Захист інформаційно-аналітичних систем в підрозділах Експертної служби Міністерства внутрішніх справ України

Юрій Обруч

Черкаський НДЕКЦ МВС України, м. Черкаси, Україна

Розвиток інформаційних технологій в Україні створює потребу у забезпеченні кіберзахисту, особливо в державних структурах. Інтеграція цифрових систем у діяльність МВС потребує ефективних заходів для запобігання витоку та спотворення інформації та контролю санкціонованого доступу.

Ключові слова: кіберзахист; кібербезпека; судова експертиза.

Protection of Information Analytical Systems in Subdivisions of the Expert Service of the Ministry of Internal Affairs of Ukraine

Yuriy Obruch

Advancement of information technologies in Ukraine necessitates cyber defense measures, particularly within governmental structures. Integrating digital systems into the activities of the Ministry of Internal Affairs requires effective measures to prevent information leakage and distortion, as well as to control authorized access.

Keywords: cyber defense; cyber security; forensic examination.

Останнім часом маємо значні досягнення в галузі інформаційних технологій, які стали глибоко інтегрованими в усі сфери суспільного життя. Зрозуміло, що розвиток цифрових технологій не залишився поза увагою зловмисників, які використовують різні методи втручання у роботу автоматизованих цифрових систем.

Інтеграція інформаційних технологій у бізнес-процеси Експертної служби Міністерства внутрішніх справ України відбувається швидкими темпами. З урахуванням посилення тенденцій реформування державних структур України, активне використання інформаційних технологій у експертній діяльності стає їх невід'ємною частиною. Неможливо проводити будь-які адміністративні дії своєчасно та правильно без доступу до різноманітної, актуальної та достовірної інформації, збирання та надання якої базується на сучасних спеціалізованих базах даних за допомогою відповідного програмного забезпечення.

Забезпечення функціонування та ефективного використання інформаційно-аналітичних систем неминуче викликає проблеми у забезпеченні належного рівня захисту інформації. Визначаючи інформаційно-аналітичну систему як комп'ютерну, що дає змогу отримувати, створювати, обробляти та аналізувати інформацію, важливо зауважити, що до таких систем може мати доступ не лише працівник підрозділу, а й зловмисник.

Безпека інформації та запобігання її витоку є складними питаннями, які вимагають виконання певного рекомендованого алгоритму та дотримання вимог і рекомендацій. Розглядаючи питання кіберзахисту, слід врахувати, що будь-яка інформаційно-аналітична система забезпечує єдиний інформаційний простір для підприємства (організації) і гарантує доступність інформації на всіх рівнях управління. Отже, у разі успішної кібератаки та отримання зловмисником несанкціонованого доступу до інформаційно-аналітичної системи, більша шкода завдається не витоком або знищенням інформації, а її спотворенням, що можна виявити лише пізніше і це матиме серйозні наслідки.

Кіберзахист — це систематичний підхід до захисту інформаційних систем від кіберзлочинів, що містить комплекс заходів технічного, організаційного та правового характеру, спрямованих на запобігання, виявлення та відновлення після кібератак. Цей підхід створює безпечне середовище для функціонування інформаційних систем та дає змогу забезпечити конфіденційність, цілісність і доступність даних [1].

На відміну від кіберзахисту, кібербезпека є ширшим поняттям, що охоплює всі аспекти безпеки в інформаційних і комунікаційних

технологіях. Крім захисту від кіберзлочинів, кібербезпека також містить заходи проти витоку інформації, зламу паролів, вірусів та інших загроз безпеці інформації. Це комплексний підхід, що враховує різноманітні аспекти та загрози для забезпечення безпеки в цифровому середовищі.

Основною метою кіберзахисту і кібербезпеки є забезпечення безпеки та надійності інформаційних систем. Обидва поняття важливі для сучасного суспільства, оскільки зростання кількість кіберзлочинів і загроз безпеці інформації ставлять під загрозу як інформаційну, так і національну безпеку. Головна проблема забезпечення кіберзахисту полягає у тому, що Експертна служба є установою, діяльність якої безпосередньо пов'язана з наданням послуг, що мають велике значення для функціонування суспільства та безпеки населення. Порушення функціонування служби може негативно вплинути на національну безпеку та оборону України. Отже, підрозділи Експертної служби є об'єктами критичної інфраструктури, а забезпечення інформаційної безпеки є фундаментом для забезпечення кіберзахисту країни взагалі.

Забезпечення кіберзахисту є складною проблемою, яка потребує врахування різних аспектів і вимог у сфері захисту інформації та інформаційних систем.

З погляду забезпечення інформаційної безпеки загалом та кібербезпеки зокрема, виникає необхідність у комплексних системах захисту інформації як злагодженої системи організаційних і технічних заходів, засобів і методів. Однак через зростання кількості атак на державні ресурси та успішних вторгнень, можна стверджувати, що такі комплексні системи захисту є недостатньо ефективними для забезпечення належного рівня кібербезпеки інформаційних і інформаційно-аналітичних систем. Забезпечення захисту інформації та контролю санкціонованого доступу має здійснюватися на етапі формування базового технічного завдання та на всіх етапах розроблення програмного забезпечення, а не лише на етапі інтеграції програмного засобу в бізнес-процеси підприємства або організації. Будь-який програмний засіб, що здатен самостійно контролювати та аналізувати дії користувача й реагувати на підозрілі ситуації, не потребує додаткових заходів.

На нашу думку, найефективнішим способом забезпечення захисту інформації та контролю за доступом є використання парадигми «Zero Trust», яка передбачає відсутність довіри до будь-яких даних і користувачів. Згідно з цією парадигмою, кожен раз, коли користувач звертається до системи, потрібно проводити повторну автентифікацію й авторизацію. Кожна спроба доступу до системи розглядається як потенційна загроза, доки не буде доведено протилежне [2, 3], що вимагає жорсткого фільтрування та перевірки всіх даних на адекватність та прийнятність.

Тому забезпечення захисту інформації в інформаційно-аналітичних системах МВС України має бути вбудованим у кожну систему, яка зберігає інформацію. Додаткові заходи (міжмережеві екрани, сканери потоків даних) можна вважати лише допоміжними, а не основними засобами захисту. Адже зазвичай кібератака — це складні заходи, ретельно сплановані для використання у вразливих системах. Якщо система не може виявити та відреагувати на такі події, ефективність заходів забезпечення кібербезпеки значно знижується.

Перелік джерел посилання

1. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua/articles (дата звернення: 01.03.2024).
2. Deogun D., Johnsson D. B., Sawano D. Secure By Design. 1st Ed. Manning, 2019. 410 p.
3. Garbis J., Chapman J. Zero Trust Security: An Enterprise Guide. Boston: Apress.