах регулює Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [3]. Відповідно до статті 8 Закону обов'язковість створення комплексної системи захисту інформації в інформаційній системі визначається двома критеріями, а саме, якщо така інформація є: власністю держави; інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Серед наявних систем електронного голосування лише система "Рада-3", що функціонує у Верховній Раді України, є державною власністю (створена та експлуатується за рахунок коштів Державного бюджету України). Інші системи органів місцевого самоврядування (обласні та міські ради) створені та експлуатуються за рахунок коштів територіальних громад, а тому відповідно до статті 327 Цивільного кодексу України *мають комунальну форму власності* [4], тобто не відповідають першому критерію.

Для дослідження відповідності інформації, що циркулює у системах електронного голосування, другому критерію звернемось до визначеної законодавством класифікації інформації з обмеженим доступом. Так, відповідно до статті 21 Закону України "Про інформацію" інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [5].

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. З одного боку, органи місцевого самоврядування не належать до жодної з гілок влади України, з іншого – статтею 16 Закону України "Про місцеве самоврядування в Україні" органам місцевого самоврядування можуть надаватися окремі владні повноваження органів виконавчої влади. Крім того, такі повноваження, як затвердження місцевого бюджету, встановлення місцевих податків і зборів, управління комунальним майном [1], теж мають ознаки "владності". Тому інформація в системах електронного голосування не підпадає під статус конфіденційної.

Аналіз Зводу відомостей, що становить державну таємницю [6], свідчить, що така інформація також не є державною таємницею.

Установлення відповідності інформації в системі електронного голосування органу місцевого самоврядування статусу службової, на нашу думку, – питання дискусійне, яке потребує окремого наукового дослідження.

З одного боку, Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, визначає обов'язковий для всіх органів місцевого самоврядування порядок обліку, зберігання, використання й знищення документів, справ, видань, магнітних та інших матеріальних носіїв такої інформації [7].

З іншого – Переліки відомостей, які містять службову інформацію, затверджуються міністерствами, іншими центральними органами виконавчої влади, Радою Міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими держадміністраціями, тобто тільки органами виконавчої влади.

Зазначене свідчить про відсутність на законодавчому рівні механізму віднесення інформації в органах місцевого самоврядування до категорії службової. Таким чином, наразі керівники місцевих рад власним рішенням у будь-який час можуть включати/виключити інформацію з категорії службової та, як наслідок, ігнорувати заходи із захисту такої категорії інформації.

Крім того, Законом України "Про місцеве самоврядування в Україні", який визначає засади організації та діяльності органів місцевого самоврядування, інформація, що циркулює в системах електронного голосування, не визначена як інформація з обмеженим доступом, що потребує обов'язкового захисту [1].

Отже, на сьогодні в Україні *законодавчо не регламентовано віднесення даних*, що циркулюють у системах електронного голосування*, до інформації*, захист якої є обов'язковим. Хоча це необхідна умова створення комплексних систем захисту інформації.

Через відповідний юридичний статус на органи місцевого самоврядування не поширюються вимоги Кабінету Міністрів України щодо порядку захисту інформації в системах, обмеження підключення їх до глобальних мереж, взаємодії з Держспецзв'язком із питань захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

Відповідно до Порядку підключення до глобальних мереж передачі даних забороняється підключати до глобальних мереж інформаційні системи, на яких обробляється інфор-

мація з обмеженим доступом, що є об'єктом державної власності й охороняється згідно із законодавством [8]. Як було доведено вище, інформація, що циркулює в системах голосування місцевих рад, не має такого статусу. При цьому в п'яти органах місцевого самоврядування наявна можливість підключення систем електронного голосування до мережі Інтернет, що створює умови для ескалації вказаних кібернетичних загроз.

Крім того, відповідно до п. 3 Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах *органи виконавчої влади* оновлюють за рекомендаціями Держспецзв'язку антивірусні програмні засоби, які пройшли державну експертизу [9]. Така норма права не поширюється на органи місцевого самоврядування. Водночас у системах електронного голосування Верховної Ради АР Крим, шести обласних рад, чотирьох міських рад взагалі не встановлено антивірусні засоби. У більшості інших систем використовуються несертифіковані засоби антивірусного захисту, що в етіологічному аспекті створює загрозу штатному функціонуванню систем місцевих рад.

Проблему захисту інформації у системах електронного голосування слід розглядати не лише в правовому та технічному аспектах. Підроблення результатів голосування чинить безпосередній вплив на суспільно-політичну стабільність у регіоні чи державі та негативно позначається на міжнародному іміджі України.

Так, законодавча невизначеність обов'язковості захисту таких систем може використовуватись вітчизняними громадсько-політичними структурами, а також іноземними моніторинговими неурядовими організаціями для звинувачень влади у фальсифікаціях результатів голосування під час прийняття важливих рішень на місцевому рівні. У 2008 році виник конфлікт між депутатами Тернопільської обласної ради під час голосування за висловлення недовіри голові ОДА із звинуваченням місцевої влади в несанкціонованому втручанні в роботу системи електронного голосування "Віче" та фальсифікації результатів. Відповідні запити було направлено в правоохоронні органи [10]. Крім того, зазначений конфлікт викликав низку протестних заходів у Тернопільській області.

Вирішити порушену проблему можливо у двох напрямах: законодавчо регламентувати віднесення даних, що циркулюють в системах електронного голосування, до інформації, захист якої є обов'язковим; органам місцевого самоврядування віднести інформацію, що циркулює в системах електронного голосування, до категорії службової.

Утім, другий напрям убачаємо неефективним. По-перше, правова неврегульованість у законодавстві України механізму віднесення інформації в органах місцевого самоврядування до категорії службової робить проблематичною уніфікацію у всіх територіальних громадах процесу надання відомостям грифу обмеження доступу "для службового користування". Крім того, небажання, наприклад, керівника місцевої ради (в умовах обмеженого фінансування) спрямовувати кошти на захист інформації в системі практично нівелює необхідність забезпечення безпеки інформаційного обміну в системах електронного голосування.

**Висновки.** Проведене дослідження свідчить про відсутність обов'язкової норми законодавства щодо захисту інформації в системах електронного голосування органів місцевого самоврядування. Для вирішення порушеної проблеми пропонуємо внести зміни до Закону України "Про місцеве самоврядування в Україні" в частині визначення вимог обов'язкового вжиття заходів захисту інформації в системах електронного голосування органів місцевого самоврядування відповідно до законодавства України.

Така пропозиція є першочерговим та необхідними кроком, що сприятиме унеможливленню фальсифікації результатів голосування під час прийняття важливих рішень на місцевому рівні.

Крім того, була виявлена відсутність на законодавчому рівні механізму віднесення інформації в органах місцевого самоврядування до категорії службової, що потребує додаткового наукового опрацювання.

## Список використаних джерел

1. Закон України від 21 травня 1997 р. № 280/97-ВР "Про місцеве самоврядування в Україні" [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua

2. Чернухін І.О. Співвідношення понять, які визначають об'єкт посягання комп'ютерних злочинів / І.О.Чернухін // Інформаційна безпека людини, суспільства, держави. – 2012. - № 3 (10). – С. 64–70.

3. Закон України від 5 липня 1994 р. № 88/94-ВР "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

4. Цивільний кодекс України від 16 січня 2003 р. № 435-IV (в редакції від 5 липня 2012 р.) [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

5. Закон України від 2 жовтня 1992 року № 2657-XII "Про інформацію" [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

6. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12 серпня 2005 р. № 440 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

7. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затверджена постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

8. Порядок підключення до глобальних мереж передачі даних, затверджений постановою Кабінету Міністрів України від 12 квітня 2002 р. № 522 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

9. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, затверджений постановою Кабінету Міністрів України від 16 листопада 2002 року № 1772 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

10. Тернопільські депутати заявляють про фальсифікації при висловлюванні недовіри губернаторові [Електронний ресурс] // Коментарії. – Режим доступу : http://ua.comments.ua/politics/96054-Ternopilski_deputati_vid_NU.html.

***Аннотация:*** Проведена классификация систем электронного голосования органов местного самоуправления, проанализированы угрозы безопасности информации в таких системах, выявлены недостатки украинского законодательства в этой сфере. Разработаны предложения по законодательной регламентации защиты информации в системах электронного голосования.

***Ключевые слова:*** система электронного голосования, защита информации, информационная система.

***Abstract:*** The article classifies electronic voting systems of local authority, analyzes threats to information security in these systems; shortcomings of Ukrainian legislation in this sphere are revealed. Legislation proposals in order to regulate protection of information in electronic voting system are developed.

***Key words:*** electronic voting system, protection of information, information system.