УДК 004.056:351.861

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОКОМУНІКАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ПРОФІЛІВ БЕЗПЕКИ

Любімов М.О.
e-mail: mykyta.liubimov@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

The study analyzes the modern approach introduced by the Cabinet of Ministers of Ukraine to system protection taking into account security profiles. Currently, three security profiles have been adopted - basic, industry and target. The study analyzes the purpose of these security profiles, analyzes the approach to forming a target security profile for information and communication systems taking into account the requirements of international standards for information security management.

На даний момент в Україні відбувається зміна підходів щодо побудови комплексних систем захисту інформації (КСЗІ). Так постановою Кабінету Міністрів України від 18 червня 2025 року № 712 [1] були затверджені «Порядок розробки та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» та «Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем». Попередній підхід передбачав атестацію КСЗІ, в якої фіксувався стан системи на момент перевірки та видався атестат терміном до 5 років. Оскільки загрози інформаційно-комунікаційним системам (ІКС) змінюються постійно, виникають нові вразливості в елементах ІКС. При цьому часто виникала ситуація, що КСЗІ ІКС через певний термін після її атестації не забезпечувала необхідний захист. В новому підході вводиться авторизація з безпеки систем, а також профілі безпеки системи. В новому підході реалізується процес управління ризиками інформаційної безпеки, впровадження механізмів захисту, які є достатніми для поточного рівня загроз. Ризик-орієнтований підхід означає, що повинні постійно оцінюватися ризики інформаційної безпеки при появі нових загроз, вразливостей, зміни бізнес-процесів. При виявленні невідповідності рівня залишкового ризика з прийнятним рівнем ризику здійснюється удосконалення системи захисту. Такий процес має бути безперервним.

Основою для ухвалення рішення про авторизацію є відповідність системи встановленим профілям безпеки. Профіль безпеки – це документ, який містить сукупність організаційних та технічних вимог до кіберзахисту. Введені наступні профілі безпеки – базовий, галузевий, цільовий.

Базовий профіль безпеки системи це мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється у системі, або функціонального призначення такої системи.

Галузевий профіль безпеки - це документ, який визначає типові вимоги до інформаційної безпеки для певної галузі або сфери діяльності (наприклад, для ІКС). Він описує, які загрози є характерними для галузі, які механізми захисту потрібно застосовувати і які вимоги до систем безпеки повинні виконуватися.

Цільовий профіль безпеки системи визначає сукупність заходів із захисту інформації з урахуванням базового та галузевого профілів до конкретної системи. Тут мають бути враховані вимоги нормативних документів для конкретної системи, призначення системи, процеси системи, структурно-функціональні характеристики системи.

Тобто базовий профіль безпеки використовується для введення типових механізмів захисту. Так перелік дій для базового профілю прийнятий наказом від 30.06.2025 р. № 409 Адміністрації Держспецзв'язку для систем, де обробляється відкрита та конфіденційна інформація [2].

Для ІКС галузевий профіль безпеки може вимагати сегментацію мережі, використання міжмережевих екранів та систем виявлення та запобігання вторгнень (IDS, IPS), використання VPN, шифрування трафіку, багатофакторну аутентифікацію, моніторинг аномальної активності та інші заходи. Вони мають бути типовими для будь-якої ІКС.

В дослідженні проводиться аналіз підходів формування цільового профілю для ІКС. Розглядаються практики, які представлені в міжнародних стандартах серії ISO/IEC 27000. Формування цільового профілю для ІКС представляється як набір взаємопов'язаних процесів з планування системи захисту, визначення критичних процесів і активів ІКС, оцінювання ризику інформаційної безпеки, вибору механізмів захисту, оцінювання якості системи захисту через процеси обробки інцидентів, аудиту, покращення системи захисту.

Список використаних джерел:

1. Постанова Кабінету Міністрів України від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем». URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text (дата звернення: 12.03.2026).

2. Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація, затверджений наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409. URL: https://cip.gov.ua/ua/news/bazovi-profili-bezpeki. (дата звернення: 11.03.2026).