УДК 004.056:[351.861:005.334]

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ПРИ ФОРМУВАННІ ЦІЛЬОВОГО ПРОФІЛЮ БЕЗПЕКИ ІНФОКОМУНІКАЦІЙНОЇ СИСТЕМИ

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 ways of implementing a risk-oriented approach to form a target security profile of an information and communication system. Based on the approaches of international standards, the procedure for implementing the risk management process is given, the final result of which is a formed target security profile. The study analyzes the content of each of the stages of risk management - identification, analysis, assessment, risk treatment.

Введення нових підходів до авторизації систем безпеки інформації (СБІ), запроваджених Постановою Кабінету Міністрів України від 18 червня 2025 року № 712, потребує необхідності розуміння їх практичної реалізації для захисту інфокомунікаційних систем (ІКС). Як показують брифінги та тренінги представників Держспецзв'язку [1] існує значне нерозуміння представниками організацій та установ процесів впровадження цих підходів. Також необхідно відмітити, що певні нормативні документи для реалізації цих підходів ще в стадії розробки.

Основою цих підходів є впровадження профілів безпеки – базового, галузевого, цільового. Базові профілі безпеки встановлюють мінімальні вимоги до будь-якої ІКС, залежать від типу інформації, що обробляється, призначенням системи, і розробляються Держспецзв'язком. Галузеві профілі безпеки розробляються відповідними міністерствами, іншими державними органами, і конкретизують вимоги для ІКС певної галузі. Цільовий профіль розробляється для конкретної організації – власника ІКС, враховуючі особливості її функціонування, основні та допоміжні процеси організації, її структури та критичних активів.

Цільовий профіль безпеки повинен забезпечити потрібний захист організації та її ІКС на відмову від базового та галузевого профілів, оскільки оперує не загальними вимогами безпеки базового профіля, і не загальними вимогами безпеки для певної галузі для галузевого профілю, а конкретними вимогами безпеки враховуючі специфічні загрози та вразливості для критичних процесів і активів цієї організації та її ІКС. Це обумовлюється застосовуванням ризик-орієнтованого підходу для формування цільового профілю безпеки.

Проведемо аналіз особливостей реалізації ризик-орієнтованого підходу для формування цільового профілю безпеки згідно з вимогами міжнародних стандартів (ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO 31010 та інші).

Послідовність дій при організації процесу управління ризиками має наступний вигляд.

1. Оцінювання внутрішнього і зовнішнього контексту організації (місія, бачення та цінності компанії, її основні і допоміжні процеси, політики та практики управління, бізнес-плани та стратегічні наміри компанії, наявні ресурси, призначення, структура та функціонування ІКС, внутрішня та зовнішня комунікація та інше).

2. Оцінювання області дії СБІ, тобто визначення, яка частина організації, які її процеси, які ІКС будуть охоплені системою безпеки інформації.

3. Формування реєстру критичних інформаційних активів організації. Інформаційні активи мають бути класифіковані за критичністю відповідно до впливу на процеси організації внаслідок втрати їх конфіденційності, цілісності та доступності. Це має відбуватися відповідно обраних категорій критичних активів (фінансові втрати, репутаційні втрати, загроза життю та здоров'ю людей та інші).

4. Визначаються критерії оцінювання ризиків і критерії прийнятності ризику. Обирається методика оцінювання ризиків.

5. Здійснюється процес ідентифікації ризиків (risk identification), при якому відбувається пошук, розпізнавання та опис ризиків, які можуть завадити організації, її ІКС досягти її цілей, призвести до порушення безпеки інформації, яка циркулює в організації і ІКС.

6. Здійснюється процес аналізу визначених ризиків (risk analysis), при якому відбувається детальний розгляд невизначеностей, джерел ризику, наслідків, ймовірностей, подій, сценаріїв, засобів захисту (контролю) та їх ефективності. На даному етапі враховуються ті засоби захисту, які були передбачені базовим та галузевим профілями безпеки.

7. Здійснюється оцінювання визначених ризиків (risk evaluation), яке передбачає порівняння результатів аналізу ризику зі встановленими критеріями ризику, щоб визначити, де потрібні додаткові дії. Також здійснюється пріоритизація ризиків, яка дозволяє визначити порядок дій по обробці ризиків.

8. Здійснюється обробка ризику (risk treatment) при якому є вибір і реалізація варіантів вирішення ризику. На цьому етапі формується цільовий профіль безпеки, обираються механізми захисту, які дозволяють знизити ризики до прийнятного рівня.

Список використаних джерел:

1. Стан та концепція розвитку сфер захисту інформації та кіберзахисту. Воркшоп Держспецзв'язку. 2026. URL: https://www.youtube.com/watch?v=pQFPl-JYSkE. (дата звернення: 21.03.2026).