УДК 004.056.5:005.934

Чаплик Олег Володимирович
(аспірант ПВНЗ «Європейський університет»)
ORCID: 0009-0009-8709-0355

Чаплик Тарас Володимирович
(аспірант ПВНЗ «Європейський університет»)
ORCID: 0009-0005-8247-8669

СИСТЕМНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ: КОНЦЕПЦІЇ, МОДЕЛІ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Анотація. *Стаття присвячена дослідженню системних засад управління інформаційною безпекою організації в умовах зростання цифрових загроз та підвищення вартості інформаційних активів. Обґрунтовано, що інформація з обмеженим доступом у сучасних організаціях стає не лише об'єктом технічного захисту, а й стратегічним ресурсом, який визначає стабільність, конкурентоспроможність і стійкість бізнес-моделі. У роботі проаналізовано концепції, моделі та організаційно-технологічні механізми побудови цілісної системи інформаційної безпеки, що інтегрує ризик-орієнтоване управління, цифрову ідентифікацію, моделі доступу, поведінковий моніторинг і превентивні методи контролю загроз. Особливу увагу зосереджено на проблематиці інформації з обмеженим доступом, структурі ризиків її витоку, сучасних підходах до моделювання загроз і формуванні корпоративної політики безпеки. Запропонована авторська таблиця систематизує механізми захисту конфіденційної інформації за моделями, функціями, ризиками та ефектами.*

Ключові слова: *інформаційна безпека, обмежений доступ, системне управління, моделі контролю доступу, цифрові ризики, корпоративна політика, кіберзагрози.*

Постановка проблеми. Управління інформаційною безпекою давно вийшло за межі технічних процедур і перетворилося на комплексну управлінську функцію, що охоплює стратегічне планування, організаційний дизайн, регламентацію процесів, поведінкові аспекти персоналу та цифрові технології. В умовах стрімкої цифровізації, зростання обсягів даних і появи високотехнологічних загроз проблема захисту інформації з обмеженим доступом набуває ключового значення. Саме ця категорія інформації виступає ядром управлінської стабільності: фінансові моделі, персональні дані, дані про клієнтів, інтелектуальна власність, внутрішні алгоритми та технічні рішення становлять основу конкурентних переваг організації.

Проблема полягає в тому, що більшість організацій, навіть маючи технічні інструменти безпеки, не мають цілісної системи управління, де технології, регламенти, людська поведінка, юридичні вимоги та корпоративні цінності формують єдину архітектуру захисту. Фрагментарність, відсутність політик, відсутність моделей ризиків, неузгодженість управління доступом, людські помилки та недостатня цифрова компетентність персоналу — усе це створює передумови для витоку конфіденційної інформації.

Аналіз останніх досліджень і публікацій. За останні роки значно зросла увага до проблематики інформаційної безпеки в управлінських системах. У працях зарубіжних дослідників (T. Sommestad, R. Anderson, L. Coles-Kemp) аналізуються питання взаємодії людини й технології у забезпеченні безпеки, а також поведінкові моделі ризиків. У рамках міжнародних стандартів — ISO/IEC 27001:2022, NIST SP 800-53 (2021) — визначено принципи ризик-орієнтованого управління інформаційною безпекою, моделі контролю доступу та вимоги до політик організацій. У роботах M. Gupta, B. Chen, N. Gruschka [2020–

2024] приділено увагу Zero Trust, класифікації цифрових загроз, проблемі внутрішніх зловживань та мультифакторної автентифікації.

Українські вчені активно досліджують інтегровані моделі інформаційної безпеки та управління ризиками у корпоративних системах. Зокрема, у працях О. Ілляшенко, В. Воронкової, І. Піддубного [2020–2023] підкреслено значення цифрових платформ у мінімізації ризиків, роль організаційних регламентів і важливість поєднання управлінського та технологічного підходів. Незважаючи на значний обсяг досліджень, питання системного управління інформацією з обмеженим доступом, її місця в архітектурі управління, системної класифікації механізмів захисту та оцінювання ефектів від їх застосування залишається недостатньо розробленим, що визначає актуальність даної статті.

Мета статті. Метою статті є обґрунтування концептуальних положень системного управління інформаційною безпекою організації, структуризація моделей та механізмів захисту інформації з обмеженим доступом і формування узагальненої таблиці механізмів, що поєднує моделі, функціональні завдання, ризики та ефекти їх застосування.

Виклад основного матеріалу дослідження. У сучасних організаціях інформаційна безпека все більше перетворюється на внутрішню філософію управління, а не на набір технічних правил. Усвідомлення того, що інформація з обмеженим доступом є ядром управлінської логіки, змінює підхід до ухвалення рішень і до самого розуміння загроз. Уже не йдеться про окремі інциденти чи випадкові атаки — цифрове середовище стає простором постійної напруги, у якому організація повинна поводитися не як пасивний об’єкт, а як активна система, здатна передбачати, реагувати, адаптуватися і накопичувати досвід. Саме ця еволюція вектора — від технічного захисту до системного управління — формує підґрунтя сучасної безпекової парадигми.

Зростання залежності від цифрових платформ, хмарних сервісів та мобільних робочих середовищ привело до того, що межі між внутрішнім і зовнішнім простором організації стають розмитими. Інформація рухається між системами, людьми, різними країнами, персональними пристроями, контрагентами, і все це створює нову складність. У таких умовах традиційна модель периметрової безпеки перестає працювати, а контроль доступу має будуватися на зовсім інших принципах — адаптивності, поведінкових особливостях, багатофакторній автентифікації та постійній перевірці довіри, що відображено у концепції Zero Trust [3].

Разом із тим саме людський фактор, а не технічні вразливості, залишається найбільшою точкою ризику. Дослідження ENISA та IBM засвідчують, що понад 70 % інцидентів пов’язані з людськими помилками, недбалим поводженням, неусвідомленим розкриттям інформації, ненавмисним порушенням політик або фішинговими атаками, на які співробітники реагують емоційно, а не раціонально [1; 8]. Це означає, що система захисту інформації з обмеженим доступом повинна враховувати психологічні, мотиваційні, поведінкові аспекти взаємодії працівника з інформацією. Розуміння того, як співробітники ухвалюють мікрорішення, які ризики вони не помічають, чому вони порушують процедури, чому користуються особистими пристроями для робочих операцій — усе це має стати частиною управлінської моделі безпеки.

Водночас цифрова складність породжує нову архітектуру інформаційних потоків. У більшості організацій конфіденційна інформація існує у різних формах: контрактні дані, фінансові прогнози, персональні відомості, технічні креслення, внутрішні алгоритми, записи переговорів, доступ до внутрішніх систем, інтелектуальні напрацювання. Кожен з цих елементів має власну логіку циркуляції, різні рівні доступу, різні ризики та різні сценарії несанкціонованого використання. Тому побудова єдиної системи захисту можлива лише тоді, коли організація правильно класифікує інформацію, визначить її чутливість і побудує взаємопов’язану систему обмежень.

Однак класифікація — лише один із кроків. Наступним елементом є правильна побудова моделі доступу, яка забезпечує рівновагу між безпекою та продуктивністю. У практиці багатьох організацій використовується комбінація класичних ролевих моделей (RBAC) та сучасних атрибутивних моделей (ABAC), де рішення про доступ ухвалюється на основі контексту: місця, пристрою, часу, поведінки, рівня ризику. Такий підхід дає змогу скоротити ймовірність внутрішніх зловживань і мінімізувати вплив ситуацій, коли облікові дані працівника можуть бути скомпрометовані. Досвід світових компаній засвідчує, що впровадження ABAC скорочує частку інцидентів, пов'язаних із надмірними правами користувачів, щонайменше на третину [4].

Ще одним ключовим елементом управління інформаційною безпекою є технологічний пласт, який доповнює організаційні рішення. Йдеться про системи контролю витоків (DLP), моніторинг подій безпеки (SIEM), поведінкову аналітику користувачів (UEBA), шифрування, сегментацію мереж, цифрові журнали аудиту. Кожна з цих технологій виконує свою мікрофункцію, однак їхня ефективність проявляється лише тоді, коли вони інтегровані у єдиний процес реагування та аналізу. Наприклад, DLP може виявити аномальну спробу копіювання файлів, SIEM — проаналізувати контекст, UEBA — оцінити поведінкові відхилення, а SOC — сформувати відповідне рішення. Усі ці механізми утворюють сучасний «цифровий контур безпеки», який працює в режимі реального часу.

Значну увагу в сучасних методиках приділяють побудові профілів ризику, які зосереджені саме на інформації з обмеженим доступом. На відміну від загальних кіберризиків, ризики конфіденційної інформації мають стратегічні наслідки: витік може вплинути на конкурентну стратегію, ринкову позицію, інноваційний потенціал та юридичну відповідальність підприємства. У міжнародних стандартах (ISO/IEC 27005:2022) пропонується формувати карти ризиків, де враховуються фактори критичності, імовірності, впливу на стейкхолдерів, відновлюваності та довгострокових наслідків. Проте в реальних умовах організації повинні також враховувати неформальні фактори — ступінь залежності від конкретних співробітників, корпоративну культуру, рівень довіри, внутрішні конфлікти, неформальні інформаційні практики.

Важливо наголосити, що інформаційна безпека — це не лише захист від зовнішніх загроз. Значна частина інцидентів виникає через внутрішні фактори: некоректне зберігання інформації, небезпечні робочі звички, використання незахищених каналів, передавання чутливих файлів у мессенджерах, робота з особистих пристроїв, несанкціоноване фотографування екранів, копіювання документів для «зручності». Саме поведінкова природа внутрішніх інцидентів вимагає побудови культури безпеки, де співробітники не просто знають правила, а розуміють їхній сенс.

Окремий аспект становить організаційна комунікація. У корпоративних середовищах інформація з обмеженим доступом часто передається горизонтально — між підрозділами, командами, проєктними групами, віддаленими працівниками. Це породжує нові виклики: розмивання відповідальності, різні інтерпретації політик, відсутність контролю за тим, як саме інформація циркулює всередині організації. Для системного управління необхідно створювати механізми фіксації рішень, централізованої класифікації документів, уніфікації форматів зберігання, контролю доступу до репозиторіїв і ведення історії взаємодій.

У контексті цифрової трансформації особливого значення набуває питання кіберстійкості. Йдеться не лише про захист від інцидентів, а про здатність організації відновлюватися, продовжувати роботу та зберігати дані навіть у разі серйозних збоїв. Концепція кіберстійкості (cyber resilience) передбачає безперервність операцій, наявність резервних копій, дублювання критичних систем, автоматизоване відновлення доступу, а також повноцінні сценарії реагування. Усе це має бути інтегровано у внутрішню політику щодо роботи з інформацією з обмеженим доступом, оскільки саме ця інформація найчастіше є критичною для відновлення діяльності.

Поряд із технологічними рішеннями дедалі важливішою стає етична складова. Багато сучасних організацій працюють із великими обсягами конфіденційних даних — персональних, бізнесових, стратегічних. Використання алгоритмів, поведінкової аналітики, цифрового моніторингу повинно відповідати вимогам законодавства, міжнародних стандартів, норм приватності та прав людини. Баланс між безпекою та приватністю стає ключовим аспектом корпоративної безпеки, особливо коли йдеться про дані співробітників.

Іншим важливим елементом є цифрова ідентичність. У сучасних організаціях ідентифікація та автентифікація користувачів перетворюється на окрему управлінську систему, яка охоплює життєвий цикл доступу: прийом працівника, зміна ролі, анулювання доступів, тимчасові дозволи, інтеграцію зовнішніх підрядників. Помилки в управлінні цифровими ідентичностями часто стають причиною витоків даних. Саме тому системи IAM (Identity and Access Management) і MFA (Multi-Factor Authentication) стають основою сучасної інфраструктури безпеки [7].

Загалом системне управління інформаційною безпекою — це гармонізація технологій, поведінки, організаційних процесів, політик і стратегічних рішень. Воно формує складний багаторівневий простір, у якому всі елементи повинні взаємодіяти синхронно. Порушення балансу в одному елементі — людському, технічному, організаційному чи процедурному — може призвести до руйнування всієї системи.

Управління інформацією з обмеженим доступом, зокрема, вимагає не лише технічних механізмів, а й концептуального цілісного бачення. Організація повинна знайти спосіб поєднати гнучкість роботи працівників із жорсткістю вимог безпеки; швидкість ухвалення рішень — із регламентованістю; свободу комунікацій — із контролем доступу; відкритість інновацій — із захистом внутрішніх активів. Цей баланс і є суттю системного підходу до управління інформаційною безпекою.

Узагальнюючи викладені положення, важливо показати, яким чином окремі елементи управління інформаційною безпекою формують цілісну систему, здатну забезпечувати захист інформації з обмеженим доступом у реальному часі та в умовах динамічних загроз. Оскільки взаємодія між стратегічними, організаційними, технологічними та операційними компонентами має нелінійний характер, доцільним є представлення їх у вигляді структурної моделі, що відображає логіку взаємозв'язків і послідовність реалізації безпекових механізмів у межах єдиного управлінського контуру. Саме така модель дає змогу не лише систематизувати ключові рівні захисту, а й підкреслити їх взаємну залежність і вплив на кінцеві результати – конфіденційність, цілісність, доступність та кіберстійкість.

Подана схема відображає поетапну побудову системи захисту інформації, у якій кожний рівень виконує власну функцію, але водночас формує єдину керовану архітектуру. Стратегічний рівень визначає політику безпеки, параметри класифікації інформації та базові принципи розмежування доступу. Організаційний рівень забезпечує людську та регламентну складову – рольові моделі, повноваження, культуру безпеки та механізми відповідальності. Технологічний рівень матеріалізує політику через цифрові засоби моніторингу, контролю та запобігання інцидентам. Операційний рівень реалізує практичне реагування на загрози, відновлення процесів і підтримання безперервності діяльності. Сукупно вони формують цільовий результат – досягнення ключових атрибутів захищеності та підвищення стійкості організації до сучасних цифрових ризиків.

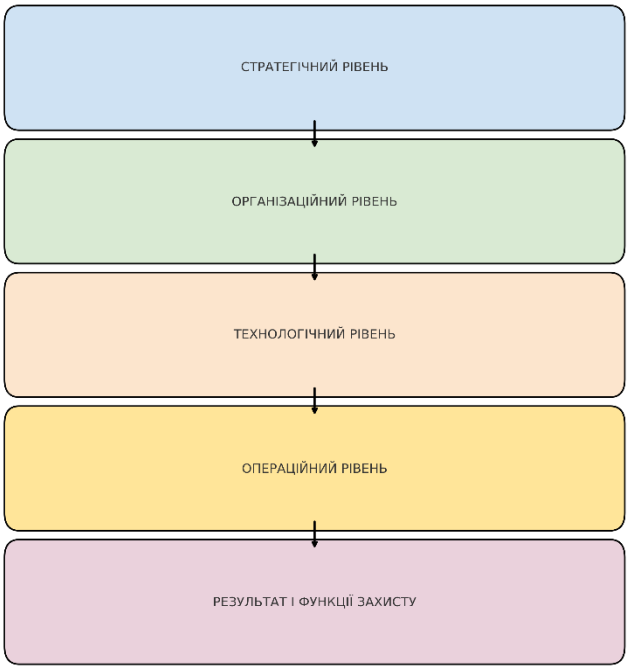

Рис.1. Системна модель управління інформаційною безпекою організації

Для розширення змісту представленої схеми та конкретизації функціонального наповнення окремих механізмів доцільним є систематичне порівняння доступних моделей захисту інформації з обмеженим доступом. Використання табличного формату дає змогу структуровано відобразити їхні призначення, базові можливості, типи ризиків, які вони мінімізують, а також потенційні обмеження та ефекти від їх впровадження. Такий підхід дозволяє краще зрозуміти комплексність управління конфіденційною інформацією та визначити, які механізми є найбільш доцільними в конкретних умовах організації.

Таблиця 1. Механізми захисту інформації з обмеженим доступом: моделі, функції, ризики, ефекти

Модель / механізм	Основна функція	Які ризики знижує	Потенційні ризики застосування	Ефекти для організації
ABAC / RBAC	Контроль доступу на основі ролей або атрибутів	Несанкціонований доступ, внутрішні зловживання	Неправильна конфігурація ролей	Зростання точності контролю
Zero Trust	Контекстна перевірка кожної дії	Компрометація облікових записів, lateral movement	Перевантаження системи автентифікації	Максимальна стійкість до вторгнень
DLP-системи	Запобігання витокам даних	Відправка конфіденційних файлів стороннім, копіювання	Фальшиві спрацьовування	Зменшення витоків
SIEM/SOC	Моніторинг і реагування на інциденти	Невиявлені загрози, затримки реагування	Надмірність даних	Безперервний контроль безпеки
MFA/IAM	Підтвердження особи	Крадіжка паролів	Складність для користувачів	Зниження рівня компрометації

Шифрування	Захист даних при передачі й зберіганні	Перехоплення, втручання в канали	Втрата ключів	Гарантія конфіденційності
UEBA	Поведінковий аналіз користувачів	Внутрішні загрози, аномалії	Хибні позитивні спрацьовування	Виявлення прихованих атак

Джерело: систематизовано автором на підставі [1,3,6]

Представлена таблиця демонструє, що ефективне управління інформацією з обмеженим доступом не може ґрунтуватися на використанні лише одного інструменту чи ізольованої моделі. Лише поєднання адаптивного контролю доступу, поведінкових технологій моніторингу, криптографічних методів, комплексного аналізу ризиків та організаційної регламентації забезпечує можливість формувати стійку до загроз систему. Важливою умовою результативності є також інтегрованість усіх механізмів у єдину управлінську логіку, що поєднує стратегічні наміри керівництва, цифрову культуру персоналу та технічні можливості інфраструктури. Саме така синергія створює підґрунтя для підвищення кіберстійкості, забезпечення конфіденційності даних і підтримання конкурентоспроможності організації в умовах зростання цифрових ризиків.

Висновки. Узагальнюючи результати дослідження, можна стверджувати, що формування ефективної системи управління інформаційною безпекою в сучасних організаціях потребує не фрагментарних рішень, а комплексного, багаторівневого підходу, у якому кожен елемент — від стратегічного планування до операційної реалізації — виконує власну незамінну функцію. Інформація з обмеженим доступом залишається найбільш чутливим і стратегічно вартісним активом, а отже, саме вона визначає логіку побудови системи захисту та характер управлінських рішень щодо ризиків, відповідальності та архітектури цифрового середовища.

Проведений аналіз показує, що сучасне бачення інформаційної безпеки не зводиться до технологічних засобів: навпаки, у центрі системи опиняється взаємодія стратегічних принципів, організаційної поведінки, цифрових інструментів і практик реагування на інциденти. Схема системної моделі демонструє, що саме синхронізація цих рівнів забезпечує здатність організації адаптуватися до загроз, запобігати їх розвитку та відновлювати функціонування після кризових ситуацій. Технологічні засоби ефективні лише в тому випадку, коли спираються на чітко визначені політики, адекватне розмежування ролей і сформовану культуру безпеки.

Аналіз механізмів захисту інформації з обмеженим доступом, систематизований у таблиці, підкреслює, що кожна модель має власні переваги й обмеження, однак значущих результатів можна досягти лише за умови їхнього комбінованого використання. Адаптивні моделі контролю доступу, багатофакторна автентифікація, поведінкова аналітика, DLP- та SIEM-рішення створюють різні рівні протидії загрозам, і саме їх скоординоване застосування формує реальну стійкість організації до внутрішніх і зовнішніх ризиків. Водночас людський фактор залишається критичним: без належної підготовки персоналу, відповідальності, усвідомлення ризиків та дотримання регламентів навіть найсучасніші технології не гарантують захищеності.

Отже, системне управління інформаційною безпекою має розглядатися як неперервний процес, орієнтований на випередження загроз і постійне вдосконалення внутрішніх механізмів. Організація, яка прагне зберегти стабільність, конкурентоспроможність і репутацію, повинна вибудовувати інтегровану модель безпеки, що поєднує стратегічне бачення керівництва, організаційну дисципліну, технологічну оснащеність та операційну готовність до реагування. Саме така модель забезпечує захист інформації з обмеженим доступом і створює основу для сталого функціонування організації в умовах цифрової невизначеності та зростаючої складності кіберзагроз.

ЛІТЕРАТУРА

1. IBM Security. Cost of a Data Breach Report 2023. IBM Corporation, 2023.
2. ISO/IEC 27001:2022 Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
3. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology, 2023.
4. Gruschka N., Mavroeidis V. Cybersecurity and Privacy in Modern IT Systems. *Journal of Cybersecurity*, 2021.
5. Gupta M., Sharman R. Handbook of Research on Information Security. IGI Global, 2021.
6. Ilyashenko S., Shypulina Y. Modern Approaches to Information Security Governance. *Marketing and Management of Innovations*, 2020.
7. Microsoft Security Team. Zero Trust Adoption Report 2022. Microsoft Corporation, 2022.
8. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2023. ENISA Publications, 2023.
9. Coles-Kemp L. Cybersecurity and Digital Behaviour: Human Dimensions of Digital Security. *Computers & Security*, 2022.
10. Mulligan D. Access Control Models in Digital Ecosystems. *Information Systems Journal*, 2021.

REFERENCES

1. IBM Security. (2023). *Cost of a Data Breach Report*. IBM Corporation.
2. ISO/IEC. (2022). *27001: Information Security Management Systems – Requirements*. International Organization for Standardization.
3. National Institute of Standards and Technology. (2023). *NIST Cybersecurity Framework 2.0*.
4. Gruschka, N., & Mavroeidis, V. (2021). Cybersecurity and privacy in modern IT systems. *Journal of Cybersecurity*.
5. Gupta, M., & Sharman, R. (2021). *Handbook of Research on Information Security*. IGI Global.
6. Ilyashenko, S., & Shypulina, Y. (2020). Modern approaches to information security governance. *Marketing and Management of Innovations*.
7. Microsoft Security. (2022). *Zero Trust Adoption Report*.
8. European Union Agency for Cybersecurity (ENISA). (2023). *Threat Landscape*.
9. Coles-Kemp, L. (2022). Cybersecurity and digital behaviour. *Computers & Security*.
10. Mulligan, D. (2021). Access control models in digital ecosystems. *Information Systems Journal*.

Chaplyk Oleh
(Postgraduate student of PVNZ "European University")
Chaplyk Taras
(Postgraduate student of PVNZ "European University")

SYSTEMIC MANAGEMENT OF ORGANIZATIONAL INFORMATION SECURITY: CONCEPTS, MODELS AND MECHANISMS FOR PROTECTING RESTRICTED INFORMATION

Abstract. *The article examines the systemic foundations of managing organizational information security in the context of escalating digital threats and the growing strategic value of information assets. It is substantiated that restricted information in modern organizations becomes not only an object of technical protection but also a strategic resource that determines the stability, competitiveness, and resilience of the business model. The study analyzes the concepts, models, and organizational-technological mechanisms for building an integrated information security system that incorporates risk-oriented management, digital identification, access control models, behavioral monitoring, and preventive threat-mitigation tools. Particular attention is given to the specifics of restricted information, the structure of risks associated with its leakage, contemporary approaches to threat modeling, and the development of corporate security policies. The proposed table systematizes mechanisms for protecting confidential information by models, functions, associated risks, and resulting security effects.*

Keywords: *information security, restricted access, systemic management, access control models, digital risks, corporate policy, cyber threats.*