Манжай Ірина Андріївна, *старший викладач кафедри інформаційних систем та технологій навчально-наукового інституту № 4 ХНУВС*

НОВИЙ НОРМАТИВНИЙ ПІДХІД ДО СТВОРЕННЯ СИСТЕМИ БЕЗПЕКИ ІНФОРМАЦІЇ

Протягом 2025 року нормативно-правове регулювання сфери безпеки інформації в Україні зазнало фундаментальної трансформації. Ключовим етапом став Закон України від 27 березня 2025 року № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який докорінно змінив підходи до захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Цей акт фактично скасував застарілу парадигму «паперової» безпеки, що була закладена в попередніх редакціях законодавства, і запровадив перехід до сучасної системи безпеки інформації.

На виконання Закону Кабінетом Міністрів України було прийнято та внесено зміни до низки постанов, зокрема № 373 від 29 березня 2006 року «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем» та № 712 від 18 червня 2025 року «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», що регламентують нові правила гри.

Роль Адміністрації Держспецзв'язку трансформувалася. Відтепер регулятор не бере безпосередньої участі у створенні кожної окремої системи чи проведенні експертиз кожної комплексної системи захисту інформації (КСЗІ). Натомість Адміністрація фокусується на формуванні базових профілів безпеки, розробці нормативних документів (НД ТЗІ) та веденні переліку авторизованих систем. Основною метою реформи є створення ризикоорієнтованої моделі, здатної забезпечити реальну стійкість держави в умовах постійних загроз.

Концепція КСЗІ остаточно поступилася місцем процедурам авторизації та сертифікації. Для забезпечення безперервності процесів встановлено такі часові межі перехідного періоду:

– системи з діючими атестатами КСЗІ продовжують функціонувати до закінчення терміну дії атестата або до завершення воєнного стану (плюс 6 місяців після його скасування), якщо не потребують модернізації;

– проєкти, розпочаті до 18.06.2025 відповідно до Постанови Кабінету міністрів України № 712, завершуються через державну експертизу, проте атестати будуть дійсними лише 12 місяців (граничний термін – 18.06.2026), після чого обов'язкова авторизація;

– для систем з державною таємницею атестати реєструються на 12 місяців з подальшим обов'язковим переходом на нові стандарти захисту;

– експериментальні проєкти, створені за процедурою декларування відповідно до Постанови Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проєкту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації», діють 3 роки з дати декларації. Сама постанова № 627 втратила чинність з 01.01.2026.

Фундаментом нової системи є три види профілів безпеки, що визначають вимоги до захисту:

1) базові профілі безпеки – це мінімальні вимоги, розроблені Адміністрацією Держспецзв'язку на основі NIST 800-53 (впроваджений як НД ТЗІ 3.6-006-24). Наразі затверджено профілі для відкритої/конфіденційної інформації (Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409), службової інформації (Наказ Адміністрації Держспецзв'язку від 02.07.2025 № 419), державної таємниці та інформації НАТО. Вони переглядаються кожні два роки;

2) галузеві профілі безпеки формуються профільними міністерствами (наприклад, Мінцифри для реєстрів) з урахуванням галузевої специфіки. Мають пріоритет над базовими профілями;

3) цільовий профіль безпеки, який є ключовим документом (дещо подібний до колишнього ТЗ на КСЗІ), що розробляється власником системи на основі аналізу ризиків. Методологія розробки закріплена в Наказі Адміністрації Держспецзв'язку від 08.12.2025 № 811.

Для динамічних систем згідно з НД ТЗІ 3.6-006-24 також використовується адаптований профіль безпеки, що дозволяє коригувати заходи захисту на плановій основі.

Процедура авторизації є циклічним процесом, що складається з таких етапів:

1. Аналіз ризиків. На цьому етапі серед іншого відбувається визначення та узгодження вимог безпеки та приватності, здійснюється розробка Концепції інформаційної безпеки та приватності.

2. Категоріювання безпеки (НД ТЗІ 3.6-005-21): визначення рівня критичності (низький, середній, високий) за критеріями конфіденційності, цілісності та доступності.

3. Вибір заходів захисту: використання каталогу заходів за НД ТЗІ 3.6-006-24. Результатом є затвердження цільового профілю безпеки.

4. Виконання вимог цільового профілю (етап впровадження): практична реалізація з урахуванням вимог НД ТЗІ 3.6-004-21 та НД ТЗІ 3.6-007-21. Для держорганів обов'язкове врахування

Постанови Кабінету Міністрів України від 21 лютого 2025 року № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» щодо життєвого циклу засобів інформатизації.

5. Оцінювання дотримання вимог: проводиться ліцензіатами або уповноваженими органами відповідно до наказів Адміністрації Держспецзв'язку від 8 грудня 2025 року № 810 «Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи» та від 11 липня 2025 року № 438 «Про затвердження Вимог до юридичних осіб, фізичних осіб – підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем». Під час оцінки також використовуються методики НД ТЗІ 2.3-025-24 Т1-Т3.

6. Авторизація (НД ТЗІ 2.6-004-21): власник формує авторизаційний пакет та подає авторизаційний лист до Держспецзв'язку для включення до переліку авторизованих систем (Наказ Адміністрації Держспецзв'язку від 11 липня 2025 року № 434 «Про затвердження Порядку ведення переліку авторизованих систем з безпеки»). Для локалізованих одномашинних комплексів діє порядок перевірки за Наказом Адміністрації Держспецзв'язку від 4 вересня 2025 року № 545 «Про затвердження Порядку перевірки авторизаційної документації».

7. Постійний моніторинг (НД ТЗІ 3.6-008-21): безперервний контроль стану безпеки, реагування на інциденти та актуалізація профілів.

Законодавство передбачає три сценарії авторизації: первинна (повний цикл при введенні в експлуатацію); планова (щорічна) (підтвердження чинності звіту, якщо ризики та цільовий профіль не змінилися); позапланова: проводиться при модернізації інформаційної системи або зміні базових профілів; оцінюються лише змінені компоненти. Альтернативою авторизації (крім систем з держтаємницею) є сертифікація системи управління інформаційною безпекою за стандартом ISO/IEC 27001. При виборі між шляхами власник має враховувати фінансову складову. Сертифікат діє 3 роки, але вимагає щорічних наглядових аудитів. Скасування авторизації відбувається у разі порушення термінів перевірок або невиправлення недоліків, виявлених держконтролем.

Отже, запроваджена модель авторизації є життєздатним механізмом, який забезпечує динамічний захист інформаційних активів держави, стимулює розвиток вітчизняних ліцензіатів та інтегрує українську кібербезпеку в світовий технологічний контекст.

Маргара Дмитро Володимирович, *викладач кафедри тактичної підготовки навчально-наукового інституту поліцейської діяльності НАВС*

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ КАДРІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Підготовка кадрів для Національної поліції України в умовах дії правового режиму воєнного стану перестала бути виключно питанням професійного навчання або формального проходження освітніх програм. Після початку повномасштабної збройної агресії рф діяльність поліцейських фактично відбувається в умовах підвищеного ризику, де працівник поліції нерідко першим прибуває на місце події, здійснює евакуацію, приймає участь у бойових діях. У таких умовах особливого значення набуває не лише рівень знань законодавства чи застосування фізичної сили, спеціальних засобів, а насамперед психологічна готовність поліцейського до прийняття швидкого рішення щодо застосування вогнепальної зброї. Саме цей елемент підготовки тривалий час залишався одним із найбільш проблемних у системі професійного навчання, оскільки на практиці поліцейський часто опиняється між необхідністю негайного реагування для захисту життя людей і страхом подальшого переслідування, службових перевірок або негативної реакції керівництва.

Відповідно до положень Закону України «Про Національну поліцію» поліцейський має право застосовувати вогнепальну зброю у випадках, прямо передбачених законом, зокрема: 1) для відбиття нападу на поліцейського або членів його сім'ї, у випадку загрози їхньому життю чи здоров'ю; 2) для захисту осіб від нападу, що загрожує їхньому життю чи здоров'ю; 3) для звільнення заручників чи осіб, незаконно позбавлених волі; 4) для відбиття нападу на об'єкти, що перебувають під охороною, конвої, житлові та нежитлові приміщення, а також звільнення таких об'єктів у разі їх захоплення; 5) для затримання особи, яку застали під час вчинення тяжкого або особливо тяжкого злочину і яка намагається втекти; 6) для затримання особи, яка чинить збройний опір, намагається втекти з-під варти, а також озброєної особи, яка погрожує застосуванням зброї та інших предметів, що загрожують життю і здоров'ю людей та/або поліцейського; 7) для зупинки транспортного засобу шляхом його пошкодження, якщо водій своїми діями створює загрозу життю чи здоров'ю людей та/або поліцейського; 8) для примусового припинення польоту безпілотного повітряного судна, якщо є обґрунтовані підстави вважати, що таке судно використовується для вчинення правопорушення або становить загрозу життю чи здоров'ю людей та/або поліцейського, шляхом пошкодження чи знищення безпілотного повітряного судна та/або складових частин безпілотної авіаційної системи.