УДК [167.7:004.056]:342.25
DOI https://doi.org/10.32840/1813-3401.2023.1.5

О. А. Галич
кандидат економічних наук, професор,
професор кафедри публічного управління та адміністрування
Полтавського державного аграрного університету

О. С. Демидкін
здобувач вищої освіти СВО Доктор філософії
Полтавського державного аграрного університету

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІСЦЕВИХ ОРГАНІВ ВЛАДИ

У статті визначено актуальність та необхідність захисту інформаційної інфраструктури функціонування органів місцевої влади, яка є ключовим інструментом прийняття обґрунтованих рішень розвитку територіальної громади, елементом е-урядування, способом патисипації громадян у взаємодії із зазначеними органами, контролю їх діяльності, засобом замовлення та отримання муніципальних послуг та складовою електронного документообігу.

Визначено, що із трансформаційними тенденціями цифровізації, інформатизації та автоматизації соціальних взаємин зростає роль та необхідність вдосконалення моделей забезпечення безпеки інформаційної системи місцевих органів влади. Зазначене й обумовлюється розвиненням видів та обсягів інформації обмеженого доступу, яка функціонує в інформаційній системі органів державної та місцевої влади, а також постійним зростанням груп загроз безпеці інформаційної системи органів місцевого самоврядування.

З метою формування ефективної системи захисту інформаційних систем органів місцевої влади запрпоновано використання сучасної моделі захисту, яка базуватиметься на концепції «defense-in-depth» та передбачатиме декілька рівнів захисту, що обумовлюють захист об'єктів інформаційної інфраструктури та захист суб'єктів (користувачів інформації) на основі убезпечення фізичного, технічного, програмного, адміністративного (включаючи рольовий) доступу та інших аспектах. Глибинний захист пропонований в цій моделі – це стратегія використання безлічі заходів безпеки для захисту цілісності інформації, яка призначена для охоплення всіх аспектів безпеки інформаційної інфраструктури органів влади, і передбачає алгоритм убезпечення від загроз таким чином, що якщо вони пройдуть одну «лінію» захисту, будуть використані додаткові рівні безпеки, щоб зупинити їх, що дозволяє усунути вразливості безпеки. Цінність ешелонованого захисту полягає в тому, що цей підхід об'єднує в собі передові інструменти безпеки, щоб захистити критично важливі дані та заблокувати загрози, перш ніж вони досягнуть кінцевих точок й мереж.

Охарактеризовано основні складові пропонованої захисту інформаційної системи органів місцевої влади на основі концепції «defense-in-depth» та розкрито особливості їх застосування.

Ключові слова: *адміністративний рівень захисту, ешелонований захист, інформаційний ресурс, концепція захисту «defense-in-depth», органи місцевого самоврядування, програмний й технічний захист, фізична безпека.*

Постановка проблеми. Умови розвитку сучасного суспільства вимагають практично повної інформаційної прозорості діяльності органів державної влади будь-якого рівня. За останні роки розроблено та прийнято безліч нормативно-правових актів, які забезпечують доступ громадян та організацій до інформаційних ресурсів органів влади, зокрема і органів місцевої влади, а також обов'язковості надання інформації посадовими особами [1; 2]. Водночас, органи державної влади також потребують великого обсягу інформації, необхідної для розробки та обґрунтування управлінських рішень, особливо це є актуальним для органів місцево-

го самоврядування, чиї рішення безпосередньо стосуються практично всіх сфер життєдіяльності громадян, у межах яких формуються великі масиви оперативної інформації, яка створюється як усередині органу місцевого самоврядування, так і у організаціях й домогосподарствах певної території.

Активізація процесів інформатизації суспільства, розвиток систем електронного документообігу, надання державних та муніципальних послуг в електронному вигляді сприяють тому, що зростає залежність органів місцевого самоврядування від використовуваної ними інформації, достовірності, якості, своєчасності її отримання. Водночас, значні масиви інформації вкрай уразливі для загроз несанкціонованого доступу до інформаційних та цифрових ресурсів, що призводить до зростання ризику й небезпеки несанкціонованих та ненавмисних впливів на інформаційну систему, і, як наслідок, виникають непередбачувані економічні та соціальні наслідки, пов'язані із порушеннями режимів безпеки інформації [3]. Власне зазначені аспекти і визначають актуальність дослідження питань захисту інформаційних систем місцевих органів самоврядування.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти, які стосуються забезпечення безпеки інформаційних систем місцевих органів влади, зокрема в умовах цифровізації, інформатизації та автоматизації соціальних взаємин висвітлені такими дослідниками як Дідик Н. І., Єременко С. А., Єсімова С. С., Ілюшик О. М., Малашко О. Є., Пархоменко-Куцевіл О. І., Терехова В., Торічного В. О., Усик С., Чмир Я. І. та іншими.

Мета статті. Головною метою цієї роботи визначення основних засад забезпечення безпеки інформаційних систем місцевих органів влади в умовах цифровізації, інформатизації та автоматизації соціальних взаємин та формування моделі забезпечення безпеки інформаційної системи місцевих органів влади.

Виклад основного матеріалу. За сучасних умов, необхідність підвищеної уваги до питань захисту інформації, цифрових та інформаційних ресурсів в органах місцевого самоврядування обумовлюються наступними факторами:

– залежність ефективної роботи адміністрацій районів від їх здатності забезпечити доступність, цілісність та своєчасність інформації;

– використання інформаційних систем, що обробляють великі обсяги відомостей різного ступеня важливості, а також уразливість даних систем від можливості несанкціонованого доступу, у тому числі й результаті ненавмисних дій, що спричиняють витік інформації;

– зростаюча кількість злочинів у інформаційній та цифровій сферах [3–5].

В свою чергу доцільно визначити види й типи інформації, яка функціонує в інформаційній системі органів місцевої влади і яку структур вона має відносно необхідності та рівня захисту (рис. 1).

Враховуючи наведенні види й типи інформації, яка функціонує в інформаційній системі органів місцевої влади, доцільно відзначити суттєву кількість видів, типів та відповідно обсягів інформації, яка повинна підлягати захисту та бути убезпечена від доступу зловмисників. З цією метою ідентифіковано загрози безпеки органів влади, у тому числі, загроз безпеки інформаційних систем державних органів місцевої влади, а також відповідний вибір та застосування ефективних засобів захисту від цих загроз, що може бути досягнуто лише за рахунок комплексного використання засобів захисту по кожному виду загроз. За спрямованістю загрози безпеки інформаційної системи органів місцевого самоврядування можна розподілити на 4 види (рис. 2).

На основі наведеного доцільно відзначити, що інформаційна система органів місцевої влади містить значні обсяги інформації, а відповідно до розвитку цифрового середовища та діджиталізації цивільних, адміністративних та інших соціальних відносин, повинна бути захищена, фізично, технічно, апаратно, програмно та адміністративно, що передбачає використання комплексного захисту інформаційної інфраструктури органів влади, зокрема й на локальному рівні.

Відтак, з метою формування ефективної системи захисту інформаційних систем органів місцевої влади пропонується використання сучасної моделі захисту, яка базуватиметься на концепції "defense-in-depth" та передбачатиме декілька рівнів захисту, що обумовлюють захист об'єктів інформаційної інфраструктури та захист суб'єктів (користувачів інформації) на основі убезпечення фізичного, технічного, програмного, адміністративного (включаючи рольовий) доступу та інших аспектах (рис. 3).

Зараз, в системах захисту інформації місцевих органів самоврядування, в більшості випадків, розгортається лише один рівень безпеки,

Рис. 1. Класифікація інформації в інформаційній системі органів місцевої влади відносно необхідності та рівня захисту

Сформовано на основі: [1; 2; 3; 5; 6; 7]

Рис. 2. Класифікація груп загроз безпеці інформаційної системи органів місцевого самоврядування

Сформовано на основі: [1; 3; 6; 9; 10; 11]

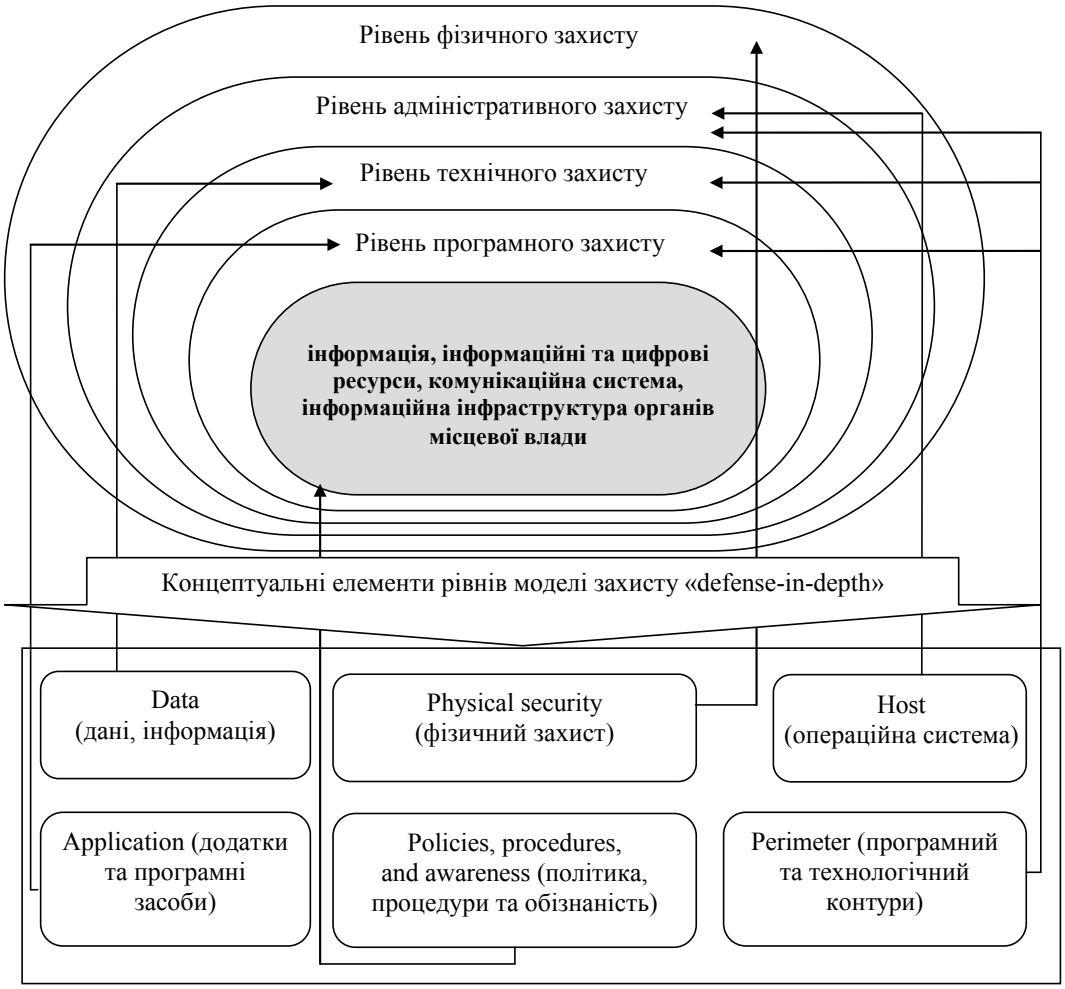

Рис. 3. Модель захисту інформаційної системи органів місцевої влади на основі концепції “defense-in-depth”

Авторська розробка

чого недостатньо для забезпечення загального захисту. Відтак, пропонована модель передбачає одночасне застосування декількох рівнів та методів захисту, що дозволить зменшити ймовірність витоку даних із інформаційної системи органів місцевої влади, поліпшити та забезпечити надійність комунікаційної системи, а також запобігти проміжним або футуристичним загрозам.

Глибинний захист пропонований в цій моделі – це стратегія використання безлічі заходів безпеки для захисту цілісності інформації, яка призначена для охоплення всіх аспектів безпеки інформаційної інфраструктури органів влади, і передбачає алгоритм убезпечення від загроз таким чином, що якщо вони пройдуть одну «лінію» захисту, будуть використані додаткові рівні безпеки, щоб зупинити їх, що дозволяє усунути вразливості безпеки, які неминуче несуть із собою технології, програмне забезпечення, користувачів інформаційної системи, їх операції в мережі тощо.

Цінність ешелонованого захисту полягає в тому, що цей підхід об'єднує в собі передові інструменти безпеки, щоб захистити критично важливі дані та заблокувати загрози, перш ніж вони досягнуть кінцевих точок й мереж.

Багаторівнева безпека – важлива частина стратегії ешелонованого захисту, а саме технічного контролю. Вона орієнтована на кібербезпеку та повний захист кінцевих точок й мереж. І хоча ешелонований захист визнає, що забезпечити повну безпеку неможливо, уповільнення загрози доти, доки вона не перестане становити небезпеку, є найефективнішим способом захисту інформаційних систем місцевих органів влади. Ешелонований захист пропонує вищий рівень безпеки він фокусується на адміністративному, фізичному, технічному та програмному контролі, здійснення якого необхідне для безпеки підприємств. Ці рівні забезпечують комплексність системи убезпечення інформації, інформаційних та цифрових ресурсів, комунікаційної

системи, інформаційної інфраструктури органів місцевої влади. Співвідношення окремих рівнів захисту та елементів цих рівнів відображено на рис. 4.

Відповідно до поданої моделі:

– фізичний контроль – це заходи безпеки, які захищають інформаційну систему органів місцевої влади від фізичної шкоди. До такого типу захисту може бути віднесено заходи щодо обмеження фізичного доступу до IT-інфраструктури не авторизованих осіб (фізичне охорона, системи СКУД, камери відео-спостереження, сигналізація, телекомунікаційні шафи із замками тощо);

– технічний контроль передбачає це методи захисту мережевих систем. Технічний контроль передбачає інформаційної системи органів місцевої влади захист апаратного і програмного забезпечення, а також мережевого рівня. Заходи з кібербезпеки, включно з багаторівневою безпекою, також належать до цієї категорії. До цього типу відносяться всі хардверні та софтові засоби захисту інформації, що дозволяють контролювати мережевий доступ до об'єктів інформаційної системи (міжмережевий екран, засоби антивірусного захисту робочих станцій, проксі-сервери, системи автентифікації та авторизації);

– програмний контроль – передбачає застування для захисту інформаційної системи спеціалізованих програмних засобів, які дають змогу захистити робочі станції, контролери та інформаційну систему в цілому через: ідентифікацію користувачів, контроль та розмежування доступу, шифрування інформації,- видалення залишкової (робочої) інформації, типу тимчасових файлів, тестового контролю системи захисту тощо. Переваги програмних засобів: універсальність, гнучкість, надійність, простота встановлення, здатність до модифікації та розвитку;

– адміністративний контроль – це політики й процедури, встановлені для працівників органів місцевої влади: документи покликані регулювати управління захистом, розподіл і обробку критичної інформації, використання програмних й технічних засобів, а також взаємодію співробітників з інформаційною сис-

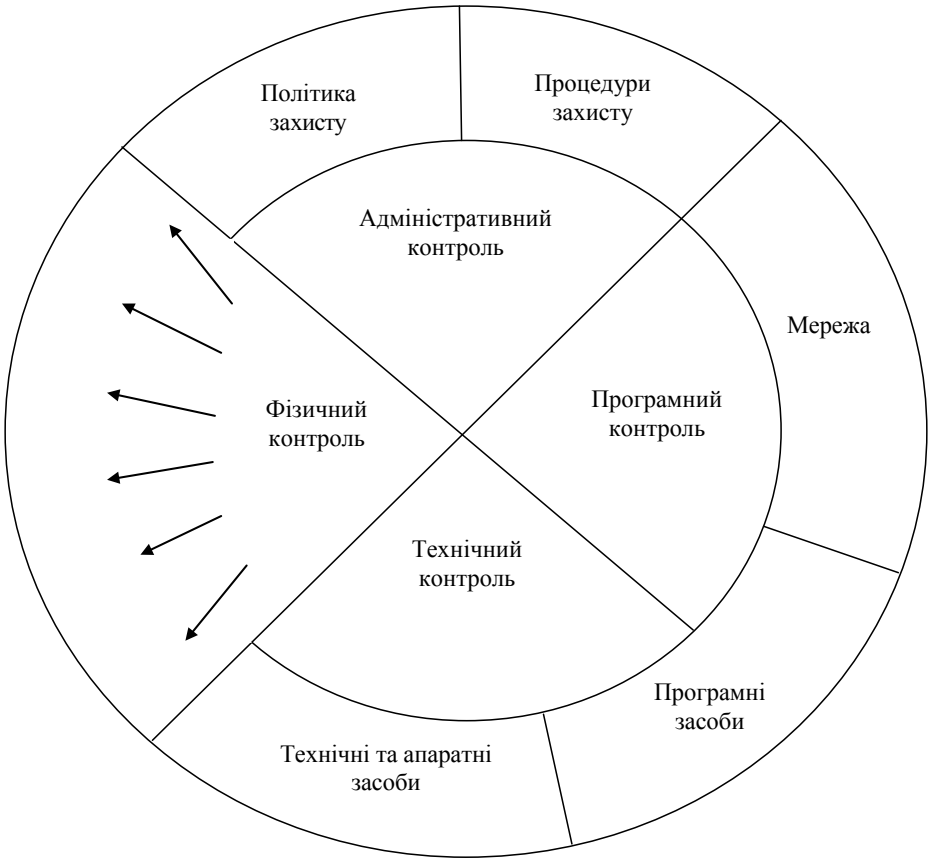

Рис. 4. Співвідношення окремих рівнів захисту та елементів моделі захисту інформаційної системи органів місцевої влади на основі концепції "defense-in-depth"

Удосконалено на основі [12]

темою, сторонніми організаціями та іншими зовнішніми суб'єктами). Прикладом адміністративного контролю є навчання працівників апарату місцевого самоврядування тому, як правильно позначати конфіденційну інформацію, і пояснення необхідності зберігання особистих файлів у відповідних папках [12].

Крім зазначених рівнів захисту, модель захисту інформаційної системи органів місцевої влади на основі концепції "defense-in-depth" передбачає застосування концептуальних елементів цих рівнів, серед яких:

– data – цей елемент рівня захисту забезпечує зберження даних із застосуванням різних технології шифрування з обов'язковим застосуванням access control list-ів з повним розмежуванням доступу користувачів до даних.

– application – елемент рівня захисту, який передбачає застосування програмних засобів, оновлених до найактуальніших версій й налаштованих таким чином, щоб не виникало «дірок» у інформаційній інфраструктурі з позиції software;

– host – розглядається операційна система, яка повинна містити найбільш актуальні версії та використовувати автентифікацію користувачів;

– internal network – на цьому рівні розглядається внутрішня мережа.з використанням захищених сегментів, сегментація мережі, використання шифрування всередині мережі;

– perimeter – передбачає обов'язкове використання FireWall. Доступ до сервісів ззовні строго обмежений, обмеження відбуваються ріхними access control листами, за допомогою суворого контролю відкриття/закриття портів, застосування ключових точок виведення інформацій та інформаційних ресурсів в «безпечну зону»;

– physical security – вбачає повний фізичний захист, коли сервери надійно фізично захищені й перебувають під «замком», наявність фізичної охорони, камер спостереження та різних технологічних засобів;

– policies, procedures, and awareness – на цьому рівні передбачається розроблення та затвердження політики й процедур. До цього рівня входять всілякі документи, що описують безпеку користувачів інформаційної системи органів місцевої влади, процедури, стандарти, а також навчання користувачів.

Основною метою пропонованої моделі захисту інформаційної системи органів місцевого самоврядування є запобігання реалізації загроз безпеці інформації шляхом:

– мінімізації ймовірності витоку, розкрадання, втрати, спотворення, підробки відомостей та блокування доступу до них;

– забезпечення правового режиму документованої інформації як об'єкта власності;

– захисту прав суб'єктів в інформаційних процесах при розробленні, виробництві та застосуванні інформаційних систем.

Відтак, зазначена модель захисту інформаційної системи органів місцевої влади на основі концепції "defense-in-depth", інформації ґрунтується на постійному та дієвому контролі її стану. Контроль стану системи захисту в органах місцевого самоврядування проводиться уповноваженими органами та полягає у перевірці відповідності системи вимогам безпеки, у періодичному контролі захищеності та в оцінці ефективності вжитих заходів щодо інформаційної безпеки.

Висновки і пропозиції. Отже, для убезпечення інформаційної інфраструктури функціонування системи органів місцевої влади, зокрема їх інформаційної системи, цифрових та інформаційних ресурсів, засобів та систем комунікацій потрібен лише комплексний підхід, який поєднуватиме належне керівництво (адміністративний рівень), використання сучасного програмного забезпечення та інформаційних технологій (програмний й технічний рівні), захист доступу до апаратних засобів (фізичний рівень) у поєднанні з зусиллями щодо переконання працівників у необхідності підвищення безпеки інформації (процедурний рівень), створення законодавства та контролю з боку держави за рівнем інформаційної безпеки (законодавчий рівень), та адаптація традиційних заходів – мережевих рішень, підвищення якості збору оперативної інформації, моделювання загроз, підвищення відповідальності розширюють межі «безпечного периметру» і створюють умови для ефективного та безпечного використання інформації в режимі реального часу.

Зазначене досягається шляхом використання пропонованої актуалізованої моделі захисту інформаційної системи органів місцевої влади на основі концепції "defense-in-depth", яка полягає у комплексному поєднані рівнів захисту та застосуванні різних методів, методик та засобів інформаційної безпеки задля ефективного функціонування системи місцевого самоврядування. Тому перспективним напрямом дослідження є формування механізму реалізації моделі захисту інформаційної системи органів місцевої влади на основі концепції "defense-in-depth".

Список використаної літератури:

1. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки : Указ Президента України від 27 вересня 2021 р. 487/2021. URL: https://zakon.rada.gov.ua/laws/show/487/2021#Text (дата звернення 20.12.2022 р.)
2. Стратегія інформаційної безпеки – 2025: що зміниться у сфері цифрових прав. 22 вересня 2021 р. URL: https://dslua.org/publications/stratehiia-informatsiynoi-bezpeky-2025-shcho-zminytsia-u-sferi-tsyfrovykh-prav/ (дата звернення 20.12.2022 р.)
3. Єременко С. А. Правові засади інформаційного забезпечення єдиної державної системи цивільного захисту України. *Інформація і право*. 2017. № 3(22). С. 117–123.
4. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного правління.* 2018. Том 6. № 9. С. 16–22.
5. Пархоменко-Куцевіл О. І. Інформаційна відкритість системи публічного управління як основа забезпечення національної безпеки. *Науковий вісник: Державне управління*. 2020. № 3(5). С. 195–203.
6. Єсімов С. С. Формування єдиного інформаційного простору в діяльності державних органів України. *Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки*. 2015. № 813. С. 48–53.
7. Ілюшик О. М., Дідик Н. І. Діяльність державних органів щодо забезпечення права особи на інформаційну безпеку. *Юридичний науковий електронний журнал.* 2021. № 12. С. 252–256.
8. Малашко О. Є., Єсімов С. С. Зміст державної діяльності із забезпечення інформаційної безпеки. *Міжнародний науковий журнал «Інтернаука».* 2020. № 15(95). Т.1. С. 46–54.
9. Терехов В. Удосконалення адміністративно-правового регулювання реалізації політики інформаційної безпеки в органах місцевого самоврядування. *Актуальні проблеми правознавства*. 2017. Вип. 1(9). С. 43–47.
10. Торічний В. О. Система інформаційного забезпечення державної безпеки України. *Державне будівництво.* 2020. № 1. URL: https://scholar.archive.org/work/iuz6ftwymvabvoo34dlra4duji/access/wayback/http://db.journal.kharkiv.ua/index.php/db/article/download/78/73 (дата звернення 23.12.2022 р.)
11. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник: Державне управління.* 2020. № 4(6). С. 266–280.
12. Defense-in-Depth. Imperva. URL: https://www.imperva.com/learn/application-security/defense-in-depth/ (дата звернення 17.12.2022 р.)

Halych O. A., Demydkin O. S. Model of ensuring information security system of the local authorities

The article defines the relevance and necessity of protecting the information infrastructure of local authorities, which is a key tool for making informed decisions on the development of a territorial community, an element of e-government, a way of citizen participation in interaction with these authorities, control of their activities, a means of ordering and receiving municipal services, and a component of electronic document management.

It was determined that with the transformational trends of digitalization, informatization and automation of social relations, the role and need to improve the models of ensuring the information security system of the local authorities is increasing. This was due to the development of the types and volumes of restricted information which operates in the information system of state and local authorities, as well as the constant growth of threat's groups to the security of the information system of local self-government bodies.

In order to form an effective system of information systems protection of local authorities, the author proposes to use a modern protection model based on the concept of "defense-in-depth" and providing for several levels of protection, which ensure the protection of information infrastructure objects and protection of subjects (information users) based on the security of physical, technical, software, administrative (including role-based) access and other aspects. The defense-in-depth proposed in this model like as a strategy of using multiple security measures to protect the integrity of information, which was designed to cover all aspects of the information infrastructure security of the authorities, and provides an algorithm for protecting against threats in such a way that if they pass one "line" of defense, additional levels of security will be used to stop them, which allows eliminating security vulnerabilities. The value of layered protection is that this approach combines advanced security tools to protect critical data and block threats before they reach endpoints and networks.

The author characterizes the main components of the proposed information system protection of local authorities based on the concept of "defense-in-depth" and reveals the peculiarities of their application.

Key words: *administrative level of protection, tiered protection, information resource, defense-in-depth concept, local government, software and hardware protection, physical security.*