DOI https://doi.org/10.36059/978-966-397-570-2-95

Кисельов В. Б.,
доктор технічних наук, професор,
професор кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Гуйда О. Г.,
кандидат наук з державного управління, професор,
завідувач кафедри комп'ютерних та інформаційних технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Омецинська Н. В.,
кандидат технічних наук, доцент,
завідувачка кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА: ПРИНЦИПИ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ

Інформаційна безпека розглядається як сукупність організаційних, технічних і програмних заходів, спрямованих на захист даних від несанкціонованого доступу, модифікації чи втрати [1]. Її ключова мета полягає у забезпеченні конфіденційності, цілісності та доступності інформації протягом усього життєвого циклу [2].

У сучасних інформаційних системах особливе значення мають такі підходи:

– Простота й прозорість архітектури – мінімізація складності дозволяє легше виявляти вразливості й проводити аудит.

– Розмежування прав доступу – користувачі повинні мати лише необхідний мінімум повноважень. Це знижує ризики при можливій компрометації.

– Контроль і аудит дій – усі операції, особливо з критичними ресурсами, мають бути зафіксовані в журналах подій для подальшого аналізу.

– Стійкість системи – наявність резервних механізмів, відмовостійкість і здатність до швидкого відновлення у випадку інцидентів.

Ці принципи особливо актуальні для розподілених та мікросервісних архітектур, де кожен компонент виконує обмежену функцію, а захист взаємодії між ними має бути чітко регламентований.

Важливим механізмом є *контроль доступу на основі ролей (RBAC) [3]*. У такій моделі система дозволяє виконувати лише ті дії, що передбачені для конкретної ролі, а всі інші – забороняються за замовчуванням. Наприклад, у сервісах перевезень лише водій може завершити поїздку, а клієнт – лише створити замовлення чи залишити відгук.

Коректна реалізація RBAC вимагає, щоб авторизація та перевірка повноважень були інтегровані в ядро системи, а не обмежувалися інтерфейсом. Недотримання цього принципу може призвести до порушення бізнес-логіки та фінансових збитків.

Логування та аудит

Журнали подій виконують функцію «цифрової історії» системи. Вони містять дані про активність користувачів, помилки, збої та підключення до ресурсів. Правильна організація логування дозволяє не лише відслідковувати інциденти, а й підвищувати підзвітність персоналу.

Найпоширенішими помилками є збереження у логах конфіденційних даних (паролів, токенів, результатів SQL-запитів). Це створює ризик витоку й компрометації системи. Для підвищення безпеки застосовуються такі практики:

– сегментація логів за критичністю;
– контроль доступу до журналів;
– дотримання законодавчих вимог, зокрема GDPR[4] та Закону України «Про захист персональних даних» [5];
– інтеграція з SIEM та SOAR-системами для автоматичного реагування на загрози [6].

Таким чином, аудит і логування виступають не лише допоміжними засобами, а повноцінним елементом системи безпеки.

Стійкість інформаційних систем

Стійкість означає здатність продовжувати роботу навіть у випадку атак або технічних збоїв. Основними її складовими є:

– відмовостійкість (резервні сервери, реплікація даних);
– толерантність до помилок (робота системи при виході з ладу окремих компонентів);
– резервне копіювання та відновлення;
– захист від кібератак (DDoS-захист, брандмауери, фільтрація трафіку);
– оперативний моніторинг та автоматичне переключення на резервні ресурси.

У разі фізичного пошкодження обладнання або зараження шкідливим ПЗ резервна інфраструктура дозволяє мінімізувати втрати та забезпечити безперервність критичних сервісів.

Сучасна інформаційна безпека ґрунтується на поєднанні контролю, аудиту та стійкості систем. Контроль забезпечує прозорість і відповідальність, аудит – можливість вчасно виявляти загрози, а стійкість –

безперервність функціонування навіть у кризових умовах. Їхня інтеграція формує основу довіри до цифрових систем і дозволяє ефективно протистояти сучасним кіберзагрозам.

Список використаних джерел:

1. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020. 1296 p. URL: https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3.pdf (дата звернення: 05.10.2025).
2. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT). БУДСТАНДАРТ Online – нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795 (дата звернення: 05.10.2025).
3. Що таке керування доступом на основі ролей (RBAC)? Визначення | Солікс. *Solix Technologies, Inc.* URL: https://www.solix.com/uk/kb/role-based-access-control/ (дата звернення: 05.10.2025).
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європ. Союзу від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 05.10.2025).
5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.10.2025).
6. Еволюція стратегій кібербезпеки: Роль SIEM та SOAR у захисті від сучасних загроз – SOFTICO.ua. *SOFTICO.ua – Компания Софтико*. URL: https://softico.ua/uk/knowledge/evolyutsiya-strategij-kiberbezpeki-rol-siem-ta-soar-u-zahisti-vid-suchasnih-zagroz/ (дата звернення: 05.10.2025).