УДК 004.056

Костерев Д. С., ст. наук. спів.
Шельвестер В.Я., начальник факультету
Житомирський військовий інститут імені С. П. Корольова

РОЛЬ ОЦІНКИ РИЗИКІВ У СИСТЕМІ АВТОРИЗАЦІЇ З БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ КЛАСУ "3", ДЕ ОБРОБЛЯЄТЬСЯ ІНФОРМАЦІЯ, ЩО СТАНОВИТЬ ДЕРЖАВНУ ТАЄМНИЦЮ

Забезпечення надійного захисту інформації в умовах сьогодення є одним із найбільш пріоритетних завдань держави, зокрема, коли йдеться про автоматизовані системи класу "3", в яких обробляється інформація, що становить державну таємницю. З ухваленням Постанови Кабінету Міністрів України № 712 від 18 червня 2025 року (далі - Постанова № 712) [1], парадигма технічного захисту інформації в Україні зазнала докорінних трансформацій. На зміну класичним, статичним комплексним системам захисту інформації (КСЗІ), які раніше проходили одноразову державну експертизу та отримували атестат відповідності на тривалий термін, прийшла гнучка, динамічна та безперервна система авторизації з безпеки. У цій архітектурі управління кіберзахистом оцінка ризиків перестала бути одним із формальних етапів передпроєктного обстеження і повернулася на новий фундамент, системо утворююча основа, яка створює весь життєвий цикл безпеки системи [2].

Роль оцінки ризиків у системі авторизації передусім виникає в тому, що вона є абсолютно обов'язковим аналітичним базисом для будь-якого проектування заходів захисту, без якого подальші процедури неможливі. В автоматизованих системах класу "3", які відзначаються високим рівнем розподільності, наявністю віддалених вузлів та підвищеними вимогами до конфіденційності й цілісності інформації, досягти абсолютної технічної безпеки на всіх безперервних рівнях практично неможливо. Саме тому оцінка ризиків дозволяє власникам (розпорядникам) автоматизованих систем стратегічно зосередитися на ідентифікації та захисті найбільш критично важливих компонентів системи, формуючи математично та економічно обґрунтовану модель протидії актуальним загрозам [2]. Згідно з методологічними алгоритмами, цей процес забезпечує глибоку ідентифікацію вразливих систем, скрупульозний аналіз і ймовірність використання вразливих сучасних загроз, оцінювання отриманих руйнівних наслідків, обчислення вартості виконання атак зловмисника та порівняння її з вартістю впровадження ефективних контрзаходів.

Основне місце оцінки ризиків яскраво розкривається через механізм формування цільових профілів безпеки, який є основою нової системи

авторизації [1]. Відповідальність для створення повноцінної, стійкої до зламів системи захисту повністю покладається на власника або розпорядника системи, який зобов'язаний розробити індивідуалізований цільовий профіль безпеки. Формування цільового профілю забезпечується шляхом додавання до вимог базового або галузевого профілю додаткових, спеціальних заходів кіберзахисту, які обираються суворо на основі результатів глибокої внутрішньої оцінки ризиків.

Оцінка ризиків критично впливає на момент ухвалення юридичного рішення про авторизацію автоматизованої системи. Відповідно до встановлених законодавством вимог, надання авторизації можливо лише за одночасного безумовного виконання двох ключових умов: по-перше, впроваджені технічні та організаційні заходи кіберзахисту повинні бути визнані достатніми для протидії поточному рівню загрози; по-друге, що є надзвичайно важливим, усі залишкові ризики повинні бути достеменно ідентифіковані, оцінені та офіційно визнані прийнятими для власника інформації [3]. Якщо залишкові ризики, пов’язані з обробкою інформації, що становить державну таємницю в АС класу “3”, значно перевищують допустимі межі і не можуть бути технічно нейтралізованими існуючими заходами, система не пройде процедуру авторизації та не отримає законного дозволу на функціонування.

Таким чином, оцінка ризиків виступає єдиним легітимним інструментом для обґрунтування того, які саме криптографічні, апаратні, програмні чи організаційні рішення повинні бути застосовані в конкретних системах для нейтралізації загроз. Під час самої процедури авторизації уповноважені органи перевіряють систему на відповідність розробленому цільовому профілю, що робить повноту первинної оцінки ризиків визначальним фактором для успішного отримання статусу авторизованої системи.

Список використаних джерел

1. Постанова Кабінету Міністрів України від 18 червня 2025 року № 712 “Про затвердження Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем”.

2. ДСТУ ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.

3. BSI-Standard 200-3. IT-Grundschutz Methodology: Risk Analysis [Electronic resource] : Federal Office for Information Security. — Bonn : BSI, 2017. — 64 p.