КОМПЛЕКСНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНОМУ УПРАВЛІННІ

COMPREHENSIVE MODEL OF INFORMATION SECURITY IN PUBLIC ADMINISTRATION

УДК 351.86
DOI https://doi.org/10.32782/pma2663-5240-2024.39.45

Лисенко С.О.
д. юр. наук, професор,
директор Інституту безпеки,
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

Стаття присвячена дослідженню розробки комплексної моделі інформаційної безпеки в державному управлінні. Вона підкреслює важливість захисту конфіденційних урядових даних, забезпечення безперервності роботи та протидії зростаючим загрозам у дедалі більш оцифрованому середовищі. У цьому дослідженні розглядаються сильні та слабкі сторони різних моделей безпеки, включаючи вербальні, графічні, структурні та математичні підходи, які разом формують основу для захисту інформаційних систем державного управління. Інтегруючи ці моделі, державні організації можуть адаптувати стратегії безпеки, які ефективно управляють ризиками та відповідають різноманітним вимогам безпеки.

У дослідженні висвітлюються ключові класичні моделі безпеки, такі як модель Белла-ЛаПадули, дискреційний контроль доступу (ДКД) та п'ятивимірна модель Хартсона, які встановлюють структуровані підходи до контролю доступу та захисту даних. У статті обговорюється, як ці моделі надають важливу інформацію про контроль доступу, забезпечення конфіденційності та класифікацію взаємодії користувачів з даними на основі рівнів безпеки. Унікальна структура кожної моделі підтримує певний аспект безпеки державного сектору, від дозволів на доступ до багатовимірних оцінок доступу.

Досліджено обмеження статичних моделей доступу, таких як DAC, особливо в динамічних середовищах, а також проблеми, пов'язані з атаками троянських коней, які використовують гнучкі права доступу в традиційних моделях. Для вирішення цих проблем дослідження припускає, що моделі обов'язкового доступу, такі як Bell-LaPadula, можуть запропонувати більш суворий контроль і зменшити ризики, пов'язані з несанкціонованим доступом. Визнання обмежень існуючих моделей допомагає визначити сфери, де потрібні адаптивні рішення для задоволення вимог безпеки в сучасному державному управлінні.

Особливої уваги заслуговує детальне вивчення унікального внеску кожної моделі безпеки в побудову комплексної системи інформаційної безпеки для державного управління. Аналізуючи вербальні, графічні, структурні та математичні моделі, стаття показує, як кожен підхід слугує цільовим потребам безпеки - від спрощення складної інформації для нетехнічної аудиторії до надання точних, заснованих на даних оцінок ризиків. Цей багаторівневий інструментарій гарантує, що державна адміністрація може розробити адаптивну та ефективну стратегію безпеки, збалансувавши як високі політичні цілі, так і практичну імплементацію.

Ключові слова: *інформаційна безпека, державне управління, моделі безпеки, модель Белла-ЛаПадули, дискреційний контроль доступу, п'ятивимірна модель Хартсона, вербальні моделі, графічні моделі, структурні моделі, математичні моделі, кібербезпека, контроль доступу, захист даних, оцінка вразливості, адаптивна система безпеки, цифрове управління.*

The article is devoted to the study of the development of a comprehensive model of information security in public administration. It emphasizes the importance of protecting sensitive government data, ensuring business continuity, and countering growing threats in an increasingly digitized environment. This study examines the strengths and weaknesses of various security models, including verbal, graphical, structural, and mathematical approaches, which together form a framework for securing government information systems. By integrating these models, government organizations can tailor security strategies that effectively manage risks and meet diverse security requirements.The study highlights key classical security models, such as the Bell-LaPadula model, discretionary access control (DAC), and the five-dimensional Hartson model, which establish structured approaches to access control and data protection. The article discusses how these models provide important information about access control, privacy, and classification of user interactions with data based on security levels. The unique structure of each model supports a specific aspect of public sector security, from access authorizations to multidimensional access scores.The limitations of static access models, such as DAC, especially in dynamic environments, as well as the problems associated with Trojan horse attacks that exploit flexible access rights in traditional models are investigated. To address these issues, the study suggests that mandatory access models such as Bell-LaPadula can offer stricter control and reduce the risks associated with unauthorized access. Recognizing the limitations of existing models helps to identify areas where adaptive solutions are needed to meet the security requirements of modern public administration.A detailed study of the unique contribution of each security model to building a comprehensive information security system for public administration deserves special attention. By analyzing verbal, graphical, structural, and mathematical models, the article shows how each approach serves a targeted security need, from simplifying complex information for a non-technical audience to providing accurate, data-driven risk assessments. This multi-level toolkit ensures that public administration can develop an adaptive and effective security strategy, balancing both lofty policy goals and practical implementation.

Key words: *information security, public administration, security models, Bell-LaPadula model, discretionary access control, five-dimensional Hartson model, verbal models, graphical models, structural models, mathematical models, cybersecurity, access control, data protection, vulnerability assessment, adaptive security system, digital governance.*

Актуальність теми дослідження. Тема розробки комплексної моделі інформаційної безпеки в державному управлінні є надзвичайно актуальною через зростаючу цифровізацію урядових операцій та чутливий характер даних, з якими працюють державні установи. Оскільки державне управління розширює свою залежність від інформаційних систем, ризики кіберзагроз, несанкціонованого доступу та витоку даних зростають в геометричній прогресії. Моделі інформаційної безпеки забезпечують структуровану основу для захисту конфіденційних даних, забезпечення цілісності урядових процесів та підтримки довіри громадян.

Це дослідження розглядає ключові питання сучасного державного управління: необхідність збалансованого підходу, що поєднує як технічні, так і політичні заходи безпеки. Розглядаючи різні типи моделей безпеки - словесні, графічні, структурні та математичні - дослідження підкреслює необхідність використання різноманітних методів для ефективної протидії загрозам. Крім того, застосування класичних моделей, таких як Белла-ЛаПадула, в цьому контексті забезпечує суворий контроль доступу, тоді як моделі дискреційного та обов'язкового доступу допомагають адаптувати протоколи безпеки до динамічних середовищ.

У контексті державного управління, де дані повинні бути захищені в численних відомствах і на різних рівнях доступу, це дослідження є незамінним для побудови стійкої та адаптивної стратегії інформаційної безпеки. Вона не лише захищає національні інтереси, але й підтримує безперервність функціонування державних функцій, що робить її наріжним каменем сучасного, безпечного та прозорого врядування.

Метою дослідження є розробка комплексної моделі інформаційної безпеки, пристосованої для державного управління, з акцентом на захист конфіденційних урядових даних, забезпечення безперервності роботи та підвищення стійкості до кіберзагроз.

Аналіз останніх досліджень і публікацій. Нещодавні дослідження та публікації в галузі інформаційної безпеки та системного моделювання створюють фундаментальну основу для розуміння та впровадження комплексних систем безпеки в державному управлінні. Автори у тематичній літературі акцентують увагу не лише на теоретичних основах, але й на практичних застосуваннях, які підвищують адаптивність та надійність у динамічних середовищах (В. В. Остроухов, М. М. Присяжнюк, О. І., Фармагей, М. М., Чеховська, В. М. Дубового, Р. Н. Квітного, О. І. Михалєва, А. В. Усов, А. К. Видибіда, Р. В. Грищук, D. E. Bell, L. J. LaPadula, X. Jin, R. Krishnan, R. S. Sandhu, M. Sharon, J. W. Armitage, M. I. Kellner), проте автором розкрито більш широкий спектр застосування моделей з огляду на безпеку та її державно-управлінський аспект.**Основний зміст дослідження.** Для побудови стійкої системи інформаційної безпеки використовуються різні методи моделювання, які охоплюють різні аспекти управління безпекою. Кожна модель - вербальна, графічна, структурна та математична має унікальні переваги в передачі, аналізі та впровадженні заходів безпеки [1]. Ці моделі орієнтовані на різні аудиторії та цілі в державному управлінні, від спрощення концепцій безпеки для нетехнічного персоналу до використання підходів, заснованих на даних, для точної оцінки ризиків.

Словесні моделі, що складаються з усних і письмових описів, відіграють важливу роль у спрощенні складних систем безпеки, роблячи їх доступними для широкої аудиторії. Розбиваючи складні процеси безпеки на прості слова, словесні моделі дозволяють нетехнічним зацікавленим сторонам зрозуміти концепції, політики та процедури безпеки. Ці моделі особливо корисні, коли йдеться про протоколи безпеки для керівництва або персоналу без технічних знань.

У державному управлінні словесні моделі часто включаються в політичні документи або посібники для персоналу. Урядова установа може використовувати вербальну модель, щоб окреслити процедуру поводження з конфіденційною інформацією, чітко описуючи кожен крок, щоб працівники на всіх рівнях могли дотримуватися протоколу. Інший сценарій може передбачати усну презентацію, під час якої співробітник служби безпеки пояснює відділу найважливіші кроки для запобігання витоку даних, надаючи практичні, прості у виконанні вказівки.

Графічні моделі використовують візуальні представлення, такі як діаграми, карти та структурні схеми, щоб передати стратегії інформаційної безпеки. Візуальні інструменти полегшують розуміння складних систем, відображаючи взаємозв'язки, ієрархії та потоки даних в організації. Цей візуальний підхід може бути дуже ефективним для адміністраторів і технічних команд, яким потрібне чітке уявлення про інфраструктуру безпеки. Ще одне застосування графічних моделей - візуалізація ієрархії дозволів на доступ в організації. Ієрархічна діаграма може окреслити, які ролі мають доступ до певних даних, пояс-

нюючи, яким відділам або рівням персоналу надаються певні привілеї. Такий підхід не лише допомагає в навчанні, але й забезпечує швидкий довідник для аудиту безпеки та внутрішніх перевірок, гарантуючи, що дозволи на доступ відповідають політиці організації.

Структурні моделі використовують таблиці, діаграми та інші структуровані формати даних для порівняння та впорядкування протоколів інформаційної безпеки в різних відділах або підрозділах. Ці моделі пропонують систематичний спосіб перегляду та коригування політик безпеки, візуально представляючи відмінності та подібності в процедурах обробки даних.

Математичні моделі застосовують формули, рівняння і статистичні методи для вимірювання і прогнозування ризиків безпеки в інформаційних системах. Ці моделі дозволяють командам безпеки кількісно визначити вразливості та оцінити ймовірність різних загроз, забезпечуючи основу для прийняття рішень на основі даних. Інша математична модель може передбачати використання рівнянь для оцінки впливу різних протоколів безпеки, наприклад, порівняння ефективності двох алгоритмів шифрування на основі їхніх відповідних історій порушень і обчислювальних вимог. Ці моделі особливо корисні, коли ресурси обмежені, дозволяючи застосувати цілеспрямований підхід, який максимізує ефективність інвестицій в безпеку. На практиці математичні моделі можуть також підтримувати аналіз сценаріїв, коли адміністратори імітують потенційні порушення, щоб побачити, як різні політики безпеки можуть запобігти або зменшити шкоду, що в кінцевому підсумку допомагає розробляти надійні системи інформаційної безпеки.

Кожен тип моделей – словесні, графічні, структурні та математичні - відіграє унікальну роль у ландшафті інформаційної безпеки державного управління [2]. словесні моделі забезпечують доступність, роблячи принципи безпеки зрозумілими для всіх, тоді як графічні моделі надають візуальне уявлення про потоки даних та ієрархічні структури. Структурні моделі полегшують порівняння та організацію, допомагаючи узгодити практики безпеки в різних відомствах, а математичні моделі пропонують точні, підкріплені даними прогнози та оцінки, керуючи розподілом ресурсів і коригуванням політики. Разом ці моделі формують комплексний інструментарій, який підтримує як стратегічні, так і практичні аспекти зусиль органів державного управління з інформаційної безпеки.

Побудова надійної інформаційної моделі для державного управління передбачає структурований процес, який забезпечує врахування всіх аспектів безпеки даних. Кожен крок є важливим для створення моделі, яка точно відображає потреби та вразливості в контексті державного управління.Першим кроком у побудові інформаційної моделі є чітке визначення її мети. Це допомагає зосередити модель на вирішенні конкретних потреб і завдань у сфері безпеки. Завдяки встановленню чіткої мети модель слугує цілеспрямованим інструментом для вирішення критично важливих питань безпеки, забезпечуючи спрямування ресурсів у сфери найвищого ризику.Після визначення мети, наступним кроком є визначення ключових властивостей, які є критично важливими для досягнення цілей моделі. Ці властивості можуть включати такі фактори, як час реагування на загрози, типи даних, що захищаються, або конкретні протоколи безпеки. Зосередившись на цих властивостях, органи державного управління можуть краще зрозуміти, наскільки швидко вони можуть реагувати на потенційні порушення, і визначити сфери, які потребують вдосконалення. Такий підхід допомагає адаптувати модель до конкретних вразливостей, забезпечуючи реалістичне і дієве розуміння ландшафту безпеки.Після визначення критичних властивостей необхідно встановити взаємозв'язки між різними елементами безпеки в організації. Відображення цих взаємозв'язків допомагає з'ясувати, як різні компоненти взаємодіють і залежать один від одного, що має важливе значення для створення інтегрованого підходу до безпеки. Наприклад, у контексті державного управління модель може відображати залежності між департаментами, які мають спільний доступ до даних, визначаючи, які з них покладаються на інші для безпечної передачі даних. Розуміння цих залежностей має вирішальне значення для виявлення слабких ланок і забезпечення відповідності заходів безпеки кожного департаменту загальним цілям організації.Останній крок полягає у виборі найбільш підходящої форми представлення моделі. Обраний формат має відповідати меті моделі та цільовій аудиторії, щоб забезпечити її зрозумілість та зручність використання. Наприклад, якщо модель має на меті надати загальний огляд для нетехнічного персоналу, може підійти вербальна або графічна модель з використанням діаграм або чітких описів для передачі основної інформації без технічних подробиць. Однак, якщо модель призначена для використання ІТ-відділом, математична або структурна модель, наприклад, набір таблиць з детальним описом рівнів доступу та протоколів безпеки, може бути

більш доречною. Вибір правильної форми підвищує ефективність моделі, полегшуючи різним зацікавленим сторонам розуміння і застосування інформації про безпеку.За допомогою цих кроків - визначення мети, виявлення властивостей, встановлення взаємозв'язків і вибору відповідного формату - можна розробити всеосяжну та адаптовану модель інформаційної безпеки для державного управління [3]. Ця модель слугує практичним посібником, що допомагає установам усунути вразливості, вдосконалити стратегії реагування та впровадити узгоджені практики безпеки в усіх департаментах.Моделі безпеки в державному управлінні можна класифікувати за різними характеристиками, що дозволяє організаціям вибрати найбільш ефективну модель, виходячи з їхніх конкретних потреб у сфері безпеки. Класифікація за методом реалізації та характеристикою процесу забезпечує структурований підхід до розуміння та ефективного застосування цих моделей [4].Одним із способів класифікації моделей безпеки є метод їх реалізації, який визначає спосіб представлення та використання моделі. Абстрактні моделі покладаються на символічне представлення для передачі концепцій і протоколів безпеки без фізичних компонентів. Ці моделі часто використовуються у вигляді політичних документів, які описують принципи і правила, що регулюють інформаційну безпеку в організації [5].

Матеріальні моделі, навпаки, зосереджені на фізичному представленні заходів безпеки. Ці моделі застосовуються за допомогою матеріальних елементів, таких як апаратне забезпечення, фізичні макети або сценарії реальних користувачів. У державному управлінні матеріальна модель може передбачати використання захищеного обладнання для обмеження доступу до секретних зон або розгортання виділених серверів для захисту конфіденційної інформації. Змішані моделі поєднують як абстрактні, так і матеріальні елементи для створення комплексного підходу. Вони можуть включати як політичні настанови, так і симуляції для тестування заходів безпеки, забезпечуючи збалансований погляд на теоретичні та практичні аспекти. Таке поєднання гарантує, що теоретичні політики перевіряються в реальних сценаріях, що дозволяє вносити корективи на основі практичних висновків.Моделі безпеки також можна класифікувати за характеристиками процесу, зосереджуючись на тому, як вони реагують на різні типи подій безпеки. Детерміновані моделі використовуються для рутинних і передбачуваних процесів, де результати є послідовними за заданих умов [6]. Ці моделі корисні для таких завдань, як відстеження стандартних журналів доступу до даних або моніторинг регулярних оновлень системи, оскільки вони дозволяють застосовувати прості, засновані на правилах підходи. Стохастичні моделі, з іншого боку, призначені для роботи з непередбачуваністю, що робить їх придатними для подій, де на результати впливають випадкові змінні [7]. Ці моделі особливо ефективні для оцінки ризиків, пов'язаних з кіберзагрозами, системними збоями або неочікуваними простоями. У державному управлінні стохастичні моделі можуть використовуватися для оцінки ймовірності успішних спроб вторгнення, спираючись на історичні дані та аналіз ймовірностей. Класифікуючи моделі безпеки на основі методів реалізації та характеристик процесів, органи державного управління можуть вибрати найбільш підходящі моделі для своїх унікальних вимог. Незалежно від того, чи використовують символічні абстрактні моделі для розробки політики, матеріальні моделі для фізичної безпеки, чи змішані підходи для поєднання теорії з практикою, ця класифікація допомагає установам створювати індивідуальні стратегії безпеки, які відповідають як на передбачувані, так і на непередбачувані виклики. Класичні моделі безпеки вже давно стали основою стратегій інформаційної безпеки в державному управлінні, забезпечуючи структуровані підходи до захисту даних та контролю доступу. Серед найбільш поширених - модель Белла-ЛаПадули (BLM), модель дискреційного контролю доступу (DAC) та п'ятивимірна модель Хартсона, кожна з яких пропонує унікальні принципи та практичне застосування в інформаційній безпеці державного сектору.Модель Белла-ЛаПадули – це фундаментальна модель безпеки, яка зосереджена на збереженні конфіденційності даних у засекречених середовищах. Вона ґрунтується на двох основних правилах, які регулюють доступ користувачів на основі рівнів допуску. Перше, правило «не читати», забороняє користувачам з нижчими рівнями допуску доступ до даних вищого рівня, гарантуючи, що конфіденційна інформація залишається в межах дозволеного персоналу. Це правило має вирішальне значення в державному управлінні, де конфіденційні дані повинні бути розподілені між різними департаментами та посадовими особами. Друге правило, «не записувати», забороняє користувачам з високим допуском обмінюватися конфіденційними даними з користувачами з нижчим рівнем. Це запобігає несанкціонованому поширенню конфіденційної інформації, гарантуючи, що дані не «вите-

чуть» до користувачів, які не мають необхідного допуску [8]. Це правило не лише захищає інформацію, але й забезпечує підзвітність, оскільки обмежує доступ до даних з високим рівнем допуску певними рівнями доступу. Дискреційна модель управління доступом - це ще один важливий підхід, який широко використовується в державному управлінні. Вона забезпечує гнучкість, дозволяючи власникам даних вирішувати, хто може отримати доступ до певної інформації, що перебуває під їхнім контролем, на основі набору дозволів. У DAC правами доступу зазвичай керують за допомогою матриці, яка деталізує привілеї кожного користувача до різних наборів даних. Наприклад, керівник відділу може встановити права доступу, визначаючи, які співробітники можуть переглядати, редагувати або обмінюватися певними файлами в межах відділу [9]. Ця матриця корисна для розподілу прав доступу між різними ролями, гарантуючи, що кожен працівник має відповідний рівень доступу до даних, який відповідає його посаді. DAC особливо корисна в тих випадках, коли відділи мають справу з різними чутливими даними. Наприклад, у відділі охорони здоров'я адміністратори можуть дозволити певним членам команди доступ до записів пацієнтів, обмеживши цей привілей для інших. Такий контроль допомагає захистити конфіденційність, водночас забезпечуючи гнучкість на основі ролей та обов'язків кожного члена команди.П'ятивимірна модель Хартсона пропонує більш детальний підхід до контролю доступу, класифікуючи взаємодію користувачів з даними на основі п'яти вимірів: користувач, ресурс, операція, стан і авторизація. Ця модель ідеально підходить для державного управління, де багаторівневий доступ і детальний контроль є важливими для задоволення різноманітних потреб у сфері безпеки [10]. Поділяючи доступ на ці виміри, модель забезпечує всебічну оцінку кожної взаємодії між користувачами та ресурсами.Наприклад, в муніципальному управлінні модель може класифікувати доступ до фінансових записів на основі ролі користувача, типу ресурсу даних, дозволених операцій (наприклад, лише перегляд або редагування), стану ресурсу (архівний або активний) та рівня авторизації. Цей метод дозволяє адміністраторам встановлювати вузькоспецифічний контроль доступу, наприклад, обмежити права на редагування фінансових даних для старших фінансових працівників, надаючи молодшим співробітникам доступ лише для читання. Такий багаторівневий контроль допомагає запобігти несанкціонованим змінам і гарантує, що доступ кожного користувача точно відповідає його рівню авторизації та посадовим вимогам.Застосовуючи ці класичні моделі безпеки, органи державного управління можуть досягти надійного захисту даних, що відповідає різним потребам безпеки. Модель Белла-ЛаПадули забезпечує суворий ієрархічний контроль за секретною інформацією, DAC пропонує гнучкість завдяки дозволам, визначеним власником, а модель Хартсона забезпечує детальне, багатовимірне управління доступом. Разом ці моделі пропонують структурований підхід до захисту конфіденційних даних, що робить їх життєво важливими компонентами стійкої стратегії інформаційної безпеки органів державного управління.

Статичні моделі доступу, такі як модель дискреційного контролю доступу (DAC), часто стикаються з обмеженнями в середовищах, що вимагають частих і швидких змін рівнів доступу. У DAC дозволи на доступ встановлюються власниками даних і, як правило, залишаються статичними, якщо не оновлюються вручну, що ускладнює відстеження динамічних умов. Наприклад, п'ятивимірна модель Хартсона, хоча і є детальною, може зіткнутися з проблемами, коли часті зміни ролей користувачів або дозволів на основі проектів вимагають постійного оновлення. У великому державному управлінні, де працівники можуть виконувати тимчасові ролі або міжфункціональні завдання, ручне оновлення дозволів доступу щоразу може бути непрактичним і збільшувати ризик нагляду. Така статичність може призвести до затримок у відкликанні доступу для користувачів, яким він більше не потрібен, що створює потенційний ризик для безпеки, оскільки дозволи відстають від поточних потреб.Ще одним обмеженням систем DAC є їхня вразливість до атак «троянських коней», які використовують гнучкість передачі прав доступу. У DAC користувачі часто мають можливість передавати права доступу іншим користувачам без значних обмежень, що підвищує вразливість системи до несанкціонованого доступу або зловмисних дій. Така відкрита можливість передачі прав означає, що якщо програма-троянський кінь буде впроваджена авторизованим користувачем, вона може поширити права доступу на неавторизованих користувачів або програми, що призведе до витоку даних або внутрішніх загроз. Щоб зменшити ці ризики, моделі обов'язкового доступу, такі як модель Белла-ЛаПадули (BLM), пропонують суворіші обмеження, що не підлягають передачі, обмежуючи рух прав доступу між користувачами. У BLM дозволи на доступ фіксуються на основі дозволів без-

пеки і не можуть бути передані на розсуд користувача. Такий суворий контроль запобігає отриманню неавторизованими користувачами підвищеного доступу за допомогою атак «троянських коней», оскільки дозволи жорстко контролюються і не можуть бути змінені окремими користувачами. Ці обмеження статичних моделей доступу та вразливість до атак «троянських коней» ілюструють проблеми, з якими стикаються традиційні моделі безпеки при адаптації до сучасних, гнучких середовищ. Для вирішення цих проблем державне управління може скористатися гібридними моделями, які включають адаптивні елементи або динамічні налаштування доступу, що дозволяє краще реагувати на мінливі потреби в безпеці, зберігаючи при цьому надійний захист від внутрішніх і зовнішніх загроз.**Висновки та перспективи подальших досліджень.** Хоча класичні моделі безпеки, такі як модель Белла-ЛаПадули (BLM), дискреційний контроль доступу (DAC) і п'ятивимірна структура Хартсона, забезпечують фундаментальні структури для інформаційної безпеки державного управління, вони також виявляють обмеження, особливо в динамічних середовищах. Ці моделі пропонують критично важливе розуміння структурованого контролю доступу, дозволів на основі ролей і багатовимірної категоризації доступу, але проблеми залишаються, особливо щодо статичних дозволів і вразливості до атак «троянських коней». Адаптація цих моделей до вимог складних, мінливих середовищ підкреслює потребу в більш гнучких і оперативних підходах до безпеки.

Подальші дослідження полягають у розробці гібридних і адаптивних моделей безпеки, які поєднують суворий контроль обов'язкових рамок доступу з гнучкістю, необхідною для сучасних адміністративних середовищ. Майбутні дослідження можуть бути зосереджені на інтеграції машинного навчання для прогнозування і реагування на загрози в режимі реального часу, автоматизації коригування дозволів на основі ролей і поведінки користувачів. Крім того, вивчення систем контролю доступу на основі блокчейну може запропонувати децентралізовані, прозорі методи управління дозволами при збереженні суворих протоколів безпеки. Дослідження в цих сферах можуть призвести до створення більш стійких і адаптивних моделей, що узгоджуватимуть інформаційну безпеку з потребами державного управління, які постійно змінюються.

ЛІТЕРАТУРА:

1. Інформаційна безпека. Підручник. В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова К.: *Видавництво Ліра-К*, 2021. 412 с.

2. Моделювання та оптимізація систем: підручник /[Дубовой В. М., Квєтний Р. Н., Михальов О. І., А.В.Усов А. В.] Вінниця : *ПП «ТД«Еднльвейс»*, 2017. 26-30 с.

3. Sharon M. Four Stages of Building Information Modeling (BIM). *Medium*. URL: https://medium.com/@matt-sharon/four-stages-of-building-information-modeling-bim-d5fb2d448169

4. Classification algorithms: Definition and main models. *Data Science Courses. DataScientest*. URL: https://datascientest.com/en/classification-algorithms-definition-and-main-models

5. CISSP Study Guide: Information Security Models Cybrary. *Cybrary: Cybersecurity Courses & Cyber Security Training Online*. URL: https://www.cybrary.it/blog/information-security-models.

6 Armitage, J. W., Kellner, M. I., “A Conceptual Schema for Process Definitions and Models”, *Proc 3rd Int Conf Software Process (ICSP-3)*, 1994, *IEEE CS Press*.7. A.K. Vidybida. Stochastic models. Institute of Theoretical Physics of the National Academy of Sciences of Ukraine. n. *N.N. Bogolyubov* Kyiv, 2006. 204 p.

8. Bell D. E., LaPadula L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation (MTR2997 Rev. 1). *Bedford, Mass.: MITRE Corp.*, 1976. 129 p.

9. Jin X., Krishnan R., Sandhu R. S. A unified attribute-based access control model covering DAC, MAC and RBAC. *LNCS*. 2012. V. 7371. P. 41-55

10. Грищук, Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія. Житомир: *Рута*, 2010. 280 с.