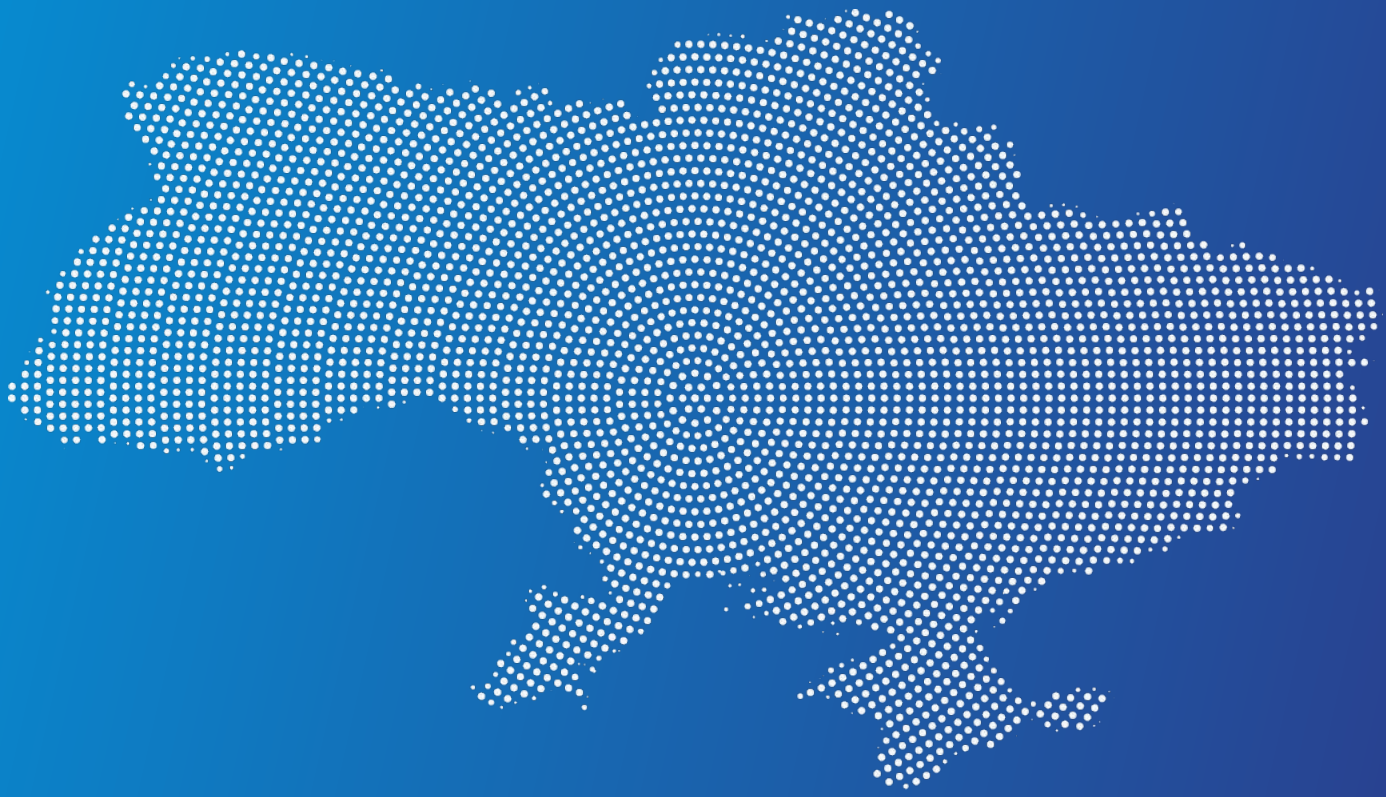
ОГЛЯД НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ 2025

Аналітичне дослідження



НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Tallinn Mechanism

Ministry of Foreign Affairs and International Cooperation

ОГЛЯД НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ 2025

Аналітичне дослідження

Цей аналітичний огляд був проведений за підтримки Міністерства закордонних справ і міжнародного співробітництва Італії в рамках Талліннського механізму.

Зміст

ВСТУП

На виконання вимог Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021 та Плану її реалізації, затвердженого Указом Президента України від 1 лютого 2022 року № 37/2022 Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України забезпечено проведення аналітичного дослідження в рамках огляду національної системи кібербезпеки.

Цей огляд дає комплексну оцінку стану національної системи кібербезпеки України у 2025 році. Це був рік, що поєднав не лише масштабне нормативне оновлення та помітні операційні здобутки, але й низку системних проблем, частина яких залишається хронічно невирішеною.

Україна одночасно веде активну кібервійну й реформує власну систему кібербезпеки відповідно до вимог євроінтеграційного процесу. Ці два завдання не лише не виключають одне одного – в окремих вимірах вони взаємно підсилюються. Проте вони ж породжують стратегічну напруженість: з одного боку це необхідність негайного оперативного реагування, а з іншого - довгострокова інституційна перебудова, яка пов’язана зі зростаючими вимогами до суб'єктів кіберзахисту і постійним дефіцитом кваліфікованих кадрів та фінансових ресурсів.

На нормативному рівні 2025 рік позначився низкою важливих законодавчих оновлень. Закон № 4336-IX та ряд постанов Кабінету Міністрів разом утворили новий регуляторний каркас який включає запровадження ризик-орієнтованого підходу, інституту керівників з кіберзахисту в органах державної влади (CISO), оновлену архітектуру реагування на інциденти. Разом із тим значна частина підзаконних актів набула чинності лише наприкінці року, а їх практична реалізація відстає від нормотворчих темпів.

На оперативному рівні зафіксовано помітні результати. Радикально зменшується кількість кіберінцидентів критичного та високого рівня, і одночасно з цим загальний показник реалізації Стратегії кібербезпеки зріс від 32% у 2022 році до 86% у 2025-му. Фактично держава продовжує системно розбудовувати власну систему кібербезпеки і це дає практичні результати. Одночасно з цим позитивна динаміка досягається в умовах зростаючого тиску з боку противника, який також системно вдосконалює інструментарій – зокрема, впроваджуючи великі мовні моделі безпосередньо у шкідливе програмне забезпечення для генерації коду в режимі реального часу.

Безпекове середовище у 2025 році якісно ускладнилось. Російські APT-групи перейшли від масованих деструктивних атак до довготривалого стратегічного закріплення в системах державного управління, оборонно-промислового комплексу та розробників безпілотних систем, синхронізуючи кібероперації з кінетичними ударами й інформаційними кампаніями. Ракетні обстріли об'єктів енергетики супроводжуються кібератаками та масованим поширенням дезінформації. Ще одним виміром ескалації стала задокументована кооперація між російськими та північнокорейськими групами у кібератаках на оборонні підприємства.

Попри позитивну динаміку, цей огляд виявив кілька стійких викликів, що обмежують розвиток національної системи кібербезпеки. Передусім це розрив між центром і регіонами у рівні технічного оснащення та кадрових спроможностей – він залишається критичним і формує вразливі точки входу для атак. По-друге, кадровий дефіцит у публічному секторі, зумовлений структурним дисбалансом між державними і ринковими умовами оплаті праці, не має системного вирішення. По-третє, законопроєкт про Кіберсили Збройних Сил України не був проголосований протягом 2025 року, що залишає певний вакуум у сфері кібероборони. І, нарешті, недофінансування з державного бюджету хоча і компенсується міжнародною технічною допомогою, однак така залежність несе власні ризики для цифрового суверенітету та розвитку вітчизняного ринку.

Цей огляд – спроба створити надійну аналітичну основу для проведення комплексної оцінки національної системи кібербезпеки, що дозволить відповідальним державним органам скорегувати свій стратегічний та оперативний порядок денний в сфері кібербезпеки, зорієнтувавши його на вирішення виявлених проблем.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Це дослідження ґрунтується на методології, розробленій для Національного координаційного центру проєктом USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, а також схожого тематичного дослідження проведеного у 2024 році.

В основі методології – поєднання трьох складових:

- Кабінетне дослідження, що базується на вивчені численних відкритих джерел: законодавства, аналізу медіа простору за релевантними тематиками, наукових досліджень тощо.
- Результати таргетованого опитування, проведеного Національним координаційним центром кібербезпеки протягом березня 2026 року шляхом надсилання відкритих питань до майже 100 державних установ: основні суб'єкти забезпечення кібербезпеки; органи державної влади центрального та місцевого рівнів; Національний інститут стратегічних досліджень. Слід зазначити, що опитувальник мав варіативну частину, яка була додана для деяких цільових відомств, для яких питання мали додаткові уточнення.
- Використання даних з внутрішніх інформаційних систем Національного координаційного центру кібербезпеки – CyberTracker.

Крім того, у рамках дослідження були використані результати низки інтерв'ю з представниками основних суб'єктів кібербезпеки та НКЦК, для більш об'єктивної оцінки питань дослідження та визначення наявних проблемних аспектів.

У дослідженні використана виключно відкрита інформація.

I. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Закон «Про основні засади забезпечення кібербезпеки України» та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Основними нормативно-правовими актами, що визначають організаційно-правову основу та пріоритети розвитку національної системи кібербезпеки (далі - НСК) є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII та Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає національну систему кібербезпеки як *сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.*

До НСК входять 10 основних суб'єктів: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, Міністерство закордонних справ України, які виконують такі основні завдання.

Державна служба спеціального зв'язку та захисту інформації України є базовим органом виконавчої влади у сфері кіберзахисту. На неї покладено формування та реалізацію державної політики щодо захисту державних інформаційних ресурсів, інформації з обмеженим доступом, критичної інфраструктури та активної протидії агресії у кіберпросторі. Служба здійснює державний контроль у відповідних сферах, забезпечує стандартизацію криптографічного і технічного захисту інформації, протидії технічним розвідкам та кіберзахисту. До її функцій належить створення і функціонування національної системи реагування на кіберінциденти, кібератаки та кіберзагрози, системи обміну інформацією про такі події, забезпечення діяльності Державного центру кіберзахисту, Центру активної протидії агресії у кіберпросторі та національної команди реагування CERT-UA. Окремим напрямом діяльності є розвиток Національної електронної комунікаційної мережі, організаційно-технічної моделі кіберзахисту, професійної кваліфікації фахівців, проведення навчання персоналу державних органів і критичної інфраструктури, а також методичне регулювання оцінювання стану кіберзахисту.

Національна поліція України забезпечує захист прав і свобод людини, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі. До її повноважень належать запобігання, виявлення, припинення та розкриття кіберзлочинів, зокрема правопорушень щодо об'єктів критичної інформаційної інфраструктури. Важливим напрямом роботи є також інформування населення з питань безпеки у цифровому середовищі.

Служба безпеки України виконує функції захисту державної безпеки у кіберпросторі. Вона здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки, миру і безпеки людства, а також злочинів терористичної спрямованості, що вчиняються із використанням кіберпростору. До компетенції СБУ належать контррозвідувальні та оперативно-розшукові заходи щодо протидії кібершпигунству, кібертероризму і кібердиверсіям, координація діяльності інших суб'єктів у цих напрямах, негласна перевірка готовності критичної інфраструктури до можливих кібератак, розслідування інцидентів щодо державних ресурсів та забезпечення реагування на кіберзагрози у сфері державної безпеки.

Міністерство оборони України та Генеральний штаб Збройних Сил України у межах компетенції відповідають за підготовку держави до відбиття воєнної агресії у кіберпросторі, розвиток спроможностей кібероборони, захист військових інформаційних систем та мереж, а також співпрацю з НАТО, міжнародними організаціями та іноземними партнерами у сфері спільної протидії кіберзагрозам.

Розвідувальні органи України здійснюють добування, аналіз та надання розвідувальної інформації щодо зовнішніх загроз національній безпеці у кіберпросторі, діяльності іноземних державних та недержавних акторів, а також інших процесів, що можуть впливати на кібербезпеку держави.

Національний банк України виконує функції галузевого регулятора кібербезпеки фінансового сектору. Він встановлює порядок, вимоги та заходи із забезпечення кіберзахисту і інформаційної безпеки банків, небанківських фінансових установ, операторів платіжних систем та технологічних операторів платіжних послуг, а також здійснює контроль за їх виконанням. НБУ забезпечує функціонування власного Центру кіберзахисту та команди реагування CSIRT-NBU, організовує систему оцінювання стану кіберзахисту установ фінансового сектору та визначає вимоги до аудиту інформаційної безпеки.

Міністерство закордонних справ України забезпечує зовнішньополітичний вимір кібербезпеки. Воно сприяє євроінтеграції України у сфері кібербезпеки, координує співпрацю з міжнародними партнерами щодо посилення кіберстійкості та спільного реагування на кібератаки, представляє державу в міжнародних організаціях з питань формування норм поведінки у кіберпросторі, сприяє спільним заходам з Європейським Союзом у сфері кіберстійкості та боротьби з кіберзлочинністю, а також координує дипломатичні й санкційні механізми реагування на деструктивну кібердіяльність.

Загальна координація діяльності у сфері кібербезпеки як складової національної безпеки здійснюється Президентом України через Раду національної безпеки і оборони України.

Ключовим міжвідомчим координаційним механізмом є Національний координаційний центр кібербезпеки як робочий орган РНБО України. Центр здійснює координацію та загальний контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, координує функціонування національної системи реагування на кіберінциденти, готує пропозиції щодо оголошення кризової ситуації у сфері кібербезпеки, координує реалізацію Стратегії кібербезпеки України та підготовку змін до неї з урахуванням стандартів Європейського Союзу. Окремим напрямом його діяльності є визначення пріоритетів та підготовка пропозицій щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони, а також координація стратегічних комунікацій у сфері кібербезпеки.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки.

Слід зазначити, що Міністерство цифрової трансформації України відповідно до Закону не належить до основних суб'єктів забезпечення кібербезпеки, водночас є членом Національного координаційного центру кібербезпеки, що забезпечує участь Мінцифри у формуванні стратегічних рішень щодо розвитку НСК.

Приватний сектор є повноцінним елементом національної системи кібербезпеки України, оскільки значна частина критичної інформаційної інфраструктури належить саме бізнесу. Закон зобов'язує компанії, що є власниками та операторами ОКІ, впроваджувати технічні та організаційні заходи кіберзахисту, забезпечувати стійкість власних інформаційних систем, виявляти та документувати кіберінциденти, а також у визначених випадках повідомляти про них CERT-UA. Це формує базовий рівень кіберстійкості держави, який залежить від зрілості та готовності приватних організацій.

Приватний сектор також бере участь у державно-приватному партнерстві, обміні інформацією про загрози та індикатори компрометації, спільних навчаннях і розвитку національних політик кіберзахисту. В умовах війни фахівці приватного бізнесу значно посилили кадровий потенціал національної системи кібербезпеки шляхом мобілізації до сектору безпеки і оборони. У підсумку бізнес виступає не лише об'єктом регулювання, а й ключовим партнером держави у зміцненні кіберстійкості країни.

Академічний сектор та система освіти відіграють стратегічну роль у національній системі кібербезпеки України, оскільки саме вони формують кадровий потенціал, наукову базу та інноваційні рішення для держави й приватного сектору. Університети, наукові установи та освітні організації забезпечують підготовку кадрів для секторів оборони, державного управління та бізнесу, розробляють навчальні програми з кібербезпеки та цифрової грамотності. Вони також проводять наукові дослідження, створюють нові технології та методи протидії кіберзагрозам, беруть участь у міжнародних проєктах і сприяють інтеграції України у глобальну кіберспільноту. Таким чином, академічний сектор формує фундамент для довгострокової кіберстійкості держави та забезпечує інтелектуальну підтримку розвитку національної політики у сфері кібербезпеки.

В цілому національна система кібербезпеки є досить збалансованою, її організаційна форма та розподіл ролей між учасниками засвідчили свою ефективність у ході протидії кібервійні рф. Національний координаційний центр кібербезпеки є координуючим ядром НСК який має забезпечувати її гармонійний розвиток та координацію. Особливістю національної системи кібербезпеки України є її мілітаризованість – адже серед 10 суб'єктів 8 (окрім НБУ та МЗС) є правоохоронними або військовими структурами – що забезпечило перевагу в ході протидії кіберагресії під час повномасштабного воєнного вторгнення рф.

II. ОГЛЯД ПОТОЧНОЇ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ТА КЛЮЧОВИХ ВИКЛИКІВ

У 2025 році регуляторне поле кібербезпеки в Україні зазнало системної «перезбірки» навколо двох взаємопов'язаних блоків: законодавчих змін, закріплених **Законом України від 27.03.2025 № 4336-IX** «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який був прийнятий з метою імплементації норм європейських директив з кібербезпеки та запровадив зміни до національного законодавства в сферах захисту інформації та кіберзахисту, а також великого масиву підзаконних актів 2025 року, спрямованих на його практичну реалізацію.

Зокрема, на виконання Закону, у 2025 році було прийнято наступні **постанови Кабінету Міністрів України**:

- № 1471 від 13.11.2025 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності»;
- № 1533 від 26.11.2025 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»;
- № 1281 від 08.10.2025 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни»;
- № 1516 від 26.11.2025 «Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади»;
- № 1470 від 13.11.2025 «Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518» *(постанова КМУ від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»);*
- № 1531 від 26.11.2025 «Про внесення змін до постанови Кабінету Міністрів України від 29 березня 2006 р. № 373» *(постанова КМУ від 29.03.2006 «Про затвердження Правил*

забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»);

- №1580 від 03.12.2025 «Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах»;
- № 1668 від 17.12.2025 «Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту»;
- № 1799 від 31.12.2025 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури».

Таким чином, нормативно-правове регулювання сфери кібербезпеки у 2025 році зазнало суттєвих змін, ключові з яких можна звести до наступних практичних трансформацій:

Новий інституційний дизайн реагування і інформаційного обміну. Було унормовано функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, а також національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози. Визначено механізми реагування на кризову ситуацію в кібербезпеці. Було визначено уповноважений орган, який забезпечує функціонування нацсистеми обміну та встановлює порядок обміну, форми повідомлень, національну таксономію інцидентів, а також порядок приєднання до платформи обміну. Одночасно закріплено обов'язок власників/розпорядників систем повідомляти відповідний CSIRT про всі кіберінциденти у порядку, визначеному уповноваженим органом.

Посилення кадрового потенціалу з кіберзахисту у держорганах та ОКІІ. Законодавчо закріплено утворення у держорганах підрозділів з кіберзахисту та введено штатні посади керівників з кіберзахисту (CISO), а для ОКІІ та органів місцевого самоврядування – призначення відповідальних осіб і (за потреби) утворення підрозділу. Була визначена процедура призначення CISO включно з механізмами погодження і перевірки, а також пряма заборона поєднувати цю роль із посадою, відповідальною за цифрову трансформацію.

Удосконалення концептуальних підходів до захисту інформації та зменшення державного контролю. Законодавчі зміни забезпечили відмову від КСЗІ та визначили процес впровадження заходів з управління ризиками та їх підтримання протягом життєвого циклу систем на основі профілів безпеки. Передбачено функціонування системи оцінювання стану кіберзахисту включно з методом аудиту без надмірного контролю з боку держави.

Зокрема, у законодавство про захист інформації було інтегровано інститут «авторизації з безпеки» та пов'язаної з ним «екосистеми» профілів безпеки (базовий/цільовий/галузевий), життєвого циклу підтвердження відповідності, відкритого переліку авторизованих систем, а також (для частини систем – без державної таємниці) альтернативи у вигляді сертифікації відповідності стандарту інформаційної безпеки. Передбачено повідомний (декларативний) принцип для прийняття рішення про авторизацію (за виключенням систем, де обробляється таємна інформація) та підтвердження дотримання нормативних вимог. Запроваджено нову архітектуру оцінювання та державного контролю через процедури самооцінювання/зовнішнього оцінювання, звітність і моніторинг.

Впровадження інструменту "вимоги про реагування". У новій редакції статті 9 Закону «Про основні засади забезпечення кібербезпеки України» передбачено, що уповноважені органи можуть надавати обов'язкові до виконання вимоги про реагування власникам/розпорядникам систем та операторам КІ/КІІ, із подальшим звітуванням про їх виконання.

Національний план реагування. У 2025 році було прийнято Національний план реагування, який визначив процедури і механізм координації/взаємодії між суб'єктами реагування та суб'єктами забезпечення кібербезпеки, включно з можливістю залучення приватних команд і міжнародних партнерів, що підкріпило модель "єдиного циклу реагування" для державного сегмента і КІІ. Із Національним планом прийнято Порядок

інформування та звітування про реагування, який визначив процедури публічного інформування або звітування про реагування на кіберінциденти, кібератаки та усунення їх наслідків.

Посилення регіональної, секторальної кіберстійкості та залучення приватного сектору. Нормативні зміні забезпечили правові підстави для розвитку мережі галузевих та регіональних центрів кіберзахисту (CERT, CSIRT) та широкі можливості для залучення приватних гравців як до спільного реагування на кіберінциденти, так і до створення галузевих або регіональних команд

Вразливості і відповідальне розкриття. Порядок 2025 року з пошуку/виявлення вразливостей запровадив системні механізми сканування, оцінки захищеності та узгодженого розкриття вразливостей, а також прямо описав координацію з Європейською базою вразливостей ENISA, що є важливим кроком до міждержавної сумісності підходів до управління вразливостями.

Стратегічні кібероперації. Вперше у національне законодавство був введений термін «стратегічні кібероперації» та започатковано правовий алгоритм формування стратегічного задуму та подальшої координації їх виконання. Зокрема, НКЦК отримав повноваження щодо визначення пріоритетів, розроблення концептуальних засад та внесення Президентові України пропозицій щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечення координації суб'єктів сектору безпеки і оборони щодо їх проведення.

Зміни у компетенціях і "балансі сил" між основними акторами

Розширення ролі Держспецзв'язку. Нормативні зміни 2025 року розширили мандат Держспецзв'язку, перетворивши його на ключовий орган не лише з нормативного регулювання, а й з операційного управління національною системою кіберзахисту.

Орган отримав комплексні повноваження щодо забезпечення функціонування національної та регіональних систем реагування на кіберінциденти (зокрема через CERT-UA), включаючи координацію взаємодії галузевих і регіональних команд, визначення їхніх спроможностей, процедур реагування, моніторинг діяльності та ведення єдиної таксономії і репозитарію кіберінцидентів. Водночас Держспецзв'язку забезпечує функціонування національної системи та платформи обміну інформацією про кіберінциденти, встановлює критерії значних інцидентів і обов'язкові формати звітності.

Суттєво посилено регуляторну та стандартизаційну роль: орган затверджує і впроваджує стандарти (з урахуванням міжнародних практик), визначає процедури оцінки відповідності, здійснює нормативно-правове регулювання у сферах криптографічного і технічного захисту інформації, кіберзахисту та протидії технічним розвідкам, а також виконує функції органу стандартизації.

Окремий блок становить методичне керівництво: оцінювання стану кіберзахисту державних інформаційних ресурсів і критичної інфраструктури, розроблення рекомендацій щодо організації підрозділів кіберзахисту та ролі CISO, впровадження процедур виявлення вразливостей, а також розвиток практик кібергігієни через інструктажі та тренінги.

Посилено й напрям розвитку людського капіталу: Держспецзв'язку відповідає за підготовку, перепідготовку та підвищення кваліфікації фахівців, запровадження системи професійних кваліфікацій, їх оцінювання та визнання, а також створення і функціонування кваліфікаційного центру.

Важливою новацією є розширення інструментів впливу: орган отримав право надавати обов'язкові до виконання вимоги щодо усунення порушень, а також здійснювати оперативне реагування, зокрема шляхом видачі приписів власникам інформаційних систем і об'єктів критичної інфраструктури для запобігання або мінімізації наслідків кіберінцидентів, особливо в умовах надзвичайного чи воєнного стану.

Додаткові повноваження НКЦК. Було також розширено повноваження НКЦК. Зокрема, закріплено загальну координацію функціонування суб'єктів національної системи

реагування на кіберінциденти та формування постійно діючої об'єднаної групи реагування (для кризових ситуацій). Крім цього НКЦК отримав повноваження щодо координації стратегічних кібероперацій, оголошення кризової ситуації в кібербезпеці, а також координації стратегічних комунікацій у сфері кібербезпеки.

Розширення функцій СБУ. Законом України від 27.03.2025 № 4336-IX СБУ було надано функції координатора діяльності суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям. СБУ отримала ефективний механізм реалізації повноважень з реагування на кіберзагрози.

Включення МЗС до складу НСК. До складу основних суб'єктів Національної системи кібербезпеки було введено Міністерство закордонних справ України, як ключовий орган, що забезпечує та координує заходи кібердипломатії. Крім цього протягом 2025 року було вжито внутрішні організаційно-правові заходи, спрямовані на посилення спроможностей МЗС із виконання зазначеної задачі.

Оператори критичної інфраструктури та власники/розпорядники ОКІІ. Для них 2025 рік означав перехід до організаційно зрілої моделі: впровадження плану кіберзахисту (щорічний перегляд), обов'язкові базові заходи, системне управління ризиками, оцінювання поточного стану кіберзахисту (самооцінювання щороку і зовнішнє оцінювання не рідше ніж раз на два роки), а також включення у цикл державного контролю (моніторинг і перевірки).

Державні органи/органи місцевого самоврядування як власники систем. На них концентруються імперативні вимоги мінімальних заходів захисту, кадрові вимоги (наявність підрозділу з кіберзахисту та CISO), процедурні вимоги реагування/інформування та обов'язкові тренінги з кібергігієни.

Ключові виклики та проблемні питання

Національна нормативно-правова база у сфері кібербезпеки України є одним із ключових елементів забезпечення національної безпеки та характеризується достатньо розвиненою інституційною архітектурою із визначеним розподілом повноважень між суб'єктами. Вона сформована з урахуванням кращих практик Європейського Союзу та НАТО і в умовах триваючої гібридної агресії демонструє здатність до адаптації, трансформуючись у дієвий інструмент протидії кіберзагрозам. Водночас, попри наявність базових правових і організаційних механізмів, розвиток НСК залишається певною мірою нерівномірним і супроводжується низкою системних, нормативних та інституційних проблем, що стримують підвищення загального рівня кіберстійкості держави.

Однією з ключових проблем є недосконаліть механізмів відповідальності за порушення вимог у сфері кібербезпеки. Чинне законодавство не передбачає ефективних інструментів притягнення до відповідальності, зокрема накладення вагомих фінансових санкцій, що знижує превентивний ефект правових норм. Адміністративна відповідальність посадових осіб у більшості випадків має формальний характер і не стимулює належного рівня дотримання встановлених вимог. Водночас відсутня чітко визначена персональна відповідальність керівництва суб'єктів за критичні недоліки в організації кіберзахисту, що ускладнює формування належної управлінської культури безпеки. Разом із тим, впровадження жорстких санкцій у період воєнного стану потребує зваженого підходу, оскільки надмірний фінансовий тиск може негативно вплинути на спроможність суб'єктів забезпечувати належний рівень кіберзахисту.

Суттєвою проблемою залишається також фрагментарність і незавершеність підзаконного регулювання. Незважаючи на прийняття низки нормативно-правових актів, значна частина ключових елементів, зокрема таксономія кіберінцидентів, стандартизовані форми повідомлень, механізми ведення репозитаріїв інцидентів та функціонування цифрових платформ обміну інформацією потребують подальшої деталізації. У результаті формується розрив між встановленими законодавчими обов'язками щодо повідомлення про інциденти та наявними практичними інструментами їх реалізації.

Додатковим викликом є наявність секторальних колізій у регулюванні, зокрема щодо фінансового сектору, який частково виведений із загального регуляторного поля. Такий підхід дозволяє уникнути дублювання функцій, однак водночас створює ризики порушення єдності стандартів у межах національної системи кібербезпеки та ускладнює ефективну взаємодію між суб'єктами під час реагування на інциденти.

Суттєвим стримуючим фактором є також обмеженість кадрового та інституційного потенціалу. Реалізація існуючих вимог щодо регулярного оцінювання стану кіберзахисту, аудиту та контролю потребує розвиненого ринку кваліфікованих спеціалістів, включаючи аудиторів, фахівців із оцінки відповідності та керівників з інформаційної безпеки. Наразі спостерігається дефіцит таких кадрів, що створює ризики формального виконання вимог без досягнення реального підвищення рівня кіберстійкості.

Окрему складність становить розвиток підходів до забезпечення безпеки ланцюгів постачання. Запровадження багаторівневих моделей оцінки ризиків та підтвердження безпеки постачальників вимагає суттєвої перебудови закупівельних процедур, договірної роботи та внутрішніх політик організацій. За відсутності уніфікованих підходів і типових рішень це може призводити до затримок у закупівлях і нерівномірного виконання вимог.

Умови воєнного стану створюють додаткові виклики для забезпечення балансу між прозорістю та безпекою. З одного боку, законодавство передбачає відкритість певної інформації щодо систем кіберзахисту, з іншого - існують обмеження, пов'язані з необхідністю захисту чутливих даних. Відсутність чітких критеріїв у цій сфері формує складнощі правозастосування та підвищує ризики як надмірного розкриття інформації, так і її необґрунтованого обмеження.

Аналіз функціонування Національної системи кібербезпеки також свідчить про домінування реактивного підходу до забезпечення кіберзахисту. Значна частина суб'єктів зосереджується на ліквідації наслідків інцидентів, тоді як заходи з їх попередження, прогнозування загроз та виявлення вразливостей залишаються недостатньо розвиненими. Така ситуація підвищує вразливість до складних багатовекторних атак і не відповідає сучасним підходам до управління кіберризиками.

Крім того, спостерігається суттєвий дисбаланс у рівні технічного оснащення та спроможностей між центральними органами влади та суб'єктами на регіональному або галузевому рівнях. Це формує так звані «слабкі ланки» у системі, які можуть бути використані як точки входу для зловмисників із подальшим поширенням атак на інші сегменти державної інфраструктури.

Окремої уваги потребує питання нормативної невизначеності процедур реагування на кіберінциденти, кіберзагрози та кризові ситуації у сфері державної безпеки. Відсутність уніфікованих алгоритмів взаємодії між різними органами, зокрема в умовах одночасного застосування механізмів антитерористичної діяльності, реагування на надзвичайні ситуації та кіберінциденти, ускладнює координацію дій і знижує ефективність реагування.

У сфері міжнародної співпраці актуальним залишається питання гармонізації законодавства України з європейськими стандартами. Зокрема, потребує завершення процес імплементації положень Другого додаткового протоколу до Конвенції про кіберзлочинність, що сприятиме підвищенню ефективності транскордонного доступу до електронних доказів. Важливим є також впровадження європейських регуляторних підходів у сфері цифрових послуг, що дозволить забезпечити належний баланс між безпекою та захистом прав громадян. Разом із тим, слід враховувати, що фактором, який унеможливлює повну імплементацію норм європейських директив у сфері кібербезпеки є те, що Україна не являється членом ЄС, що обмежує поширення на Україну окремих механізмів, передбачених європейським кібербезпековим законодавством, наприклад включення до загального механізму ЄС з реагування на кризові події тощо.

Суттєвим викликом залишається протидія кібертероризму та кібердиверсіям як складовим гібридної війни. Попри наявність загального визначення кібертероризму, законодавство не містить чітко сформульованого складу відповідного злочину, а також визначення кібердиверсії. Це ускладнює правозастосування, процеси розслідування та

притягнення винних осіб до відповідальності. Додатковою проблемою є відсутність чітко визначених механізмів координації дій між різними відомствами у випадках комплексних кризових ситуацій та процедур невідкладного доступу до даних у разі виникнення ознак терористичного акту.

З урахуванням викладеного, подальший розвиток організаційно-правових основ Національної системи кібербезпеки має бути спрямований на вдосконалення механізмів відповідальності з урахуванням принципу пропорційності, завершення формування підзаконної нормативної бази та цифрової інфраструктури обміну інформацією, усунення секторальних колізій, посилення кадрового та інституційного потенціалу, а також розвиток проактивних підходів до управління кіберризиками. Важливим є забезпечення узгодженості з європейськими стандартами, формування ефективних механізмів державно-приватного партнерства, а також створення чітких процедур реагування на кіберзагрози та кризові ситуації.

Загалом, ключовим завданням є перехід від переважно реактивної моделі забезпечення кібербезпеки до системи, що базується на принципах превентивності, ризик-орієнтованості та інтегрованого управління, що дозволить підвищити стійкість держави до сучасних і майбутніх кіберзагроз.

Також вже більше чотирьох років залишається невирішеним питання формування правової основи для створення та функціонування в Україні кіберсил, що потребує невідкладного прийняття відповідного законодавчого акта. Зокрема законопроєкт № 12349 від 19.12.2024 «Про Кіберсили Збройних Сил України» так і не був проголосований народними депутатами у 2025 році, що значно послаблює спроможності держави з кібероборони в умовах агресії рф[1].

III. ОСНОВНІ ЗДОБУТКИ

Незважаючи на воєнні і геополітичні виклики, швидку еволюцію ландшафту кіберзагроз, Україна змогла досягти помітного прогресу за усіма основними напрямами.

Правові заходи

Здійснено масштабне оновлення нормативно-правової бази, що дозволило гармонізувати українське законодавство з європейськими стандартами (зокрема NIS2 та DORA) та передовими світовими практиками.

Оновлення ключового законодавства: Прийнято Закон № 4336-IX та низку підзаконних актів, якими імплементовано європейські підходи до кібербезпеки та захисту критичної інформаційної інфраструктури. Закон також розширив інституційні спроможності та повноваження ключових суб'єктів – Держспецзв'язку, СБУ, МЗС, НКЦК.

Інституціоналізація ролей: Офіційно запроваджено інститут керівників з кіберзахисту (CISO) в органах державної влади та на об'єктах критичної інфраструктури, розроблено та затверджено Порядок призначення керівника з кіберзахисту (Постанова КМУ від 26.11.2025 № 1516), Методичні рекомендації щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту (Наказ Адміністрації Держспецзв'язку від 03.12.2025 № 798).

Унормування реагування на інциденти, обміну інформацією про кіберзагрози, виявлення вразливостей: Забезпечено функціонування національної системи реагування на кіберінциденти, національної системи обміну інформацією про кіберінциденти, системи виявлення вразливостей. Затверджено Національний план реагування на кіберінциденти (Постанова КМУ від 26.11.2025 №1533), Порядок взаємодії суб'єктів національної системи

[1] Станом на час написання цього огляду у І кварталі 2026 зазначений законопроєкт також не був схвалений Верховною Радою України

реагування на кіберінциденти (Постанова КМУ від 13.11.2025 №1471), які чітко алгоритмізували порядок взаємодії та реагування на кіберінциденти.

Стимулювання кібергігієни: Затверджено Порядок проведення обов'язкових інструктажів та систематичних тренінгів щодо кібергігієни для держслужбовців та розроблено проект Національної стратегії кібергігієни.

Державно-приватне партнерство: Розроблено та передано на розгляд парламенту проєкт Закону «Про державно-приватну взаємодію у сфері кібербезпеки», що створює легальні рамки для обміну даними та спільного кіберзахисту.

Технічні заходи

Технічний потенціал держави зазнав якісної модернізації, що дозволило нейтралізувати значну кількість атак ще на етапі їх підготовки.

Проактивний кіберзахист та моніторинг: СБУ успішно реалізувала проактивну модель, зосередившись на завчасному виявленні загроз, протидії кібертероризму та контррозвідувальних перевірках ІТ-інфраструктур. ДЦКЗ Держспецзв'язку значно покращив моніторинг подій безпеки в державних органах: було підключено нові організацій до підсистеми NDR та встановлено 24 сенсори збору телеметрії (загальна кількість сенсорів – 93), а також забезпечено моніторинг і захист понад 46,5 тисяч серверів та робочих станцій через підсистему захисту кінцевих точок (EDR/MDR).

Система фільтрації фішингових доменів Protective DNS: Система фільтрації фішингових доменів, до якої підключено понад 500 провайдерів, виявила та заблокувала близько 72 тисяч фішингових ресурсів, пов'язаних із фінансовим шахрайством та стилізованих під урядові портали Кабінету Міністрів України, Дія, «єДопомога», «Зимова ЄПідтримка», «ЄВідовлення», «ЄПільга», «ЄВиплата», Портал Гуманітарної допомоги, українських банків та платіжних сервісів. Це дозволило убезпечити 2,3 млн запитів українців та щомісяця попереджати шахрайство на суму 25-30 млн грн. Здійнюється розбудова національного сервісу доменних імен DNS для проактивного захисту від кіберзагроз.

Модернізація архітектури безпеки: Державні органи активно впроваджували багатофакторну автентифікацію (MFA), централізоване логування та моніторинг подій безпеки, архітектуру «нульової довіри» (Zero Trust), інтегрували свої системи з платформами обміну індикаторами компрометації, платформою MISP.

Організаційні заходи

Система управління кібербезпекою зазнала важливих структурних трансформацій для підвищення оперативності та ефективності прийняття рішень.

Розвиток спроможностей сектору оборони: набули розвитку спроможності кібероборони Збройних Сил України, забезпечено авторизацію з безпеки ряду ключових інформаційно-комунікаційних систем ЗСУ; впроваджено інститут штатних служб захисту інформації та впроваджено в новосформованих армійських корпусах штатних посад офіцерів з кібербезпеки; розпочато створення SOC в ЗСУ; курс базових заходів з кібербезпеки ЗСУ розміщено на Порталі Армія+ для підвищення його доступності та зручності проходження.

Структурне посилення відомств: У Мінцифри утворено спеціалізований Директорат з кіберзахисту та хмарних послуг, в МЗС Відділ кіберзахисту виокремлено у самостійний підрозділ. Створено та сертифіковано нові галузеві центри SOC та CSIRT (зокрема в ДПСУ).

Кібербезпека регіонів: ініційовано процес підвищення рівня кібербезпеки та посилення спроможностей на регіональному рівні. СБУ активно розвиває спроможності регіональних підрозділів, Держспецзв'язку створює нові регіональні центри, що дозволить підвищити ефективність виявлення та реагування на кіберінциденти.

Ідентифікація об'єктів критичної інфраструктури: забезпечено функціонування Реєстру об'єктів критичної інфраструктури. До Реєстру внесено відомості про понад 4600 об'єктів.

Прогнозування атак на українську інфраструктуру: Забезпечено покращення ситуаційної обізнаності та можливості з прогнозування атак завдяки регулярному обміну інформацією про кіберзагрози в рамках роботи Об'єднаної групи реагування на кіберінциденти при НКЦК.

Розвиток спроможностей і кадрового потенціалу

Професійна освіта: закладами фахової передвищої і вищої освіти за спеціальністю 125 «Кібербезпека» підготовлено 3541 осіб (17 докторів філософії, 1192 магістрів, 2263 бакалаврів). На спеціальність F5 «Кібербезпека та захист інформації» на освітній ступінь бакалавра було зараховано 3753 особи, магістра – 1353 особи, доктора філософії 74 особи.

Кібернавчання та підвищення кваліфікації: проведено майже 100 навчальних заходів (семінарів, тренінгів, навчань) з підвищення кваліфікації за різними напрямами кібербезпеки для представників державних органів, об'єктів критичної інфраструктури, приватних компаній. Основні суб'єкти забезпечення кібербезпеки активно брали участь у провідних міжнародних тактичних і командно-штабних навчаннях під егідою НАТО та союзників, зокрема: Cyber Coalition 2025, Locked Shields 2025, CWIX-2025, Defence Cyber Marvel 4, Amber Mist-2025.

Масова кіберграмотність та залучення молоді: На державному порталі «Дія» навчання за програмами кіберграмотності пройшли близько 1 мільйона громадян. За ініціативи НКЦК успішно проведено загальнонаціональний Місяць кібербезпеки з охопленням всіх регіонів. Підготовлено посібники «Кібергігієна. Безпека в Інтернеті» та «Зброя інформаційної війни», які розповсюджувались в якості навчальних матеріалів, що забезпечило єдину інформаційну рамку кампанії по всій країні. Кіберполіція провела Всеукраїнський конкурс «Cyber Security Camp», що охопив понад 12 тисяч студентів із 289 навчальних закладів.

Лідерство, інклюзивність та інновації у спорті: НКЦК продовжило реалізовувати Національну ініціативу із залучення жінок у галузь, проведено перші кіберзмагання «CTF for Women». Спільно з Мінмолодьспорту запроваджено новий вид військово-технологічного спорту та проведено перший Чемпіонат України з CTF. Розроблено та впроваджено програму стратегічного лідерства у кібербезпеці «Sophos. Joint. Cyber».

Співробітництво

Високі темпи демонструють розвиток державно-приватного партнерства, заходи кібердипломатії та міжнародної взаємодії в сфері кібербезпеки.

Інтеграція до ЄС та НАТО, підтримка глобальних ініціатив: Представник НКЦК вперше направлений як національний експерт для роботи в Агентстві ЄС з кібербезпеки ENISA, забезпечено дієву взаємодію з Центром колективної кібероборони НАТО CCDCOE, де також Україна представлена на рівні національного експерта. Україна здобула статус кандидата на приєднання до Глобального партнерства зі штучного інтелекту (GPAI). Налагоджено системний обмін інформацією про кіберзагрози з країнами ЄС.

Талліннський механізм та міжнародна підтримка: В 2025 році значно активізувалася міжнародна співпраця у межах Талліннського механізму[2] – міжнародної ініціативи, спрямованої на підтримку кіберстійкості цивільної та критичної інфраструктури України. У квітні 2025 року запрацював Проєктний офіс Талліннського механізму (Tallinn Mechanism Project Office, TMPO)[3], покликаний посилити координацію між партнерами й забезпечити стабільну довгострокову підтримку цифрової безпеки України. Ініціатором створення TMPO виступило Міністерство цифрової трансформації України. Офіс плідно співпрацює з українськими партнерами Талліннського механізму – Держспецзв'язку, МЗС, СБУ та НКЦК. Також розширився перелік країн-учасниць: до механізму долучилися Норвегія (липень 2025 року), Фінляндія (жовтень 2025 року) та Чехія (січень 2026 року). Загалом у 2025 році країнам-

[2] https://platform-tm.com/who-we-are

[3] https://platform-tm.com/news/tallinn-mechanism-project-office-launches-in-ukraine-to-strengthen-cyber-resilience

донорам вдалося акумулювати понад 61 млн євро на реалізацію проєктів та активностей у межах Талліннського механізму. До їх імплементації через тендери долучається і український кіберсектор, що створює умови для плідної співпраці між українськими та міжнародними кіберкомпаніями, а також посилює державно-приватне партнерство.

Міжнародна співпраця: Проведено раунди кібердіалогів з ЄС та Нідерландами. В рамках двосторонньої взаємодії Держспецзв'язку уклало 9 нових меморандумів про співпрацю з кіберагентствами країн-партнерів (Чехія, Фінляндія, США, Велика Британія тощо) та провідними світовими ІТ-компаніями.

Державно-приватне партнерство і цифровий суверенітет: Започатковано ініціативу щодо підтримки розвитку конкурентоспроможних національних рішень та експорту технологій в сфері кібербезпеки. До реалізації проєктів міжнародної технічної допомоги долучаються українські кібербезпекові компанії. Провідні українські постачальники хмарних сервісів ініціювали створення «Українського альянсу цифрового суверенітету».

Формування ролі України як регіонального лідера: Ініційовано створення Кіберальянсу Україна–Румунія–Молдова, це новий формат стратегічної співпраці, спрямований на зміцнення регіональної кіберстійкості. Проведено Київський міжнародний форум кіберстійкості 2025, який об’єднав українських та міжнародних представників державного сектору, міжнародних організацій, бізнесу, кіберспільноти, технологічних компаній і провідних експертів галузі для обговорення ключових викликів кібербезпеки.

Формування політик атрибуції та відповідальності: Україна забезпечила узгодженість політичних заяв із державами-партнерами щодо атрибуції кібератак. На міжнародному рівні (включно з майданчиками ООН та ОБСЄ) активно просувалася позиція щодо необхідності притягнення до відповідальності за кібератаки на об'єкти цивільної інфраструктури як за воєнні злочини. Департамент кіберполіції також тісно співпрацював з Європолом та Інтерполом для координації розслідувань транснаціональних кіберзлочинів.

IV. КЛЮЧОВІ ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

Кібервійна в Україні є першим у світі прикладом повномасштабного гібридного конфлікту, де кібератаки не просто супроводжують, а синхронізуються з кінетичними ударами та інформаційними операціями. Почавшись ще у 2014 році, вона перейшла у фазу високої інтенсивності напередодні повномасштабного вторгнення 2022 року. Російські APT групи застосовали деструктивні програми-вайпери для знищення даних у державних установах та атакували супутниковий зв'язок, щоб паралізувати управління військами в перші години нападу. Впродовж останніх років росія здійснює тисячі кібератак на критичну інфраструктуру, об’єкти енергетики, фінансовий сектор, інформаційні ресурси державних органів, прагнучи підірвати національну безпеку нашої держави.

В залежності від обстановки на полі бою та геополітичної ситуації змінюються пріоритети, цілі та тактики проведення російських кібероперацій. У 2025 році ключовими пріоритетами діяльності російських хакерських груп були підтримка ведення бойових дій, внутрішня дестабілізація в Україні, вплив на союзників нашої держави для зменшення військової та політичної підтримки. Кіберактивність в основному спрямовувалась на отримання доступу та стратегічне закріплення для збору розвідувальних даних в інформаційних системах державних органів, об’єктів критичної інфраструктури, військових системах ситуаційної обізнаності та керування, які використовуються урядом та силами безпеки і оборони. Пріоритетними цілями кібератак були організації сектору безпеки і оборони, держані органи, підприємства сектору електронних комунікацій, енергетики, ІТ, логістики, оборонні підприємства, медіа.

В той же час, російські спецслужби не відмовились від деструктивних операцій, проводячи вибіркові атаки на життєво важливі об'єкти. Так, у грудні 2023 року кібератака на

Київстар призвела до зникнення зв'язку у 24 мільйонів абонетів, у грудні 2024 року було здійснено спробу знищення інформації у Єдиних і Державних реєстрах Мінюсту, у лютому 2025 року здійснювались деструктивні атаки на об'єкти енергетики та теплопостачання, у березні 2025 року для пошкодження залізничних перевезень було здійснено кібератаку на Укрзалізницю. Ці атаки мали виразний національний вимір та торкнулись життя значної кількості громадян.

Окремо потрібно відмітити зміщення фокусу кібератак на регіони – на місцеві органи влади, комунальні підприємства забезпечення населення водою, теплом, енергією, місцевих провайдерів інтернет, тощо. І насамперед це стосується прифронтових областей України.

В рамках підтримки ведення бойових дій підрозділи спецслужб та збройних сил рф здійснювали кібератаки, спрямовані на отримання доступу до військових систем ситуаційної обізнаності та керування військами, масові атаки з використанням соціальної інженерії на військовослужбовців Сил оборони України для отримання доступу до переписки в месенджерах. рф активно використовує кіберрозвідку, включаючи злам камер відеоспостереження, для коригування та оцінки наслідків кінетичних ударів по місцях дислокації підрозділів СОУ, логістиці, критичній цивільній інфраструктурі.

Одним з пріоритетів рф на полі бою стало подолання «kill zone» лінії дронів, тому з початку 2025 року значно зросла інтенсивність кібератак на підприємства оборонно-промислового комплексу, розробників та виробників безпілотних систем. Цілями цих атак є як знищення даних, модифікація прошивок і програмного забезпечення безпілотних апаратів, промислове шпигунство, так і ідентифікація місць виробництва, логістики, ланцюгів постачання для подальшого нанесення кінетичних ударів.

росія постійно покращує інтеграцію (координацію) кібератак з інформаційними операціями та військовими діями, швидко адаптуючи їх під зміни обстановки. У воєнній доктрині рф кібератаки не є ізольованими подіями, натомість є складовою комплексних операцій. Яскравим прикладом є кампанія «Чорна зима», в рамках якої з осені 2025 року ракетні обстріли енергетики синхронізуються з кібератаками на підприємства енергетичного сектору та масованим поширенням дезінформації та панічних настроїв у соцмережах.

Впродовж останніх років рф системно посилює спроможності з проведення наступальних кібероперацій, збільшуючи кількість задіяного персоналу, розвиваючи інструментарій та впроваджуючи нові технології. У 2025 році відбувся якісний стрибок у застосуванні ШІ: від генерації фейкових новин (дезінформаційні мережі Doppelgänger, CopyCop, Pravda) росія перейшла до використання великих мовних моделей (LLM) безпосередньо у шкідливому програмному забезпеченні. Зафіксовано використання групою UAC-0001/APT28 (ГРУ) інструментів (наприклад, LameHug), де ШІ генерує шкідливий код «на льоту», що робить такі віруси «невидимими» для традиційних засобів захисту. Російські актори загроз активно застосовують публічні ШІ сервіси та локальні LLM моделі для розвідки та профілювання цілей, розробки шкідливого ПЗ та експлойтів, автоматизації кібератак. Це дозволяє рф масштабувати кібероперації та залучати до них більшу кількість персоналу з нижчим рівнем компетенцій. Також ШІ масово використовується для створення діпфейків та автоматизованого фішингу високої якості українською мовою.

До кібератак на українську інфраструктуру залучені не тільки російські спецслужби, але і контрольовані ними фінансово-мотивовані злочинні групи (в тому числі ransomware групи). Для посилення таких кіберзлочинних груп спецслужби рф передають їм новітні розробки, вразливості та інструментарій для здійснення кібератак (в тому числі для мобільних пристроїв), що створює ризики неконтрольованого розповсюдження «кіберзброї», яка була раніше доступна тільки державам. Так, в Telegram каналах російських кіберзлочинців було виставлено на продаж ПЗ Pegasus для віддаленого зламу мобільних телефонів. Ця пропозиція знайшла своїх покупців, компанія Apple була змушена інформувати своїх клієнтів про чергову компрометацію через застосування Pegasus.

Стратегія рф демонструє цілеспрямоване розширення географії кібератак та інформаційних операцій на країни ЄС і НАТО. Метою цих дій є втручання у виборчі процеси європейських держав, підрив єдності союзників та зменшення рівня військової, політичної і

громадської підтримки України. Для виконання цих завдань спецслужби рф активно залучають підконтрольні угруповання псевдохактивістів, які фокусуються на спробах саботажу роботи західної критичної інфраструктури, зокрема об'єктів водопостачання, енергетики та транспорту, а також власних громадян, які проживають у західних країнах. Одночасно рф систематично проводить гібридні операції «під чужим прапором», активно формуючи імідж «жертви кібервійни» та атакуючи інфраструктуру країн ЄС (Польща, Словаччина, Франція) під виглядом «українських хакерів» або абстрактних груп. Атаки на водопостачання та логістику в Європі супроводжуються інформаційними кампаніями, що мають на меті посіяти недовіру до України та зменшити обсяги військової допомоги.

У 2025 році кібервійна остаточно вийшла за межі двостороннього конфлікту. Було виявлено десятки кіберінцидентів, які були атрибутовані до діяльності КНДР. При цьому за низкою векторів кібератак спостерігалася кооперація між діяльністю державних акторів загроз рф та КНДР. У листопаді 2025 року було виявлено, що групи Gamaredon (фсб рф) та Lazarus (КНДР) використовували спільну інфраструктуру для кібератак на європейські оборонні підприємства та українських виробників безпілотних систем з метою крадіжки технологій.

росія та її союзники масштабують кібератаки на ланцюги постачання, розглядаючи інфраструктуру країн ЄС як вхідний вектор для завдання шкоди Україні. Метою таких операцій є не лише шпигунство, а й зрив постачання озброєння, розвідданих та технологій подвійного призначення компаніями-партнерами.

Одночасно росія докладає системні зусилля для створення цифрової «залізної завіси» з метою захисту власного кіберпростору. Впроваджено блокування дзвінків у WhatsApp/Telegram, примусовий перехід на національний месенджер «Макс», фільтрацію трафіку на рівні протоколів (блокування Cloudflare, Speedtest), блокування VPN сервісів. Це створює автономний інформаційний простір для тотального контролю над населенням, в тому числі на тимчасово окупованих територіях України. Незважаючи на це, рф демонструє системні недоліки у кіберзахисті власної критичної інфраструктури, що є наслідком в тому числі санкцій країн Заходу.

Ключовими викликами для національної системи кібербезпеки в умовах війни є:

Розвиток проактивної кібероборони та протидія агресії. Безпека військових систем і мереж та спроможності впливу на противника у кіберпросторі є невід'ємною складовою оборони. Втрата управління військами та зброєю призведе до краху держави та нівелює значення решти елементів національної оборони. Розвиток наступальних спроможностей в кіберпросторі здатен забезпечити асиметричну перевагу над противником, що має значно більші військові, економічні та інші ресурси.

Посилення кіберстійкості критичної інфраструктури. Одним з ключових викликів є забезпечення безперервного функціонування та швидке відновлення об'єктів критичної інфраструктури в умовах комбінованих атак, які включають кібератаки, інформаційні операції, масовані обстріли.

Окремо виділяється **проблема нерівномірного розподілу ресурсів та спроможностей** в сфері кібербезпеки між центром та регіонами, як на національному рівні, так і на рівні окремих організацій.

Стратегічним ризиком для національної безпеки України є **велика база застарілого програмного забезпечення та обладнання**, в тому числі промислових систем (OT//ICS/SCADA) на об'єктах критичної інфраструктури, для якого зростають ризики виявлення та експлуатації вразливостей. Крім того, негативний вплив має використання неліцензійного програмного забезпечення та особистих пристроїв працівників для службових цілей.

Крім того, викликом є **трансформація моделі національної системи кібербезпеки** з реактивного реагування на наслідки кібератак на проактивне виявлення та попередження кіберзагроз.

Розвиток кадрового потенціалу. Однією з найвразливіших ланок національної системи кібербезпеки залишається низький рівень кібергігієни та обізнаності про ризики кібербезпеки серед громадян, державних службовців та працівників підприємств. Водночас

державні органи та об'єкти критичної інфраструктури потерпають від значного кадрового дефіциту у сфері кібербезпеки. Через високу конкуренцію та неможливість запропонувати оплату праці на рівні з міжнародними чи приватними компаніями відбувається постійний відтік досвідчених фахівців із державного сектору. Неврегульованими залишаються питання залучення за фаховими спеціальностями ІБ спеціалістів в ході мобілізації.

Швидкі технологічні зміни та забезпечення цифрового суверенітету. Стрімкий розвиток технологій штучного інтелекту, квантових обчислень створює додаткові ризики та вже помітно впливає на сферу кібербезпеки. Технології ШІ дозволяють автоматизувати як процеси захисту, так і нападу, що розширює можливості акторів загроз. Впровадження квантових комп'ютерів створює можливість розшифрування державних, військових та фінансових комунікацій, перехоплення критичних даних і руйнування систем автентифікації.

Зростає **рівень залежності від малого кола глобальних постачальників рішень**, що в середньостроковій перспективі створює потенційні загрози втрати контролю над інфраструктурою і даними.

Швидка еволюція кіберзагроз. Швидка еволюція кіберзагроз створює високодинамічне та складно прогнозоване середовище, що вимагає від суб'єктів кібербезпеки безперервної адаптації, постійного оновлення практичних навичок персоналу та пошуку нових проактивних механізмів захисту. ШІ забезпечує нападникам новий рівень масштабованості, адаптивності та швидкості, що робить атаки значно складнішими для виявлення за допомогою традиційних засобів захисту, дозволяє планувати та здійснювати складні кібератаки навіть малокваліфікованим особам без глибоких знань. Відбувається стрімка розвиток тактик і векторів атак – від схем соціальної інженерії до глибоко прихованих і комплексних операцій із застосуванням вразливостей нульового дня.

На глобальному рівні виклики для національної системи кібербезпеки створює:

Гармонізація законодавства з вимогами ЄС. Як кандидат на членство Україна активно імплементує вимоги і стандарти ЄС в сфері кібербезпеки, що є викликом для організацій через високу вартість їх провадження. Імплементація кібербезпекового законодавства ЄС вимагає від України значних інвестицій у підготовку відповідних фахівців, перебудову систем кібербезпеки, безпеку ланцюгів постачання тощо.

Глобальна мілітаризація кіберпростору, активне використання кіберзасобів у міжнародній конкуренції, розвиток та неконтрольоване поширення кіберзброї. Відносини між США та КНР в сфері кібербезпеки все більше набувають рис жорсткого суперництва. Глобальні лідери вживають дзеркальні заходи щодо зменшення своєї технологічної залежності один від одного, заявляючи при цьому про системні приховані вразливості у технологіях один одного. Країни світу все частіше заявляють про формування та активну діяльність своїх кіберсил, які проводять не лише оборонні, але і наступальні кібероперації. Країна-агресор здійснює гібридні операції, направлені на пошкодження глобальної інфраструктури інтернет, зокрема, фізичне пошкодження підводних кабелів. Це розширює простір загроз для української системи кібербезпеки.

V. ЛАНДШАФТ КІБЕРЗАГРОЗ У 2025 ТА ЗАГРОЗИ У 2026 РОЦІ

Ландшафт кіберзагроз

Національна команда реагування на кіберінциденти CERT-UA в 2025 році опрацювала 5927 кіберінцидентів, на 37,4% більше, ніж в 2024 році[4]. За загальною кількістю виявлених кібератак на свою інфраструктуру Україна посіла 5 місце у світі, а за інтенсивністю

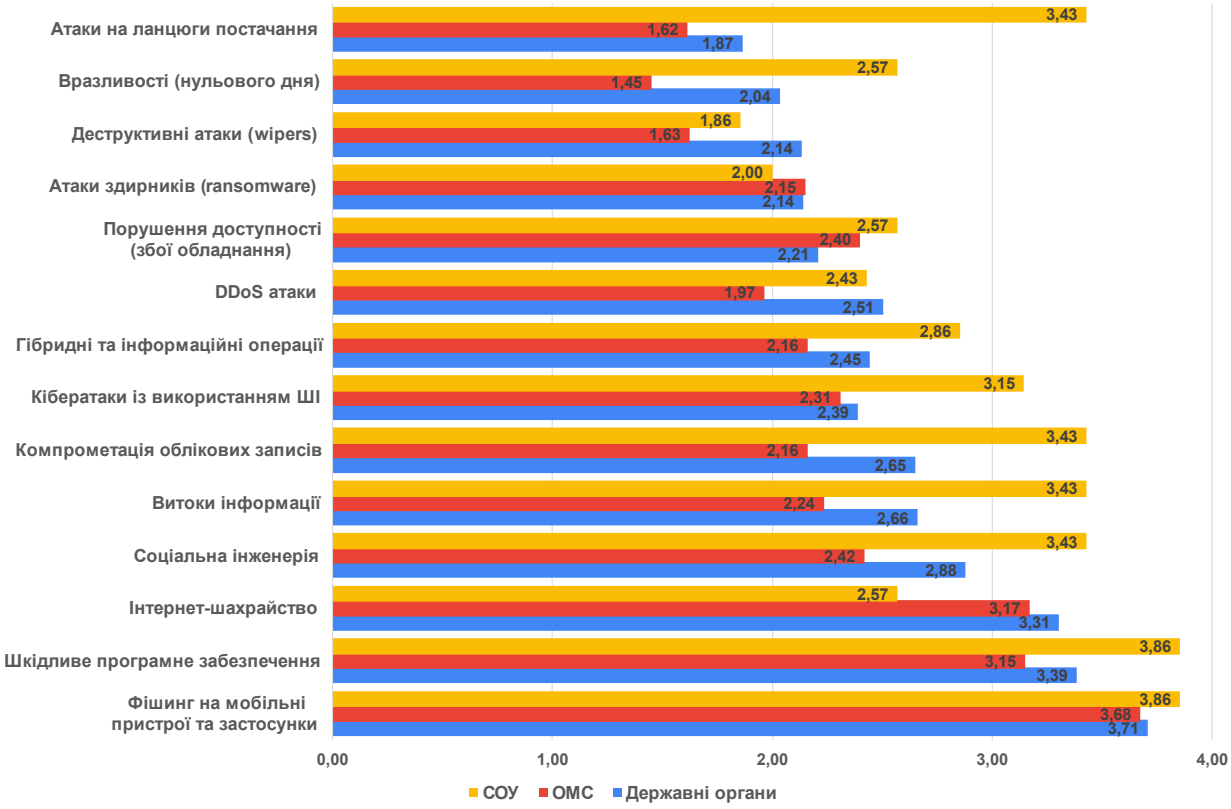
[4] https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

високопрофесійних атак з боку державних хакерських груп – 1 місце в Європі та 3 місце у світі після США та Ізраїлю[5].

Найбільшу кількість кібератак у 2025 році було спрямовано на державні органи, сектор безпеки і оборони, енергетичний сектор, оборонно-промисловий комплекс, сектори охорони здоров'я, IT, електронних комунікацій, транспорту і логістики, медіа. Незмінною залишилась тенденція **збільшення долі кібератак на регіони** України, яка спостерігалася як у публічному, так і в приватному секторі. При цьому найбільше зростання фіксувалося у прифронтових областях.

Головними загрозами 2025 року стали цілеспрямовані APT-атаки, фішингові кампанії із залученням технологій генеративного штучного інтелекту, масштабна компрометація облікових записів, атаки через ланцюги постачання, використання деструктивного програмного забезпечення і програм-вимагачів, інтернет-шахрайство.

Найбільш актуальні загрози за результатами опитування експертів державного сектору наведено на рис. (актуальність загрози оцінювалася за шкалою від 0 до 5).



Основним джерелом загроз для національної системи кібербезпеки у 2025 році була діяльність російських хакерських груп. Впродовж року зафіксовано діяльність акторів загроз з інших країн, проте вона не мала вирішального впливу на розвиток ландшафту кіберзагроз.

Група UAC-0057 (Ghostwriter), пов'язана із спецслужбами Республіки Білорусь, здійснювала фішингові розсилки на представників державних органів та сектору безпеки і оборони. Основний інструментарій – PicassoLoader, Cobalt Strike, зафіксовано експлуатацію вразливостей CVE-2024-42009, CVE-2025-49113 у Roundcube. Основна мотивація – шпигунство.

Актори загроз КНДР здійснювали фішингові атаки на окремі органи державного сектору з метою збору розвідувальних даних. Крім того, у листопаді 2025 року було виявлено, що групи UAC-0010 (фсб рф) та Lazarus (КНДР) використовували спільну інфраструктуру для кібератак на європейські оборонні підприємства та українських виробників безпілотних систем з метою крадіжки технологій.

[5] https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

Найрезонанснішим кіберінцидентом національного рівня у 2025 році стала масштабна деструктивна атака на ІТ-системи АТ «Укрзалізниця» у березні, яка мала на меті дестабілізувати логістику та спричинила тривалий збій у роботі онлайн-сервісів перевізника, хоча й не зупинила рух поїздів.

Основні тенденції

Еволюція соціальної інженерії

Соціальна інженерія помітно еволюціонувала у 2025 році, а різноманітні види фішингу стали основним вектором початкового проникнення.

Фішингові кібератаки еволюціонували від масових нецільових розсилок до **глибокої персоніфікації**. Ворог систематично збирає розвідувальні дані з відкритих джерел, зокрема з порталів державних закупівель, аналізує витоки та дані попередніх атак для профілювання цілей та виявлення контактів цільових осіб. У фішингових повідомленнях зловмисники маскуються під керівництво, колег або державні установи, використовуючи точні імена, посади та військові звання, розуміючи поточні задачі цільової особи, що критично підвищує рівень довіри до шкідливого повідомлення.

Спостерігалося суттєве зростання **фішингу в месенджерах**: від звичайних текстових повідомлень зловмисники перейшли до **повноцінного голосового спілкування**. Первинна взаємодія дедалі частіше здійснюється через телефонні дзвінки з українських номерів, після чого, встановивши довіру, жертві надсилався шкідливий файл у месенджер. Крім того, зафіксовано використання штучного інтелекту для чат-ботів та генерації голосових повідомлень українською мовою.

Пріоритетною метою залишається **перехоплення акаунтів у месенджерах** Signal, WhatsApp та Telegram. У першому півріччі спостерігалось масове застосування техніки **створення паралельних сесій** (GhostPairing) за допомогою підроблених **QR-кодів**[6]. Для компрометації також активно експлуатуються **емоційні тригери**: прохання проголосувати за дітей у конкурсах малюнків[7] або підписати електронні петиції на сайті Президента України. Отримавши доступ, ворог проникає у закриті чати військовослужбовців для збору розвідданих та проведення подальших атак.

З лютого 2025 року з’явилась тенденція використання складних технічних **«експлойтів» соціальної інженерії**, що маніпулюють діями користувача. Масово застосовується тактика **ClickFix**[8]: жертві демонструється фейкова перевірка безпеки (CAPTCHA), для проходження якої користувача змушують власноруч скопіювати та запустити в консолі шкідливий PowerShell-скрипт. Зловмисники також використовували **OAuth Phishing**[9], **Device Code Phishing**[10] для створення прихованих сесій у корпоративному середовищі Microsoft (Teams, O365), Google **App-Specific Passwords (ASP) Phishing**[11] для легального отримання несанкціонованого доступу до сервісів Google через надання дозволів шкідливим застосункам.

Ще однією тактикою була масова реєстрація доменів, що імітують цільові організації та легітимні бренди (**domain impersonation**). Так, в ході підготовки комплексної атаки на підприємства оборонно-промислового комплексу було створено інфраструктуру з майже 1000 фішингових доменів західних та українських оборонних компаній. Зловмисники **створювали високоякісні фейкові сайти** державних реєстрів, обласних адміністрацій, застосунків

[6] https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/
[7] https://cyber.bank.gov.ua/news/179
[8] https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2025/
[9] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[10] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/?msockid=16b08e5738b6661a2d9b9c1d390d6782
[11] https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia

«Резерв+» та «Дія», міжнародних фондів (зокрема Червоного Хреста) для поширення шкідливого ПЗ, викрадення акаунтів та масштабного збору персональних і платіжних даних громадян.

Додатковою сталою тенденцією є **маскування шкідливої активності під легітимні процеси**. Для розміщення фішингових сторінок, приховування командно-контрольної інфраструктури та передачі викрадених даних зловмисники активно зловживали довіреними публічними хмарними сервісами, такими як Dropbox, Google Drive, GitHub, Cloudflare Tunnels тощо.

Кібератаки на мобільні пристрої

У 2025 році збільшилась кількість кібератак на мобільні пристрої посадових осіб, військовослужбовців та громадян. Зловмисники фокусувалися на викраденні чутливої інформації, перехопленні комунікацій та відстеженні місцезнаходження цілей.

Однією з найбільш критичних загроз стало використання **комерційного шпигунського програмного забезпечення** (такого як Pegasus, Candiru, Predator) для таргетованих атак на вище українське військово-політичне керівництво та дипломатів[12].

Масового характеру набуло поширення **шкідливих файлів у форматі APK** для операційної системи Android, які маскувалися під легітимні державні або благодійні сервіси. Зловмисники розповсюджували фейковий застосунок «єПідтримка» безпосередньо через Google Play для викрадення платіжних даних, контактів та доступу до СМС-повідомлень. В іншій кампанії шкідливий APK-файл пропонувався під виглядом отримання фінансової допомоги від французької організації, що дозволяло хакерам непомітно перехоплювати дані банківських застосунків. Через фейкові сайти розважального контенту під виглядом відеоплеєра поширювалось мобільне шпигунське ПЗ CamelSpy. Окремим вектором є розповсюдження інфікованих версій спеціалізованого мобільного програмного забезпечення військових систем ситуаційної обізнаності[13], які використовуються для відстеження переміщень військових підрозділів.

Використання штучного інтелекту

У 2025 році використання штучного інтелекту набуло масового характеру, перетворившись на ключовий фактор масштабування та підвищення ефективності кібероперацій.

Штучний інтелект кардинально змінив підходи до **підготовки фішингу**, зробивши атаки із застосуванням соціальної інженерії втричі ефективнішими[14]. APT групи та фінансово мотивовані актори використовували ШІ для написання якісних персоналізованих текстів в електронній пошті та месенджерах. Зафіксовано використання індивідуальних голосових повідомлень (**дипфейків**) українською мовою для атак на військовослужбовців Сил оборони України.

ШІ-чатботи активно застосовуються для масштабування вербування громадян з метою здійснення диверсій, підпалів та збору розвідданих.

Помітною інновацією року стала поява **шкідливого програмного забезпечення**, **яке динамічно керується ШІ**. Російська група UAC-0001 (гру) застосувала нове шкідливе ПЗ LameHug, що використовувало відкриту велику мовну модель (Qwen 2.5-Coder-32B-Instruct) через публічне API для генерації системних команд «на льоту» на основі текстових описів природною мовою[15].

Актори загроз угруповання з рф, Китаю, КНДР та Ірану систематично **експлуатували публічні платформи** (ChatGPT, Gemini) для розвідки цілей, дослідження ІТ-систем, розробки

[12] https://www.rnbo.gov.ua/ua/Diialnist/7305.html
[13] https://cert.gov.ua/article/6280563
[14] https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/
[15] https://cert.gov.ua/article/6284730

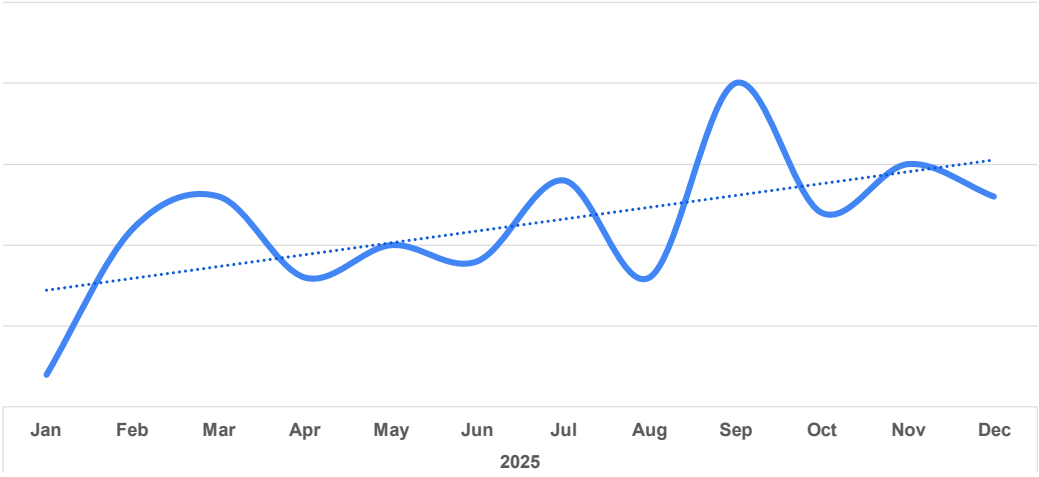
та налагодження експлойтів і шкідливого коду[16] [17]. Наприклад, російські хакери використовували ChatGPT для створення та вдосконалення бекдору ScopeCreep, інтегруючи туди функції обходу засобів захисту та підвищення привілеїв. Хоча західні компанії блокують таку активність, зловмисники обходять обмеження за допомогою одноразових та скомпрометованих акаунтів, або ж розгортають на власних серверах локальні відкриті моделі (зокрема Llama-3 від Meta).

У сфері **інформаційних операцій** рф масштабувала мережу фейкових медіа (таких як CopyCop), контент яких генерується за допомогою ШІ, що радикально здешевило створення дезінформації[18]. Однією з основних цілей було «отруєння ШІ»: через величезні обсяги створеної росією дезінформації в інтернеті, популярні публічні ШІ-чатботи під час навчання інтегрують ці фейки у свої бази знань і згодом видають їх користувачам як достовірні факти[19].

Використання інфостілерів та компрометація облікових записів

У 2025 році **компрометація облікових записів** та масове викрадення даних авторизації стали одним із домінуючих векторів кіберзагроз. Російські APT-групи та кіберзлочинці систематично атакували корпоративні поштові сервери Microsoft O365, Roundcube, Zimbra[20], акаунти у популярних поштових сервісах ukr.net, i.ua та месенджерах Signal, WhatsApp, Telegram.

У порівнянні з попереднім роком зафіксовано **зростання використання інфостілерів** (програм-викрадачів даних і файлів). Спостерігається застосування як спеціалізованих розробок (наприклад, HomeSteel, WreckSteel[21], FileMess[22]), так і комерційного шкідливого ПЗ Lumma, Amatera, Rhadamanthys, RedLine, Snake Keylogger тощо. Інфостілери постійно розвиваються: від звичайного збору паролів вони перейшли до комплексних платформ розвідки (як GiftedCrook[23]), здатних ексфільтрувати файли, VPN-конфігурації, токени сесій та криптогаманці безпосередньо у Telegram-канали зловмисників. Зростання атак інфостілерів у 2025 році наведено на рисунку.



[16] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[17] https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf
[18] https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets
[19] https://www.enterprisesecuritytech.com/post/russia-s-pravda-disinformation-network-is-poisoning-western-ai-models
[20] https://www.eset.com/ua/about/newsroom/press-releases/malware/rosiyski-khakery-atakuyut-derzhavni-ustanovy-y-oboronni-kompaniyi-v-ukrayini-ta-yes/
[21] https://cert.gov.ua/article/6282902
[22] https://cert.gov.ua/article/6285731
[23] https://cert.gov.ua/article/6282946

Російські елітні APT-групи (зокрема UAC-0190/Void Blizzard[24] [25]) скуповували на Darknet-форумах **логи викрадених даних**, зібрані комерційними інфостілерами. Купівля готових доступів та токенів авторизації дозволяє пришвидшувати проникнення в цільову інфраструктуру та маскувати шпигунські операції під звичайну кіберзлочинність.

Кібератаки на ланцюги постачання

У 2025 році **атаки на ланцюги постачання** все частіше розглядалися як одна із значних загроз, яка дозволяє швидко масштабувати наслідки кібератак.

Одним із прикладів є компрометація системи електронного документообігу, яка широко використовується у державних органах, з подальшими атаками на міністерства і відомства влітку 2025 року.

У жовтні 2025 року в рамках атак на виробників безпілотних систем було скомпрометовано сайт розробника популярного застосунку для прошивки FPV-дронів. Зловмисники замінили файли застосунку на інфіковану версію, що призвело до встановлення шкідливого ПЗ віддаленого доступу у користувачів сайту.

Значним ризиком залишається **інфікування через неліцензійне програмне забезпечення**. Частково комп'ютерну техніку до сектору безпеки і оборони надають волонтери, які з метою економії можуть встановлювати завантажене із неофіційних джерел програмне забезпечення. Цей вектор активно експлуатується хакерами з Sandworm (гру), які системно розповсюджують інфіковані образи операційної системи Windows, пакету MS Office, інших програм та «активаторів» до них. Це неодноразово призводило до компрометації комп'ютерів в українських силових структурах.

Діяльність російських акторів загроз

Основні тенденції та тактики

Протягом 2025 року рівень кіберзагроз з боку російських хакерських груп залишався стабільно високим. У порівнянні з 2024 роком вони значно підвищили інтенсивність атак та варіативність застосованого інструментарію, сфокусувавшись на отриманні розвідувальної інформації та забезпеченні тривалої присутності в скомпрометованих мережах для підготовки наступних фаз атак. Крім того, кібероперації часто синхронізувалися з кінетичними ударами, що було особливо помітно під час зимових атак на підприємства тепло- та енергопостачання.

Основними векторами початкового проникнення у 2025 році стала соціальна інженерія, експлуатація вразливостей, використання скомпрометованих облікових записів RDP, VPN, атаки на ланцюги постачання, використання неліцензійного ПЗ, яке вже містить вбудовані бекдори на етапі встановлення. Зросла доля фішингу у месенджерах (Signal, WhatsApp), таргетованих атак з глибокою персоналізацію, використанням голосових викликів та попередньо скомпрометованих акаунтів для встановлення довіри.

Актори загроз демонструють чітку **спеціалізацію у векторах атак та виборі цілей**. фсб зосереджена на утриманні довгострокового доступу до державних ресурсів, гру виконує деструктивні та військово-розвідувальні завдання. Група UAC-0010 фокусується на масовому зборі розвідданих з інформаційних систем державних органів та сектору безпеки і оборони; спеціалізовані кластери загроз UAC-0099, UAC-0184, UAC-0218 сфокусовані виключно на військових; UAC-0232 проводить кампанії, спрямовані на окремі регіони; UAC-0246 розсилає фішингові листи на особисті поштові скриньки громадян України, насамперед на сервісі i.ua; кампанії UAC-0187, UAC-0102 направлені на компрометацію облікових записів користувчів поштового сервісу ukr.net.

[24] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

[25] https://www.aivd.nl/documenten/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

Для масштабування наступальних операцій рф постійно формує **нові кластери загроз** (UAC-0218, UAC-0219, UAC-0226, UAC-0227, UAC-0244, UAC-0245) та залучає «свіжу кров» – осіб з базовими навичками, спеціалістів з приватного сектора, кіберзлочинців, шахраїв, випускників військових навчальних закладів. Це призвело до надзвичайної варіативності методів соціальної інженерії: від різних форм шахрайства до використання штучного інтелекту.

Технічний інструментарій доставки та **початкового виконання коду** базується на використанні архівів з паролями та вкладених архівів; скриптів JS, VBS, PowerShell; файлів HTA, CPL та графічних SVG, PNG з вбудованим шкідливим кодом; документів MS Office з макросами, PDF/HTML-приманок.

Російські хакерські групи дедалі частіше **відмовляються від використання доменних імен** на користь прямих звернень до IP-адрес для обміну даними з командно-контрольними серверами та завантаження додаткового шкідливого коду на скомпрометовані пристрої. Зокрема, UAC-0010 відмовилися від використання сервісів Telegram / Telegraph для динамічного отримання адрес своїх серверів; натомість вони почали жорстко прописувати IP-адреси безпосередньо в коді свого шкідливого програмного забезпечення. Подібну тактику активно застосовує і група UAC-0184, яка здійснює завантаження вірусів на комп'ютери військовослужбовців за прямими посиланнями на IP-адреси без використання DNS-імен.

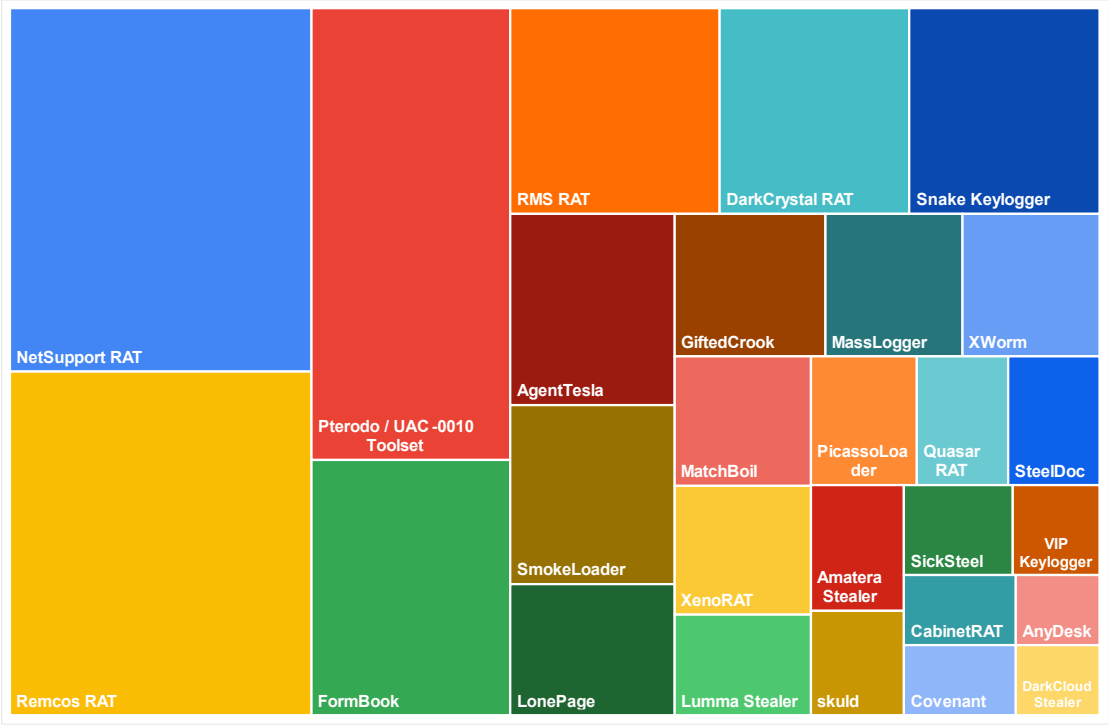
Щоб уникнути блокування з боку систем кіберзахисту, APT групи і фінансово мотивовані кіберзлочинці масово використовували **легальні сервіси** для розміщення командно-контрольної інфраструктури та ексфільтрації даних. Розміщення шкідливих файлів та передача інформації здійснювалась через довірені платформи, такі як Dropbox, Google Drive, E-Disk від UKR.NET, а також через сервіси тунелювання Cloudflare Tunnels.

Канали керування та ексфільтрації включали SMTP, HTTP/HTTPS, TCP, FTP, а також Telegram-боти.

Для виконання шкідливих команд, завантаження шкідливого ПЗ та ексфільтрації даних актори загроз активно експлуатували вбудовані інструменти операційних систем (**техніка LOLBin**, Living off the Land Binary). Зокрема, зафіксовано використання cmd, PowerShell, certutil, rundll32, mshta.exe, wmic.exe, curl.exe, скриптів PowerShell тощо.

У 2025 році спостерігається концептуальна зміна у підходах російських хакерських груп до **використання шкідливого програмного забезпечення**: від тактики швидкого викрадення даних без закріплення («Steal & Go») до забезпечення довготривалої прихованої присутності в IT-інфраструктурах[26]. При цьому для ускладнення атрибуції APT групи російських спецслужб (гру, фсб) дедалі частіше застосовували «комерційні» інструменти та шкідливе ПЗ з відкритим кодом (Remcos RAT, XWorm, DarkCrystal RAT, Lumma Stealer). Інновацією стало застосування генеративного штучного інтелекту безпосередньо в архітектурі шкідливого програмного забезпечення (бекдор LameHug). Найбільш часто використовуване шкідливе ПЗ наведено на діаграмі.

[26] https://cip.gov.ua/services/cm/api/attachment/download?id=74646



Для прихованого встановлення шкідливого ПЗ на комп'ютери російські групи активно використовували механізми альтернативних потоків даних (ADS) у файлових системах Windows, а також вбудовували шкідливі скрипти у спеціально сформовані графічні SVG-файли.

У 2025 році російські спецслужби, насамперед група UAC-0002 (Sandworm) та її підкластери, продовжили використовувати **деструктивні кібератаки** як інструмент гібридної війни для нанесення прямої шкоди критичній інфраструктурі та економіці. Метою було знищення даних, серверів віртуалізації та систем резервного копіювання, часто у координації з кінетичними ударами та інформаційними операціями.

У лютому, під час різкого зниження температури, було здійснено кібератаки на низку підприємств теплопостачання. Зловмисники вивели з ладу теплові пункти та порушили зв'язок з контролерами. 23 березня критичної деструктивної атаки зазнала «Укрзалізниця»: було знищено системи віртуалізації та резервного копіювання на основному й резервному майданчиках, що призвело до зупинки всіх онлайн-сервісів продажу квитків. Здійснювались деструктивні атаки на інфраструктуру життєзабезпечення, державні установи і реєстри, об'єкти енергетики, транспорту, приватні компанії агропромислового сектору, логістики.

Початковим вектором доступу для деструктивних атак найчастіше була експлуатація вразливостей у ланцюгах постачання та використання скомпрометованих облікових записів VPN без багатофакторної автентифікації. Також для початкового проникнення використовувались атаки на ланцюги постачання та методи соціальної інженерії. Зокрема, для розсилки шкідливого ПЗ теплоенергетичним та комунальним підприємствам по всій країні було скомпрометовано поштові акаунти одного з постачальників відповідного обладнання.

Для знищення даних використовувались програм-вайпери ZEROLOT, Sting[27], PathWiper[28].

У 2025 році продовжилась тенденція щодо **розширення географії російських кібератак** на країни ЄС та НАТО. Вектор кібератак все більше зміщується з виключно українських цілей на критичну інфраструктуру і сектор оборони країн ЄС[29] та НАТО. За даними Microsoft[30], Україна стала основною ціллю для 25% кібератак рф, а в першу десятку

[27] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
[28] https://blog.talosintelligence.com/pathwiper-targets-ukraine/
[29] https://www.cert.europa.eu/publications/threat-intelligence/tlr2025/pdf
[30] https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

найбільш атакованих російськими акторами загроз увійшли тільки країни ЄС і НАТО. Головною метою цих атак на партнерів України є підрив єдності Заходу, зменшення військової та фінансової підтримки України та дестабілізація суспільно-політичної ситуації в країнах-партнерах.

Кібератаки як інструмент підтримки інформаційних операцій

У 2025 році російські спецслужби системно використовували **кібератаки як інструмент підтримки інформаційних операцій**, де технічне проникнення в системи було етапом для поширення дезінформації та впливу на громадян.

Одним з векторів є атаки на провайдерів з метою підміни телевізійного сигналу. Зокрема, напередодні Нового 2025 року було зафіксовано гібридну атаку, під час якої трансляцію українських каналів замінили фейковим повідомленням про підготовку удару балістичними ракетами «Орєшнік», що мало на меті масштабувати суспільну тривогу.

В іншій атаці для просування наративу про «втому Заходу» та припинення підтримки України було використано Viber-канал інтернет-провайдера, де було розміщено фейк про нібито перехід регіональних провайдерів під юрисдикцію рф внаслідок вигаданих домовленостей між лідерами США та росії. Щоб отримати доступ до корпоративного каналу, зловмисники з використанням інфостілера скомпрометували особисті акаунти працівника компанії.

В рамках постійної інформаційної кампанії із дискредитації Сил оборони України командирам військових частин розсилали листи з фальшивими повідомленнями про те, що їх військовослужбовці розповсюджують наркотики серед цивільного населення. До таких емоційних листів нібито від родичів додавалися архіви з «доказами», що експлуатували вразливість WinRAR (CVE-2025-6218) для встановлення інфостілера Vidar.

На підтримку комплексної кампанії проти українського сектору оборонних технологій псевдохактивістські групи KillNet та «Берегині» синхронно заявляли про нібито злам серверів компанії «Бойові Птахи України» і витік секретних розробок. У межах цієї операції зловмисники стверджували про компрометацію бази даних виробників БПЛА, а також заявляли про доступ до платформи Brave1 та Українського фонду стартапів.

У 2025 році продовжилась системна робота рф щодо зміни сприйняття на міжнародному рівні її ролі у кіберпросторі та **формування образу «жертви» кібервійни**. Для цього використовуються звіти підконтрольних підсанкційних компаній (таких як F.A.C.C.T., Positive Technologies, Лабораторія Касперського), в яких описуються численні атаки нібито українських хакерів на цивільну інфраструктуру рф, а також Європи. Зокрема низка російських звітів безпідставно атрибутували атаки на польську інфраструктуру до діяльності українських груп з метою дискредитації України та створення підґрунтя для звинувачень у порушенні норм міжнародного права.

росія проводить кібератаки та гібридні операції проти країн ЄС та НАТО **«під чужим прапором»**, намагаючись видати їх за дії України або пов'язаних з нею груп. Яскравим прикладом є інцидент із кібератакою на кадастрові системи Словаччини, де проросійські сили намагалися знайти «український слід». Російські хакерські групи, зокрема UAC-0050, вдаються до мімікрії під українських активістів. Вони здійснюють розсилки шкідливого програмного забезпечення та DDoS-атаки на європейські організації, використовуючи символіку та гасла «IT Army of Ukraine». Це робиться для того, щоб знизити рівень міжнародної підтримки України, а також сформувати хибне уявлення про Україну як про «ненадійного партнера» та джерело кіберзагроз для Європи.

У 2025 році суттєво загострилася проблема ІТ-тероризму, що проявляється у **масовій розсилці фіктивних повідомлень про мінування**. Близько 70% таких загроз надходять із території РФ або тимчасово окупованих територій і мають на меті дестабілізацію ситуації в Україні. Для здійснення розсилок залучають ресурси підконтрольних груп кіберзлочинців, зокрема UAC-0050. Характерною особливістю звітного періоду стало значне збільшення кількості таких повідомлень та поява нових підходів, зокрема масового «мінування» потягів

міського та міжнародного сполучення. Для розсилок використовуються анонімні електронні скриньки, за один раз розсилаються погрози для десятків різних об'єктів, що змушує правоохоронців залучати значні ресурси для перевірки кожної локації. Для дискредитації Сил оборони такі розсилки часто здійснюються нібито від імені колишніх військовослужбовців.

Фінансово-мотивована активність

У 2025 році спостерігалося подальше зростання кількості кіберзлочинів та інцидентів, пов'язаних з діяльністю фінансово-мотивованих груп. Основним чинником цієї тенденції стала складна ситуація в країні: велика кількість людей, які потребують соціальної допомоги, стали мішенню для шахраїв, які маскувалися під урядові програми допомоги, благодійні та міжнародні організації. Також на зростання злочинності суттєво впливала агресія з боку рф. Ворог активно використовував кіберзлочинців як інструмент у війні, спрямовуючи їхні зусилля на викрадення даних та коштів українських громадян та організацій. Таким чином, активізація кіберзлочинності у 2025 році була зумовлена як прагненням зловмисників до незаконного збагачення на гуманітарних потребах населення, так і зовнішнім втручанням з метою дестабілізації цифрового простору України.

За даними Департаменту кіберполіції Національної поліції України[31], у 2025 році зареєстровано 4 539 подій онлайн-шахрайств з використанням платіжних реквізитів, виявлено та заблоковано 72 803 фішингових доменів, що використовувались кіберзлочинцями. Кіберполіція опрацювала 57,4 тис. звернень громадян через сайт та 30,5 тис. вхідних дзвінків від громадян. Впродовж року підрозділами кіберполіції було зареєстровано понад 2,1 тисяч кримінальних правопорушень, закінчено розслідування та скеровано до суду понад 2,7 тис. кримінальних правопорушень. Постраждалим було відшкодовано понад 342,6 млн грн.

Основними загрозами залишаються масовані розсилки шкідливого ПЗ для викрадення коштів, фішинг під виглядом допомоги від держави, благодійних фондів та міжнародних організацій, атаки вірусів-шифрувальників на бізнес.

Основні тенденції та тактики

В атаках на організації, метою яких є викрадення коштів, найчастіше використовувалися **масові розсилки фішингових електронних листів**, що імітували переписку з контрагентами та надсилання фінансових документів (рахунків, договорів, платіжних інструкцій тощо). Метою цих атак є отримання доступу до систем дистанційного банківського обслуговування з подальшим створенням несанкціонованих платежів.

Такі масові розсилки зазвичай здійснювалися з попередньо скомпрометованих адрес приватних компаній або державних органів. Для обходу засобів захисту використовуються архіви з паролями, файли образів (IMG, ISO), або посилання на легальні сервіси Dropbox, Google Drive, OneDrive, Bitbucket або 4Sync. Архіви і посилання містять файли-приманки PDF, а також документи з макросами, виконувані файли, LNK-файли чи JS-скрипти, призначені для завантаження наступних стадій шкідливого програмного забезпечення.

Технічний арсенал зловмисників включає широкий спектр шкідливого ПЗ, зокрема інструменти віддаленого доступу (RAT) та інфостілери: NetSupport RAT, Remcos RAT, DarkCrystal RAT, FormBook, Snake Keylogger, AgentTesla, а також завантажувачі IDAT Loader та GuLoader. Використання таких інструментів дозволяє зловмисникам повністю контролювати інфікований пристрій, досліджувати систему на наявність цінної фінансової інформації та здійснювати приховане викрадення конфіденційних даних.

Для підвищення рівня довіри у назвах файлів-приманок використовуються бренди відомих українських банків та великих компаній. У другій половині року група UAC-0050 підвищила персоніфікацію фішингу, додавши до теми листів назву атакованої організації.

Для громадян, насамперед внутрішньо переміщених осіб, основну загрозу створюють **фішингові сайти, що експлуатують тему соціальних виплат та компенсацій**. Зловмисники

[31] https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/

маскували свої ресурси під офіційні державні портали, такі як «Дія», «єДопомога», «Зимова єПідтримка», «єВідновлення», а також під урядовий Портал Кабінету Міністрів, Портал гуманітарної допомоги. Для введення в оману вони використовували айдентику і логотипи популярних українських банків. Також активно поширювались шахрайські схеми з використанням ресурсів, стилізованих під OLX, Укрпошту, Нову Пошту, АТБ, WOG, ДТЕК.

Основними майданчиками для поширення шахрайських посилань стали соціальні мережі та месенджери, зокрема Facebook, Telegram, Instagram, TikTok, Viber та WhatsApp. Через канали, боти та групи зловмисники масово розсилають повідомлення, що заманюють користувачів обіцянками виплат. Метою таких атак є викрадення платіжних даних або отримання доступу до онлайн-банкінгу громадян під виглядом авторизації на фейкових ресурсах.

Спостерігалася тенденція розміщення шахрайських ресурсів на легальних публічних хостинг-платформах, зокрема Cloudflare Pages, Cloudflare Workers, Deno Deploy, Railway.

У другому півріччі 2025 року зафіксовано **кібератаки з використанням вірусів-вимагачів (ransomware)**[32], спрямовані на шифрування даних та вимагання викупу. Зокрема, група UAC-0238 атакувала органи місцевого самоврядування, отримуючи доступ до комп'ютерів через протокол віддаленого робочого столу (RDP). Зловмисники використовували шкідливе програмне забезпечення сімейства Proton для шифрування файлів у системах Windows, попередньо видаляючи тіньові копії операційної системи, щоб унеможливити відновлення даних.

Інше угруповання, UAC-0243, використовувало вразливості серверів Microsoft SharePoint як точку входу до локальних мереж організацій. Для безпосереднього шифрування даних вони застосовували програму X2anylock (Warlock), що є варіацією LockBit 3.0. Для закріплення в системі, горизонтального переміщення мережею та викрадення великих масивів даних хакери використовували низку легітимних сервісів та утиліт, в тому числі Cloudflare Tunnel, Velociraptor та RClone, що дозволяло їм маскувати свою активність під звичайні робочі процеси.

Окрему загрозу становили **фішингові операції**, що підтримуються спецслужбами рф та спрямовані на **збір даних про військовослужбовців** Сил оборони України. Ворог створював сайти-двійники благодійних фондів, які нібито пропонують допомогу військовослужбовцям та їхнім родинам. Такі ресурси містять детальні анкети, де користувачів спонукають завантажувати фото військових квитків, вказувати місця проходження служби та надавати іншу конфіденційну інформацію.

Діяльність хактивістів

Проросійські псевдохактивістські групи функціонують як інструмент прикриття («проксі») для кадрових спецслужб рф. Офіційні звіти[33] [34] підтверджують їхній прямий зв'язок із російськими силовими структурами: зокрема, діяльність групи Cyber Army of Russia Reborn курується підрозділом ГРУ (в/ч 74455), а NoName057(16) – підконтрольним кремлю Центром молодіжних ініціатив. Головною метою використання таких груп є забезпечення правдоподібного заперечення причетності держави-агресора до міжнародних кібердиверсій та проведення інформаційних операцій і кібероперацій «під чужим прапором».

Географія атак свідчить про їхню стратегічну орієнтацію на країни ЄС та НАТО. Протягом 2025 року більшість атак була спрямована на інфраструктуру демократичних країн Заходу (Польща, Німеччина, Франція, Італія, Іспанія, Литва тощо), тоді як безпосередньо з Україною були пов'язані лише 10-20% інцидентів. Діяльність груп часто синхронізувалося з важливими геополітичними подіями, такими як підготовка до виборів у демократичних країнах, з метою дестабілізації суспільно-політичної ситуації. В Україні їхніми мішенями

[32] https://cip.gov.ua/services/cm/api/attachment/download?id=74646
[33] https://www.cisa.gov/sites/default/files/2025-12/aa25-343a-pro-russia-hacktivists-conduct-attacks_0.pdf
[34] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a?utm_source=AA25-343a&utm_medium=PressRelease

найчастіше ставали підприємства оборонно-промислового комплексу, банки, логістичні компанії та місцеві органи влади.

Основні тенденції та тактики

У 2025 році постерігалася небезпечна еволюція тактик псевдохактивістів: до базових **DDoS-атак** та **дефейсів** вебсайтів вони додали цілеспрямовані **злами промислових систем управління** (OT/ICS) на підприємствах критичної інфраструктури. У секторах енергетики, водопостачання та сільського господарства зловмисники сканували мережі на наявність відкритих портів дистанційного доступу VNC та використовували техніку **підбору паролів** для доступу до інтерфейсів управління. Метою таких дій є маніпуляція технологічними процесами, що може призвести до фізичного пошкодження критичної інфраструктури.

Діяльність псевдохактивістів глибоко інтегрована у російські **інформаційно-психологічні операції**. Групи створювали публічні альянси для масштабування публічного резонансу та активно публікували у Telegram-каналах заяви про витоки даних і злами. В більшості випадків їхні заяви були перебільшеними або фейковими: наприклад, злам системи-приманки (honeypot) видавався за реальну атаку на водоочисну станцію, а втрата окремого файлу з контактами видавалася за злам державних баз даних виробників БПЛА. Це робиться для створення ефекту паніки, тиску на суспільство та штучного завищення власних спроможностей.

Аналіз заяв російських псевдохактивістських груп (CARR, NoName057(16), Z-Pentest, Берегині та інших) свідчить про те, що їхня діяльність у 2025 році в більшості випадків була інструментом стратегічних комунікацій та ІПСО.

Більшість їх заяв про «злам критичної інфраструктури» були перебільшеними. Часто ці групи демонстрували доступ до другорядних систем або панелей керування, які не мають прямого впливу на технологічні процеси, але виглядали ефектно на відео. У багатьох випадках «злам енергосистеми» на практиці виявлявся лише зміною назви заставки на моніторі або отриманням доступу до офісного принтера. Такі групи, як «Берегині» та «Джокер ДНР», зазвичай не «зламували» складні системи самостійно. Їхня роль – бути майданчиком для «зливу» інформації, яку вже здобули інші APT-групи. Це робиться з метою створити ілюзію масового внутрішнього супротиву в Україні та технічної всемогутності «народних російських хакерів».

Вразливості

У 2025 році експлуатація програмних та апаратних вразливостей залишалася одним із ключових векторів проникнення, який використовувався як пов'язаними з спецслужбами APT групами, так і фінансово мотивованими кіберзлочинцями. Тенденцією стало значне скорочення часу від публікації інформації про вразливість до її експлуатації в атаках на інформаційні системи. При цьому активно використовувались і давно відомі вразливості, для яких виправлення доступні вже декілька років.

Значна частина атак була зосереджена на популярному програмному забезпеченні для кінцевих користувачів. Групи UAC-0010 (Gamaredon), UAC-0002 (Sandworm) та UAC-0180 (RomCom) масово використовували критичні вразливості в архіваторі WinRAR (CVE-2025-6218, CVE-2025-8088) для прихованого встановлення шкідливого коду через фішингові електронні листи. Крім того, на початку року група UAC-0006 успішно застосовувала вразливість «нульового дня» CVE-2025-0411 в архіваторі 7zip з метою обходу засобів антивірусного захисту.

Фінансово мотивовані групи систематично використовували «старі» вразливості в Microsoft Office (CVE-2017-11882, CVE-2017-0199), виявлені ще у 2017 році, для масового розповсюдження шкідливого програмного забезпечення (Remcos RAT, Formbook, Snake Keylogger, LokiBot, XWorm).

Корпоративні поштові сервери стали пріоритетною ціллю для масштабного кібершпигунства. Зловмисники активно експлуатували XSS-вразливості у серверах Zimbra

(CVE-2025-48700) та Roundcube (CVE-2024-42009, CVE-2024-37383, CVE-2025-49113) за допомогою спеціально сформованих листів. Успішна експлуатація цих вразливостей дозволяла зловмисникам перехоплювати токени авторизації, обходити двофакторну автентифікацію та приховано ексфільтрувати архіви листування й адресні книги користувачів.

Критичною загрозою для організацій стали атаки на мережеве обладнання та шлюзи віддаленого доступу. Вразливості в пристроях Fortinet (CVE-2024-55591, CVE-2024-21762, CVE-2025-24472) системно експлуатувалися для отримання доступу до конфігурацій та створення точок входу для подальшого просування в мережах.

У жовтні фіксувалася глобальна кампанія з експлуатації вразливостей «нульового дня» (CVE-2025-20333, CVE-2025-20362) у VPN-шлюзах Cisco ASA/AnyConnect для встановлення буткітів. Критична вразливість із максимальним рейтингом небезпеки 10/10 (CVE-2025-49844) у базах даних Redis створювала ризик віддаленого виконання коду на сотнях українських серверів. Також було виявлено критичні вразливості у серверній імплементації протоколу захищеного месенджера Matrix (CVE-2025-49090, CVE-2025-54315), що потенційно дозволяли зловмисникам несанкціоновано приєднуватися до закритих військових та корпоративних чатів.

Підкластер Sandworm (UAC-0212) використовуваув вразливість CVE-2024-38213 в ході атак на автоматизовані системи управління технологічними процесами.

Окремим стратегічним вектором стали таргетовані атаки на мобільні пристрої посадовців та системи захищених комунікацій. Вразливість «нульового дня» (CVE-2025-43300) в операційних системах Apple iOS та macOS застосовувалася у високопрофільних атаках на надпріоритетні для ворога цілі.

Оцінка впливу кіберзагроз

У більшості випадків українські організації не оцінюють масштаб збитків та наслідків кібератак, обмежуючись заходами із відновлення після інциденту, або не роблять таку інформацію доступною публічно.

Для оцінки загальних наслідків кібератак використані результати опитування 317 експертів, які представляли державні органи, обласні військові адміністрації і органи місцевого самоврядування, Сили оборони України. В рамках опитування було запропоновано надати оцінку наскільки суттєвими були наслідки кібератак на українську інфраструктуру у 2025 році за шкалою від 0 до 5 балів.

Для цілей дослідження в рамках цього звіту були обрані наступні види наслідків кіберінцидентів:

- Цифрові наслідки, що стосуються недоступності систем, пошкодження даних або витоків інформації.
- Економічні наслідки, що стосуються прямих і непрямих фінансових втрат.
- Соціальні наслідки, що стосуються втрати довіри внаслідок порушення важливих публічних сервісів, або витоку персональних даних громадян.
- Репутаційні наслідки, що стосуються можливого негативного сприйняття громадськістю організації, яка стала жертвою кіберінциденту.
- Фізичні наслідки, що стосуються травм чи шкоди громадянам.

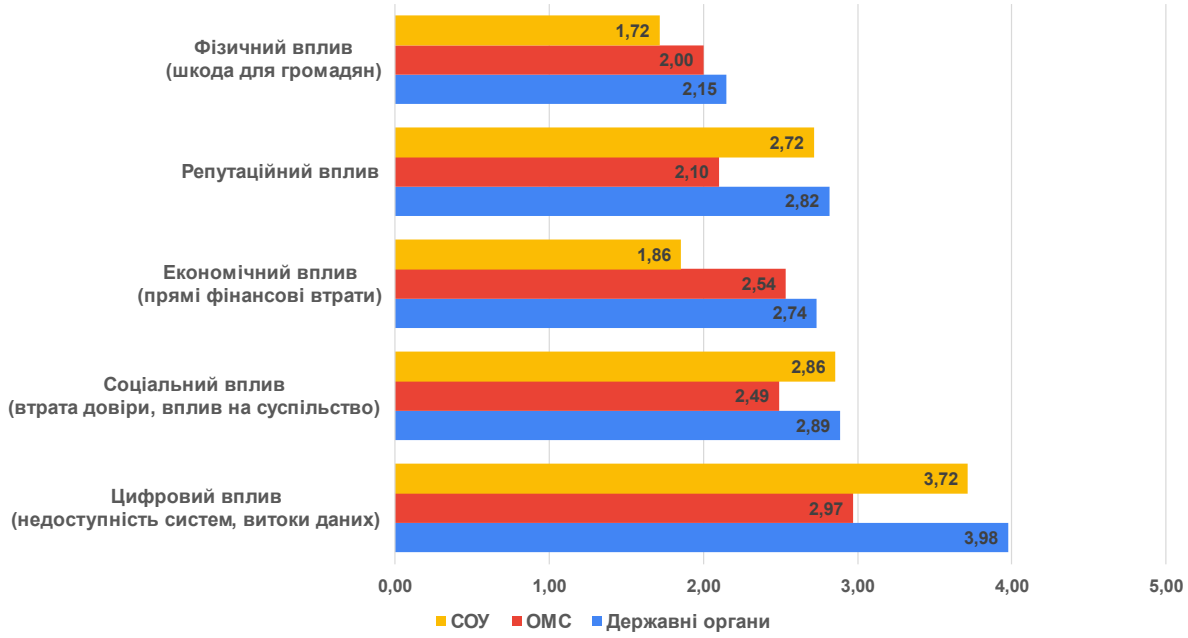


Рис 1.Оцінка наслідків реалізації кіберзагроз

Найбільшими наслідками від кібератак в 2025 році є цифрові наслідки; соціальні, економічні та репутаційні втрати вважаються менш важливими; фізичні наслідки кібератак не розглядаються як суттєві.

Незважаючи на спільний загальний тренд, існує різниця в оцінці наслідків між центральними і регіональними державними органами, Силами оборони України. Регіональні органи влади загалом набагато нижче за інші категорії респондентів оцінюють наслідки кібератак, що свідчить про недостатню обізнаність про ризики кібербезпеки. Сили оборони помітно нижче оцінюють економічний та фізичний вплив кібератак, що ймовірно пов'язано із значно вищими ризиками фізичних наслідків внаслідок бойових дій.

Ключові тенденції та висновки

Перехід до тотальної кібервійни.

У 2025 році кібервійна РФ проти України перейшла у фазу тотального системного протистояння. Кібератаки і операції є частиною єдиної стратегії з чітким розподілом завдань між спецслужбами, кіберкриміналом та псевдохактивістами. Завдяки нарощенню кадрового і аналітичного потенціалу та вдосконаленню планування, ворог здійснює безперервний скоординований тиск на Сили оборони, державу, приватний сектор; кібер- та інформаційний вплив на громадян. Це демонструє значний контраст з інтенсивними, але хаотичними кібератаками «по площах» на початку повномасштабного вторгнення у 2022 році.

Пріоритезація розвідувальних операцій

Російські кібероперації у 2025 році змістили фокус із деструктивних атак на стратегічне шпигунство. Ключовим пріоритетом ворога стало отримання доступу та закріплення в інформаційних мережах держорганів, критичної інфраструктури та військових системах керування. Збір розвідувальних даних у реальному часі у 2025 році був пріоритетнішим за деструктивні дії. Великі деструктивні атаки проводилися нечасто і мали на меті переважно інформаційно-психологічний вплив. Така зміна стратегії зробила загрози менш помітними, але значно небезпечнішими, оскільки активність агресора стала більш «тихою» та складнішою для виявлення.

Конвергенція акторів загроз

Ландшафт загроз характеризується конвергенцією різних груп зловмисників під егідою російських спецслужб. Межа між державними APT-групами, фінансово мотивованими злочинцями та хактивістами практично розмилася. Спецслужби рф забезпечують криміналітету «дах» та сучасний інструментарій («кіберзброю») в обмін на розширення масштабів атак і доступ до розвідувальних даних. Водночас російський хактивізм остаточно перетворився на контрольований державою проєкт для інформаційних операцій, де учасники дедалі більше фокусуються на монетизації своєї діяльності під прикриттям державних інтересів.

Еволюція соціальної інженерії

Кібератаки з використанням соціальної інженерії трансформувалася завдяки поєднанню людського досвіду та технологій штучного інтелекту. Залучення (мобілізація, вербовка) фахівців із різних галузей – від IT-сектору до професійних шахраїв – посилило спроможності росії реалізовувати складні та креативні сценарії атак, адаптовані під конкретні цільові аудиторії. У поєднанні із використанням інструментів аналізу великих даних та ШІ це дозволило проводити унікальні таргетовані кампанії, спрямовані на конкретних посадових осіб або громадян. У 2025 році значно зріс рівень персоніфікації фішингових атак, зробивши їх складнішими для виявлення та протидії.

Експансія інфостілерів

У 2025 році зросло застосування інфостілерів та збільшилась кількість випадків компрометації облікових записів. Такий метод проникнення у мережі дозволяє уникнути складних технічних атак на периметр, а викрадення токенів авторизації дозволяє обходити навіть багатофакторну автентифікацію. Попит на скомпрометовані облікові дані та доступи стимулював розвиток кримінальної екосистеми: російські спецслужби дедалі частіше виступали кінцевими споживачами послуг «брокерів доступу» (access brokers).

Асиметрія застосування ШІ

Штучний інтелект створює суттєвий дисбаланс у кіберпросторі, надаючи атакуючій стороні стратегічну перевагу. Кібератаки з використанням ШІ демонструють гнучкість у зміні тактик, здатність миттєво обробляти великі масиви даних, надзвичайний потенціал для автоматизації. Натомість у сфері захисту потенціал ШІ був обмежений переважно оптимізацією рутинних задач аналітиків у межах локальних периметрів. Цей розрив посилюється через недостатнє врахування розробниками захисних систем реалій сучасної кібервійни, що робить ШІ більше інструментом прориву для наступу, ніж ефективним засобом підтримки для захисту.

Прогноз загроз 2026 року

Російські хакерські групи залишатимуться головним джерелом загроз для національної системи кібербезпеки України. Очікується високий рівень інтенсивності кібератак на Сили оборони України, державні органи, підприємства критичної інфраструктури. Зростатиме кількість кібератак на фінансову систему, у секторі охорони здоров’я, агропромисловому секторі, оборонній промисловості.

Зростаючий глобальний попит на безпекові та оборонні рішення зробить розробників і виробників високотехнологічної зброї, технологій подвійного призначення (dual-use) та оборонних технологій (mil-tech) пріоритетними цілями. Розшириться коло акторів і їх мотивація. Окрім воєнних цілей, які переслідуватимуть російські спецслужби, актори загроз з інших країн та кіберзлочинці будуть здійснювати атаки з іншою мотивацією: викрадення

інтелектуальної власності, конкурентна боротьба, впровадження «закладок» і вразливостей для подальшої експлуатації в ході бойових дій тощо.

Продовжиться еволюція методів соціальної інженерії, зросте застосування дипфейків (голос, відео) у складних фішингових атаках. Використання генеративних моделей ШІ дозволить автоматизувати створення індивідувальних фішингових сценаріїв одночасно для великої кількості цілей.

Збережеться тенденція використання легальних сервісів для розміщення командно-контрольної інфраструктури та ексфільтрації даних з метою обходу засобів захисту. Також розвиватиметься екосистема скомпрометованих облікових даних, включаючи API доступи до сервісів та пристроїв (ботів), які будуть формувати приховані децентралізовані мережі для проведення кібератак та ускладнення атрибуції.

Посилиться тенденція збільшення кібератак на мобільні пристрої та компрометації месенджерів та інших застосунків.

Штучний інтелект стане основним інструментом масштабування атак. Автономні ШІ агенти будуть використовуватись для здійснення комплексних багатоетапних атак, від проведення попередньої розвідки і профілювання цілей до планування та проведення операцій, включаючи пошук вразливостей і помилок конфігурації, розробку експлойтів, методів «тихого» просування в мережі тощо.

росія продовжить нарощувати кіберактивність та інформаційні операції проти країн ЄС і НАТО, розглядаючи їх як атаки на глобальні ланцюги постачання для завдання шкоди Україні.

VI. ЗАХИСТ КРИТИЧНОЇ ІНФРАСТУРКТУРИ ТА КЛЮЧОВІ КІБЕРІНЦИДЕНТИ

З початку повномасштабного вторгнення об’єкти критичної інфраструктури (ОКІ) України залишаються головною ціллю для російських кібератак, оскільки їхнє пошкодження має безпосередній вплив на життєдіяльність усього суспільства та обороноздатність держави. Серед найбільш атакованих секторів – енергетика, електронні комунікації, системи життєзабезпечення, транспорт, державні органи, публічні сервіси.

Наймасштабніші атаки останніх років були спрямовані саме на організації, які працюють у цих секторах – кібератака на Укрзалізницю (березень 2025 року) для пошкодження залізничних перевезень; деструктивні атаки на об'єкти енергетики та теплопостачання в ряді регіонів України (лютий 2025 року); спроба знищення даних у Єдиних і Державних реєстрах Мінюсту (грудень 2024 року); зникнення зв'язку у понад 24 мільйонів абонентів внаслідок кібератаки на Київстар (грудень 2023 року).

Слід зазначити, що дані про об'єкти критичної інфраструктури є інформацією з обмеженим доступом, тому публічно доступні лише узагальнені дані щодо переліку ОКІ. За даними Державної служби спеціального зв'язку і захисту інформації України[35], яка є уповноваженим органом у сфері захисту критичної інфраструктури України, ключовим інструментом для єдиного обліку та категоризації є Реєстр об'єктів критичної інфраструктури. Станом на кінець 2025 року до Реєстру внесено відомості про понад 4600 об'єктів, протягом останнього року до Реєстру було додано 2046 нових об'єктів, що свідчить про активну роботу секторальних органів з ідентифікації критичних активів. Облік ведеться за 24 секторами критичної інфраструктури, а об'єктам присвоюється одна з чотирьох категорій критичності, що визначає рівень вимог до їх захисту. Погоджено 1306 паспортів безпеки на ОКІ, наявність яких є обов'язковою для об'єктів 1-ї та 2-ї категорій критичності.

[35] https://cip.gov.ua/ua/news/do-reyestru-ob-yektiv-kritichnoyi-infrastrukturi-vzhe-vneseno-vidomosti-pro-ponad-4600-ob-yektiv

Аналітичні матеріали Держспецзв'язку[36] за 2024–2025 роки демонструють тенденцію, що незважаючи постійне зростання сумарної кількості кіберінцидентів, кількість успішних кібератак високого та критичного рівнів постійно зменшується. Завдяки співпраці об'єктів критичної інфраструктури з основними суб'єктами забезпечення кібербезпекиі більшість спрямованих на ОКІ кібероперацій вдається нейтралізувати на ранніх етапах. У 2024 році кількість інцидентів критичного та високого рівнів за рік склала 59 випадків, у 2025 році вона зменшилась на 80% до 12 випадків. При цьому у другому півріччі 2025 року не було зафіксовано жодного критичного інциденту, а інцидентів високого рівня стало лише 5.

Українська держава приділяє пріоритетну увагу кіберзахисту критичної інфраструктури, переходячи від суто регуляторного нагляду до моделі активного партнерства з операторами стратегічних об'єктів. Окрім розробки нормативних вимог та стандартів, державні органи забезпечують глибоку інтеграцію підприємств у національну систему кібербезпеки. Це передбачає не лише контроль за дотриманням правил, а й створення єдиного інформаційного простору для оперативного обміну даними про загрози.

Практична допомога від держави включає надання конкретних технічних послуг, спрямованих на безпосереднє зміцнення кіберстійкості підприємств.

Підрозділи Служби безпеки України, Держспецзв'язку забезпечують постійний моніторинг подій безпеки на пріоритетних об'єктах критичної інфраструктури, надають фахову підтримку у реагуванні на інциденти, відновленні після кібератак, методичну допомогу у проведенні інвентаризації активів та оцінок стану захищеності. Державним центром кіберзахисту Держспецзв'язку забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. У 2025 році до підсистеми збору телеметрії системи було підключено 24 нових організацій[37], яким надано сенсори для для моніторингу мережевого трафіку. Для 97 організацій забезпечено захист кінцевих точок, у результаті чого здійснюється моніторинг подій безпеки понад 46,5 тисяч робочих станцій і серверів. Це дозволило попередити 730 кіберінцидентів різного рівня складності.

Внаслідок моніторингу і аналізу майже 290 мільярдів подій безпеки у інформаційних системах об'єктів критичної інфраструктури та державних органів Ситуаційним центром забезпечення кібербезпеки СБУ у 2025 році виявлено та нейтралізовано 1169 кіберзагроз високого рівня критичності[38], припинено 3010 критичних кіберінцидентів та кібератак.

У секторі фінансової та банківської діяльності у 2025 році командою реагування на кіберінциденти в банківській системі України CSIRT-NBU виявлено та проведено аналіз близько 2 тис. зразків шкідливого програмного забезпечення та своєчасно поінформовано банки України про виявлені інциденти кібербезпеки й зафіксовані спроби вчинення кібератак. На платформі обміну інформацією про актуальні кіберзагрози MISP-NBU, до якої підключено 60 банків та ключові небанківські фінансові установи, було надіслано 340 повідомлень про кіберінциденти та індикатори кіберзагроз.

Завдяки скоординованій роботі основних суб'єктів забезпечення кібербезпеки підприємства критичної інфраструктури на постійній основі отримують аналітику кіберзагроз, актуальні індикатори компрометації та методичні рекомендації, що дозволяють виявляти підготовку кібератак на ранніх етапах. Держава також пропонує сервіси з регулярного сканування зовнішніх мереж на наявність вразливостей, допомагає у проведенні стрес-тестів систем та організовує навчання та тренінги для керівників і технічного персоналу об'єктів критичної інфраструктури.

Такий комплексний підхід, що поєднує методичну допомогу із безпосереднім технічним супроводом, дозволяє підприємствам ефективніше адаптувати свої системи кіберзахисту до сучасних викликів.

Ключові виклики кібербезпеки критичної інфраструктури:

[36] https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku
[37] https://cip.gov.ua/services/cm/api/attachment/download?id=73033
[38] https://www.facebook.com/cybercentresbu/posts/846904218314422

Атаки на ланцюги постачання. Через постійне зростання рівня кіберзахисту, безпосередні атаки на об'єкти критичної інфраструктури стали значно складнішими. Тому актори загроз компрометують постачальників спеціалізованого програмного забезпечення або IT-послуг для критичної інфраструктури, які часто мають слабший кіберзахист.

Технологічні вразливості та застарілі системи. У промислових системах управління все ще використовуються застарілі версії операційних систем (Windows XP, Windows 7), що спрощує експлуатацію вразливостей. Поширення пристроїв інтернету речей (IoT) створює додаткові точки входу для проникнення в корпоративні мережі через їхній слабкий захист.

Кадрові і фінансові виклики. Плинність кадрів та недостатній рівень кібергігієни персоналу залишаються критичними факторами. Спостерігається системний брак фінансування кіберзахисту на об'єктах як в державному, так і в приватному секторі, а фрагментація ринку заважає створенню єдиної національної екосистеми.

Регуляторне навантаження. Зростання кількості нормативних вимог та часткова неузгодженість між нормативною базою в сфері кібербезпеки і в сфері захисту критичної інфраструктури створює додаткове навантаження на організації. Внаслідок цього частина критичних приватних підприємств відмовляється отримувати статус ОКІ або штучно занижує категорію критичності, що визначає рівень вимог до їх захисту.

Синхронізація кінетичних і кібератак. Ворог систематично координує кібератаки на критичну інфраструктуру із масованими ракетно-дроновими обстрілами. Це робиться для максимального деструктивного впливу, перешкоджання логістиці та ускладнення своєчасного реагування та відновлення.

Серед найбільш критичних кібератак, які відбулися у 2025 році, слід відмітити березневу кібератаку на АТ «Укрзалізниця», яка вплинула на надання онлайн сервісів споживачам.

Хронологія та наслідки: 23 березня 2025 року було зафіксовано збій в IT-системах Укрзалізниці, що вивів з ладу сервіси онлайн-продажу квитків, вебсайт та мобільний застосунок. Пасажири були змушені купувати паперові квитки в касах, що призвело до значних черг на вокзалах. Відновлення базових онлайн-сервісів (у резервному режимі) зайняло близько 89 годин, а поетапне відновлення функціоналу тривало кілька тижнів. Незважаючи на припинення роботи частини IT-систем, рух поїздів не зупинився. Витоку чутливих даних не відбулося, а на етапі відновлення CERT-UA та СБУ додатково перевірили резервні копії на наявність вразливостей та ворожих «закладок». 8 травня 2025 року було оголошено про повне завершення робіт з усунення наслідків та повернення до штатного режиму розрахунків за перевезення.

Мета та технологія: Атака мала багаторівневий комплексний характер і була спрямована на руйнування доступності сервісів. Метою атаки була дестабілізація ключового транспортного оператора України, порушення логістики (пасажирські та вантажні перевезення), підірив довіри населення та створення соціальної напруги як елемент гібридної війни.

Атрибуція: кластер загроз, пов'язаний із UAC-0002 (Sandworm), інцидент класифікується як акт кібертероризму.

Також у 2025 році відбулося 2 значні кібератаки на банківський сектор України: компрометація таємного ключа СЕП банку через вразливий веб-застосунок із подальшою спробою повторної атаки після зміни ключів та деструктивна атака на один із банків із безповоротним знищенням даних через заміну вмісту файлів на послідовність «zov» (включно з пошкодженням усіх резервних копій). Разом із тим, в наслідок скоординованого та оперативного реагування, ці кібератаки не мали суттєвого негативного впливу на банківсько-фінансовий сектор України.

VII. СТАН РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни»[39] було схвалено рішенням Ради національної безпеки і оборони України від 14 травня 2021 року та введено в дію Указом Президента України № 447/2021 від 26 серпня 2021 року.

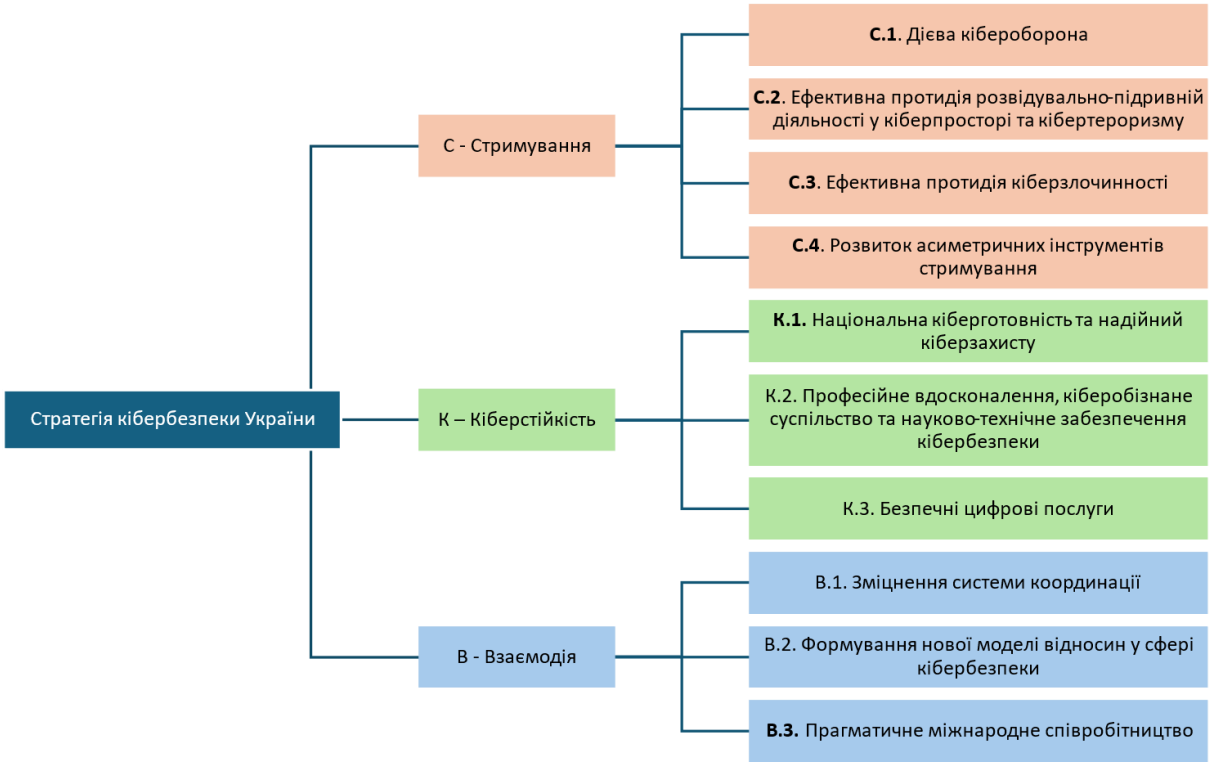
З одного боку, документ став відповіддю на стрімку цифровізацію світу, зумовлену, зокрема, пандемією COVID-19, та активні процеси цифрової трансформації в Україні, що змінили соціальну поведінку та економічні процеси (дистанційна робота, хмарні сервіси, сервіси Дія). З іншого боку Стратегія чітко визначила серед основних загроз збройну агресію рф (використання кібератак як інструменту збройної агресії, проведення розвідувально-підривної діяльності, кібершпигунства та поширення дезінформації), що дозволило сфокусуватись на стримуванні ворога в кіберпросторі та в подальшому забезпечити кіберстійкість державних органів та критичної інфраструктури під час повномасштабного вторгнення рф в Україну. Кібербезпека була визнана одним із пріоритетних завдань держави та ключовим компонентом національної оборони в умовах триваючої агресії рф.

Координатором реалізації Стратегії визначено Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України. План реалізації Стратегії[40], розроблений НКЦК та схвалений рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року, уведеним в дію Указом Президента України від 1 лютого 2022 року № 37/2022, є основою для щорічного планування заходів з реалізації Стратегії. Кабінетом Міністрів України було доручено Адміністрації Держспецзв'язку готувати щорічні плани заходів з реалізації Стратегії кібербезпеки України та надавати кожні півроку до Кабінету Міністрів України та Апарату Ради національної безпеки і оборони України зведену інформацію про стан виконання Плану реалізації Стратегії. На виконання доручення у 2025 році Адміністрацією Держспецзв’язку підготовлено та затверджено Кабінетом Міністрів України розпорядження[41] від 7 березня 2025 року №204-р «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України» та підготовлено аналітичний звіт[42] про стан виконання Плану реалізації Стратегії.

Стратегія кібербезпеки України передбачає три основних напрями, які поділяються на 10 стратегічних цілей, кожна з яких передбачає виконання ряду завдань. Загалом План реалізації Стратегії визначає 94 завдання, виконання яких спрямоване на досягнення стратегічних цілей Стратегії.

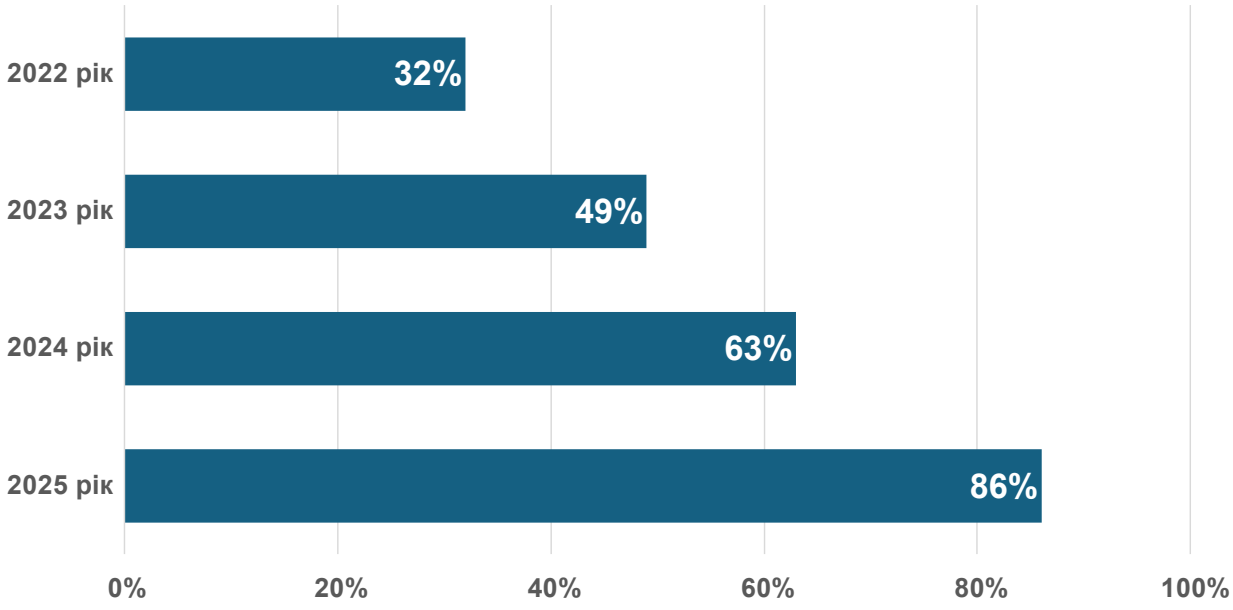
Структурну схему Стратегії наведено на рисунку.

[39] https://zakon.rada.gov.ua/laws/show/447/2021#Text
[40] https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
[41] https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text
[42] https://cip.gov.ua/services/cm/api/attachment/download?id=73801



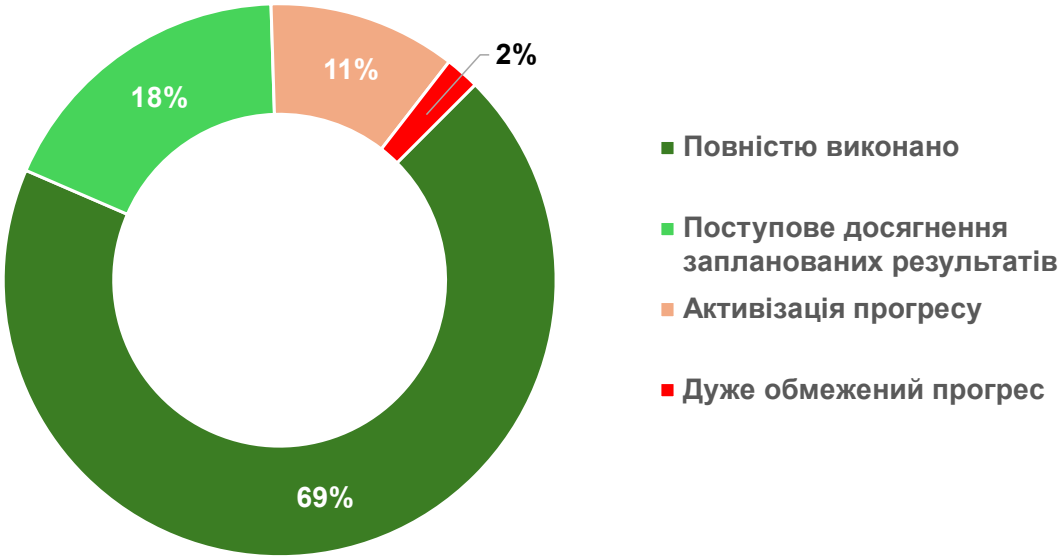
Станом на кінець 2025 року загальний показник реалізації Стратегії складає 86%. При цьому стала позитивна динаміка спостерігається впродовж всього терміну виконання Стратегії – від 32% у 2022 році до 86% у 2025 році. Це є свідченням того, що національна система кібербезпеки успішно пройшла шлях від становлення до зрілості, навіть в умовах екстремальних викликів воєнного часу.

На рисунку наведено діаграму стану виконання Стратегії за 2022-2025 року.



Ключові статистичні показники реалізації станом на 2025 рік:

- **Загальна кількість завдань**: 94 (з них 93 підлягали оцінці);
- **Повністю виконано**: 64 завдання (69%);
- **Поступове досягнення запланованих результатів**: 17 завдань (18%);
- **Активізація прогресу**: 10 завдань (11%);
- **Дуже обмежений прогрес**: 2 завдання (2%);



Враховуючи п’ятирічний цикл планування та швидкі зміни у безпековому середовищі у сфері кібербезпеки, на момент розробки чинної Стратегії та Плану її реалізації 2025 рік був визначений завершальним етапом у її виконанні.

Досягнення показника реалізації у 86% можна вважати позитивним результатом, що свідчить про високий рівень досягнення стратегічних цілей. В той же час, близько 14% завдань Стратегії залишилися нереалізованими, 38% завдань мали прострочені терміни виконання. Основними причинами стали зміни зовнішніх умов (повномасштабна збройна агресія рф проти України, геополітичні зміни) та розвиток ландшафту кіберзагроз (стрімке впровадження технологій штучного інтелекту, збільшення кількості акторів загроз). Це призвело до необхідності переорієнтації ресурсів, оновлення пріоритетів державної політики у сфері кібербезпеки та часткового коригування запланованих завдань.

Варто підкреслити, що Стратегія кібербезпеки України була розроблена у період мирного часу, тому окремі її положення втратили актуальність або потребують перегляду в контексті нових викликів воєнного періоду. Зокрема, це стосується завдань, орієнтованих на довгостроковий розвиток цифрової інфраструктури та запровадження ініціатив, що не відповідали реаліям воєнного стану.

Напрямок «Стримування» (С)

Для формування потенціалу стримування (С) необхідним є досягнення чотирьох стратегічних цілей: ціль С.1. Дієва кібероборона; ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму; ціль С.3. Ефективна протидія кіберзлочинності; ціль С.4. Розвиток асиметричних інструментів стримування.

Загалом за напрямом визначено 34 завдання, загальний стан виконання – 76%. Напрям Стримування продемонстрував найвищий приріст виконуваності у 2025 році – на 35%.

Ключові статистичні показники реалізації стратегічних цілей за напрямом Стримування станом на кінець 2025 року:

- **Загальна кількість завдань**: 34;
- **Повністю виконано**: 21 завдання (62%);
- **Поступове досягнення запланованих результатів**: 5 завдань (15%);
- **Активізація прогресу**: 7 завдань (20%);
- **Дуже обмежений прогрес**: 1 завдання (3%).

Із позитивних основних моментів за напрямком Стримування (С) варто відзначити продовження здійснення заходів з кібероборони, створення цілісної системи виявлення кібератак, посилення кадрового потенціалу та впровадження технічних рішень для проведення негласних перевірок готовності об’єктів критичної інфраструктури до атак, врегульовано сектор електронної комерції через обов'язкову верифікацію продавців, створено систему навчання співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів, забезпечення конституційних прав людини в цифровому просторі та проведення масштабних кампаній, затвердження єдиної методики збору кіберстатистики, запроваджено гармонізовані санкції проти підрозділів рф та ключових суб'єктів кіберагресії, налагоджено постійний обмін технічними даними з кіберкомандуваннями країн НАТО та ЄС.

Із негативних основних моментів за напрямком Стримування (С) – високий показник прострочених термінів (44%), кадрова нестача у державному секторі та недостатнє фінансування залишаються критичними бар'єрами, що сповільнюють розгортання технічних спроможностей (зокрема MIL.CERT-UA), наявні труднощі у створенні технічних умов для проведення оперативно-розшукових заходів на мережах постачальників послуг, що наразі перебувають лише на стадії обговорення, впровадження програм кіберзахисту на рівні ОВА гальмується через відсутність єдиних навчальних стандартів та брак фахівців на місцях.

Крім того, серед основних невирішених завдань за напрямом Стримування є нормативне забезпечення створення у системі Міністерства оборони України кібервійськ – станом на квітень 2026 року законопроєкт №12349 «Про Кіберсили Збройних Сил України» все ще знаходиться на розгляді у Верховній Раді України.

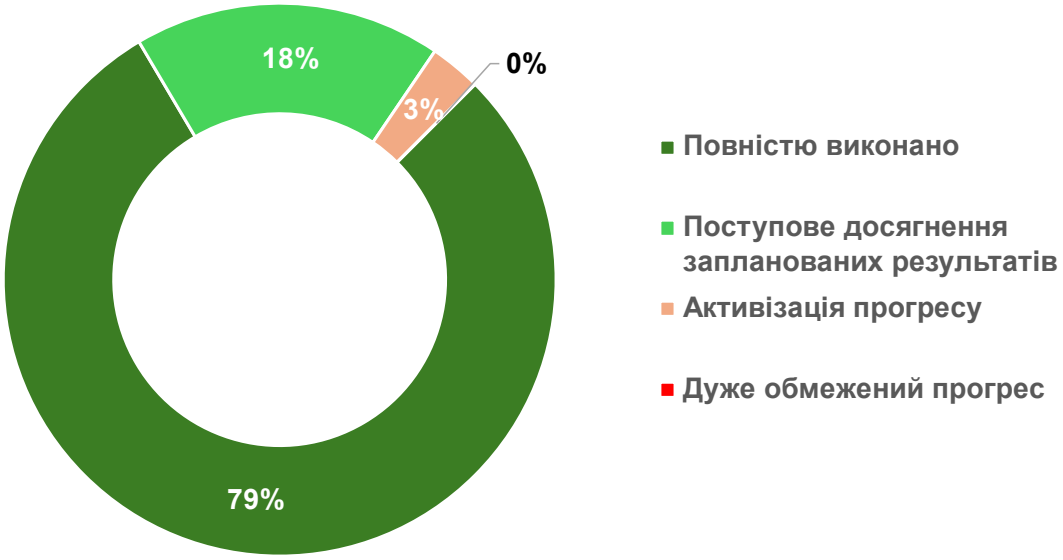
Напрямок «Кіберстійкість» (К)

Для набуття кіберстійкості (К) необхідним є досягнення трьох стратегічних цілей: ціль К.1. Національна кіберготовність та надійний кіберзахист; ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки; ціль К.3. Безпечні цифрові послуги.

Загалом за напрямом визначено 33 завдання, загальний стан виконання – 97%. Напрям кіберстійкості є найбільш реалізованим, прогрес якого зріс у 2025 році на 12%.

Ключові статистичні показники реалізації стратегічних цілей за напрямом Кіберстійкість станом на кінець 2025 року:

- **Загальна кількість завдань**: 33;
- **Повністю виконано**: 26 завдань (79%);
- **Поступове досягнення запланованих результатів**: 6 завдань (18%);
- **Активізація прогресу**: 1 завдання (3%);
- **Дуже обмежений прогрес**: 0 завдань (0%).



Із позитивних основних моментів за напрямком Кіберстійкість (К) ухвалення Національного плану реагування на кіберінциденти, впровадження стандарту NIST CSF 2.0, запуск платформи «CISO Campus», тотальна цифровізація через портал «Дія» (понад 150 послуг та 22,7 млн користувачів), гармонізація законодавства з європейським GDPR, а також розвиток освітнього потенціалу, що охопив підготовку тисяч фахівців та впровадження 21 нового професійного стандарту в галузі кібербезпеки. З негативного за напрямком Кіберстійкість (К) варто відзначити зростання відсотку прострочених завдань, показник яких збільшився з 15% до 36%, повільний процес розгортання повноцінного національного сервісу доменних імен.

Напрямок «Вдосконалення взаємодії» (В)

Для вдосконалення взаємодії (В) необхідним є досягнення трьох стратегічних цілей: ціль В.1. Зміцнення системи координації; ціль В.2. Формування нової моделі відносин у сфері кібербезпеки; ціль В.3. Прагматичне міжнародне співробітництво.

Загалом за напрямом визначено 26 завдань, загальний стан виконання – 88%. Зростання показника виконання у 2025 році – 23%.

Ключові статистичні показники реалізації стратегічних цілей за напрямом вдосконалення взаємодії станом на кінець 2025 року:

- **Загальна кількість завдань**: 26;
- **Повністю виконано**: 17 завдань (65%);
- **Поступове досягнення запланованих результатів**: 6 завдань (23%);
- **Активізація прогресу**: 2 завдання (8%);
- **Дуже обмежений прогрес**: 1 завдання (4%).

Із позитивних основних моментів за напрямком Вдосконалення взаємодії (В) варто відзначити створення правового поля для державноприватного партнерства (законопроєкт № 14150) та легалізація Bug Bounty для держорганів. На міжнародній арені Україна досягла глибокої інтеграції з ENISA та CERT-EU, адаптувала вимоги європейської Директиви NIS2 та посилила технічну взаємодію з НАТО через платформу MN-MISP, одночасно розвиваючи соціальні проєкти, такі як портал StopCrime та масштабна кампанія #ШахрайГудбай.

Із негативного за напрямком Вдосконалення взаємодії (В) варто відзначити відсутність документа, яким встановлюється порядок проведення огляду національної системи кібербезпеки, запровадження системи страхування від кіберризиків, відсутність внутрішніх фінансових механізмів, обмеженість співпраці з окремими структурами НАТО.

Узагальнена характеристика стану реалізації Стратегії

Від моменту введення у дію Стратегії кібербезпеки України у серпні 2021 року було досягнуто чимало:

- ухвалено План кібероборони України як складову частини плану оборони України;
- забезпечено ефективну взаємодію основних суб'єктів забезпечення кібербезпеки та сил оборони, розвиток підрозділів кіберборотьби;
- розпочато створення національної системи управління інцидентами, визначено механізми виявлення вразливостей;
- створено загальнодержавну систему виявлення кібератак, що об’єднує технічний моніторинг, оперативне реагування та контррозвідувальні заходи;
- затверджено переліки об’єктів критичної інфраструктури (ОКІ) та об’єктів критичної інформаційної інфраструктури (ОКІІ), забезпечено функціонування реєстрів ОКІ та ОКІІ;
- розпочато імплементацію положень NIS2 Директиви ЄС, впроваджено низку міжнародних стандартів та настанов з кібербезпеки для посилення безпеки об’єктів критичної інформаційної інфраструктури;
- затверджено Порядок реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, Національний план реагування на кіберінциденти, кібератаки та кіберзагрози;

- створено комплексну систему посилення кадрового потенціалу, запущено національні ініціативи щодо залучення жінок в кібербезпеку, реінтеграції ветеранів;
- запроваджено нові професійні стандарти з підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також запущено перший кібербезпековий Кваліфікаційний центр;
- систематично проводяться міжнародні, національні та секторальні командно-штабні навчання, навчальні заходи та кіберзмагання для покращення навичок та поліпшення координації зацікавлених сторін;
- забезпечено розвиток державно-приватного партнерства;
- підписано Робочу угоду з Агентством Європейського Союзу з кібербезпеки (ENISA) та набуто членство України в Об'єднаному центрі передових технологій з кібероборони НАТО (NATO CCDCOE);
- спільно з міжнародними партнерами було вибудовано систему підтримки України в частині отримання кібербезпекових технологій;
- створено інститут кібердипломатії у державі, на міжнародному рівні формується роль України як регіонального лідера в сфері кібербезпеки.

Загалом, чинна Стратегія кібербезпеки України реалізована на 86%. Одночасно з цим реалізація Стратегії стикнулась з низкою системних викликів, які унеможливили її повноцінне виконання. Зокрема, початок повномасштабної агресії через півроку після затвердження Стратегії ускладнив процеси планування та реалізації її заходів. Також агресія скорегувала плани щодо фінансового забезпечення виконання Стратегії, оптимізувавши видатки на інші складові сектору безпеки і оборони. Реалізація Стратегії стикнулась і з організаційними складнощами – досвід її реалізації показав низьку ефективність моделі річних планів як моделі виконання Плану реалізації Стратегії кібербезпеки України, затвердженого Указом Президента України. В багатьох випадках все ще спостерігається брак кваліфікованих фахівців, а також достатньої підготовленості керівництва органів щодо розуміння важливості питань актуальності кібербезпеки як на об’єктовому, так і національному рівнях.

Крім того, на системному рівні існує неузгодженість між документами стратегічного планування в сфері національної безпеки і урядовими планами дій. Плани пріоритетних дій Уряду на 2025 рік (розпорядження КМУ від 18.02.2025 №131-р, від 10.09.2025 №1003-р) містять лише фрагментарні цілі, що стосуються забезпечення кібербезпеки. Наприклад, План заходів на 2025-2027 роки з реалізації Державної стратегії регіонального розвитку на 2021-2027 роки (розпорядження КМУ від 25.09.2025 №1047-р) взагалі не встановлює цілей в сфері кібербезпеки, хоча підвищення рівня кіберзахисту на регіональному рівні наразі є одним з пріоритетних стратегічних завдань. Таким чином, неузгодженість планування створює умови для дублювання завдань та розпорошення фінансових ресурсів, недофінансування критичних напрямів кібербезпеки. Як наслідок, недофінансування з державного бюджету є однією з причин неповного виконання завдань Стратегії кібербезпеки України.

В умовах обмежень фінансування з державного бюджету реалізація окремих заходів з реалізації Стратегії здійснюється за рахунок коштів міжнародної технічної допомоги, підвищуючи загальний показник виконуваності. Проте в багатьох випадках донори зацікавлені у наданні сервісів та рішень від національного виробника, залученні до виконання робіт фахівців з власних країн. Це уповільнює розвиток екосистеми вітчизняного ринку кібербезпеки, що у середньостроковій перспективі може створювати додаткові ризики для національної системи кібербезпеки. Крім того, це збільшує залежність від пропрієтарних рішень малого кола глобальних постачальників продуктів та послуг, що створює ризики втрати цифрового суверенітету за низкою критичних напрямів та збільшує ризики ланцюгів постачання.

Чинна Стратегія кібербезпеки України була розроблена у період мирного часу, тому окремі її положення втратили актуальність або потребували перегляду в контексті нових викликів воєнного періоду. В той же час, незважаючи на передбачений документом механізм

внесення змін до Плану реалізації Стратегії, такі зміни не вносились. Однією з причин є складний організаційний механізм планування та звітування, що включає цикли різної тривалості – півроку, рік, 5 років. Впровадження автоматизованого інструменту CyberTracker для моніторингу виконання Стратегії кібербезпеки України дозволить підвищити ефективність контролю за реалізацією заходів Стратегії та сприятиме підготовці управлінських рішень, спрямованих на швидку адаптацію до змін у безпековому середовищі, усунення та мінімізацію негативних тенденцій у сфері кібербезпеки.

Попри наявні обмеження, досягнення рівня реалізації Стратегії кібербезпеки України у майже 90% можна вважати успіхом. Таке досягнення підтверджує стійкість інституційної спроможності національної системи кібербезпеки, здатність органів державної влади оперативно адаптуватися до кризових умов, а також демонструє результати у вигляді розвитку спроможностей суб'єктів національної системи кібербезпеки, розширення взаємодії між усіма зацікавленими сторонами, підвищення ефективності координації між державними, військовими та приватними суб’єктами та активізації міжнародного співробітництва у сфері кібербезпеки.

Результати аналізу стану виконання чинної Стратегії кібербезпеки України свідчать про те, що, незважаючи на складні обставини, основні стратегічні цілі було досягнуто.

VIII. КІБЕРСТІЙКІСТЬ СУСПІЛЬСТВА ТА ГРОМАД

Громадянський сектор, що займається кіберстійкістю, представлений кількома функціональними типами організацій. Перший - просвітницько-освітній: неурядові організації (НУО), що розробляють або поширюють навчальні матеріали з кібергігієни для широких аудиторій, зокрема для громадян, учителів, бібліотекарів і волонтерів[43]. Другий - адвокаційно-аналітичний: організації, що публікують матеріали для НУО-середовища, акцентуючи на кіберстійкості самих інституцій громадянського суспільства – захисті донорських і персональних даних, операційній безпеці[44]. Третій – муніципально-орієнтований: організації, що виступають посередниками між рівнем місцевого самоврядування та фаховою кіберспільнотою, зокрема шляхом підписання угод про співпрацю у сфері кібербезпеки та запуску консультаційних служб для громад[45].

Тематична активність НУО у 2025 році зросла у порівнянні з попередніми роками: кіберстійкість набула більшої ваги в дискусіях про відновлення та стійкість громад в умовах тривалої збройної агресії. Водночас структурна проблема сектору зберігається: НУО, що займаються кіберграмотністю, не мають надійних і стабільних джерел фінансування, що обмежує сталість їхніх програм та можливості для інституційного розвитку. Більшість із них реалізують короткострокові проєкти в межах донорських грантів, здебільшого американських і канадських фондів, без гарантованого продовження. Ця нестабільність тим більш відчутна на тлі того, що на державному рівні 2025 рік позначився суттєвим зрушенням у нормативному оформленні відповідальності за кіберзахист на місцях.

Закон № 4336-IX[46] запровадив принципово нову вимогу: в органах місцевого самоврядування (як в усіх державних організаціях та на об’єктах ОКІ) мають бути призначені

[43] Науково-просвітницька асоціація кібербезпеки (SCSA). Офіційний сайт. URL: https://scsa.org.ua/en/mainpage/ (дата доступу: квітень 2026).

[44] Ресурсний центр ГУРТ. Тренди з кібербезпеки в благодійності у 2025 році. URL: https://gurt.org.ua/articles/105442/ (дата доступу: квітень 2026).

[45] Асоціація малих міст України. Новини про співпрацю у сфері кібербезпеки громад та Службу підтримки. URL: https://atu.net.ua (дата доступу: квітень 2026).

[46] Верховна Рада України. Закон № 4336-IX від 27.03.2025 «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/4336-20

особи, що виконують функції керівника з кіберзахисту[47]. Відтак кібербезпека на рівні громади перестала бути факультативною – вона стала законодавчо закріпленим обов'язком. Протягом 2025 року Кабінет Міністрів затвердив низку підзаконних актів на виконання цієї норми, зокрема Порядок призначення керівника з кіберзахисту в органі державної влади[48], а також Порядок проведення інструктажів та систематичних тренінгів щодо кібергігієни[49].

Реалізація нових вимог на місцях відбувалася з різною інтенсивністю. Серед регіонів, що демонструють найбільш послідовний підхід, виділяється Львівська область: усі її громади визначили відповідальних за інформаційну безпеку, а профільний підрозділ ОВА констатує, що це «лише початок», і вже готує відповідну програму навчання[50]. На рівні окремих громад фіксуються перші приклади видання організаційно-розпорядчих актів – із визначенням функціональних обов'язків відповідальних осіб, включно з організацією кіберінструктажів, управлінням ризиками та взаємодією з CERT-UA[51]. Разом із тим затверджені плани реагування на кіберінциденти залишаються поодиноким явищем: публічно доступних підтверджень того, що більшість ОМС мають такі документи, у відкритих джерелах не виявлено. Перехід від формальної інституціоналізації до реально функціонуючих систем реагування лишається завданням на наступний період.

Паралельно з інституційними змінами розгортався масштабний освітній процес. Ключовою платформою масового навчання залишається Дія.Освіта: загальна кількість реєстрацій на ній протягом 2025 року перевищила 3 мільйони, за рік зареєструвалися 617,5 тисячі нових користувачів[52]. Серед найпопулярніших тем – кібергігієна та онлайн-безпека; за рік користувачі отримали понад 1,44 мільйона сертифікатів[53], а тема кібергігієни зокрема набрала 1,1 мільйона переглядів[54]. У 2025 році кількість громадян, які пройшли навчання за програмами кіберграмотності на порталі Дія, склала близько 1 млн осіб[55].

Демографічний профіль платформи свідчить про концентрацію аудиторії в середній віковій групі: серед зареєстрованих у 2025 році 56,9% становлять жінки, 31,5% – чоловіки, найбільша вікова група – 31–60 років, молодь 15–24 років формує близько п'ятої частини нових реєстрацій[56]. Ці дані вказують на те, що основна аудиторія - доросле економічно активне населення. Охоплення державних службовців і військовослужбовців забезпечується через окрему систему обов'язкових інструктажів і тренінгів, запроваджену постановою Уряду № 1281 від 8 жовтня 2025 року; Держспецзв'язку затвердила відповідні методичні рекомендації[57], проте кількість охоплених осіб у публічних звітах не зазначено. Для вчителів

---

[47] LexInform. Підрозділи з кіберзахисту з'являться в органах державної влади. URL: https://lexinform.com.ua/zakonodavstvo/pidrozdily-z-kiberzahystu-z-yavlyatsya-v-organah-derzhavnoyi-vlady/ (дата публікації: квітень 2025).

[48] Кабінет Міністрів України. Постанова від 26.11.2025 № 1516 «Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади». URL: https://cip.gov.ua/ua/news/kabmin-zatverdiv-poryadok-priznachennya-kerivnikiv-z-kiberzakhistu-v-organakh-derzhavnoyi-vladi

[49] Кабінет Міністрів України. Постанова від 08.10.2025 № 1281 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни». Цит. за: https://sud.ua/uk/news/ukraine/344461 (дата публікації: 23 жовтня 2025).

[50] Львівська ОВА. Усі громади Львівщини визначили відповідальних за інформаційну безпеку. URL: https://loda.gov.ua/news/136841 (дата доступу: серпень 2025).

[51] Сквирська міська рада. Наказ про призначення відповідальної особи з питань інформаційної безпеки та кіберзахисту. URL: https://skvyrska-gromada.gov.ua/docs/2192719/ (дата публікації: листопад 2025).

[52] Bazilik Media. Дія.Освіта у 2025 році: як і чого навчалися українці. URL: https://bazilik.media/diia-osvita-u-2025-rotsi-iak-i-choho-navchalysia-ukraintsi/ (дата публікації: 10 січня 2026).

[53] Fintech Insider. Як українці навчалися протягом року: 10 фактів з аналітики Дія.Освіта. URL: https://fintechinsider.com.ua/yak-ukrayinczi-navchalysya-protyagom-roku-10-faktiv-z-analityky-diya-osvita/ (дата публікації: 8 січня 2026).

[54] Міністерство цифрової трансформації України. Місяць цифрової грамотності 2025. URL: https://thedigital.gov.ua/news/education/misiats-tsyfrovoyi-hramotnosti-2025 (дата публікації: 3 листопада 2025).

[55] Міністерство цифрової трансформації України, 2025.

[56] Там само

[57] Судово-юридична газета. Кібергігієна в держорганах - затвердили Методичні рекомендації для навчання посадовців. URL: https://sud.ua/uk/news/ukraine/344461 (дата публікації: 23 жовтня 2025).

та педагогічних працівників доступні курси академічних партнерів у сфері кібербезпеки обсягом від 17 до 35 годин, тоді як консолідована статистика по цій та інших цільових групах – медиках, місцевих посадовцях, МСБ – у загальнодоступних джерелах відсутня.

Поряд із кількісним охопленням 2025 рік відзначився й якісними змінами у підходах до кіберосвіти. По-перше, Держспецзв'язку затвердила методичні рекомендації (наказ від 21.10.2025 № 661), що встановлюють єдиний системний підхід до навчання персоналу державних установ: з урахуванням організаційної структури, оцінюванням знань та документуванням участі. По-друге, 12 листопада 2025 року відбулась публічна презентація проєкту Національної стратегії кібергігієни – документа горизонту до 2030 року, що визначає рамку системного розвитку культури безпечної поведінки в цифровому середовищі та враховує досвід США, ОАЕ, Естонії, Сингапуру, Фінляндії та Японії[58]. Захід організовано за партнерства НКЦК при РНБО, Держспецзв'язку та Міністерства цифрової трансформації[59]. По-третє, самі платформи змінюють формат: Дія.Освіта запустила інструмент на основі штучного інтелекту для персоналізованого навчання; 70,9% користувачів проходять курси зі смартфонів, а найбільший обсяг взаємодій припадає на тести Цифрограми (1,55 млн) та освітні серіали (1,15 млн) – що фіксує виразний зсув до мобільного, асинхронного та короткоформатного навчання. Освітні серіали на тему цифрової безпеки для початківців та основ кібергігієни створено за ініціативи Мінцифри за підтримки USAID та за участі академічних партнерів[60].

Важливою складовою змістового оновлення є міжнародна співпраця. У березні 2025 року підписано меморандум між НКЦК та Європейським центром компетенцій у сфері кібербезпеки (ECCC), поглиблено співробітництво з партнерами з ЄС і НАТО[61,62]. Міжнародне фінансування загалом залишається системоутворюючим чинником. Започатковані у 2024 році проєктом USAID «Кібербезпека критично важливої інфраструктури України»[63] курси, кіберполігони в університетах та методологічний інструментарій продовжують використовуватись і у 2025 році. Держдепартамент США підтримує програми підвищення кіберстійкості громад через профільні організації[64], Канада долучилася до фінансування регіональних заходів через Global Affairs Canada[65], ЄС підтримує цифрову трансформацію через програму DT4UA, що розпочала новий етап у жовтні 2025 року[66].

Попри значний обсяг навчальних активностей, охоплення вразливих і недостатньо представлених груп залишається структурно слабким місцем системи. Доступні кіберосвітні матеріали частково адаптовані для аудиторії старшого віку[67], однак статистика 2025 року показує, що домінуюча вікова аудиторія платформ – 31–60 років, тоді як сегмент 65+ залишається маргінальним. Жодна з аналізованих державних програм не виокремлює ВПО як

[58] РНБО України. Україна презентувала проєкт Національної стратегії кібергігієни. URL: https://www.rnbo.gov.ua/ua/Diialnist/7325.html (дата публікації: 13 листопада 2025).
[59] Кабінет Міністрів України. Представлено проект Національної стратегії кібергігієни. URL: https://www.kmu.gov.ua/news/predstavyly-proekt-natsionalnoi-stratehii-kiberhihiieny (дата публікації: 12 листопада 2025).
[60] Дія.Освіта. Базові знання з кібергігієни; Кіберняні. URL: https://osvita.diia.gov.ua/courses/basic-knowledge-of-cyber-hygiene; https://osvita.diia.gov.ua/courses/cybernanny (дата доступу: квітень 2026).
[61] Кібербез. Цифровий щит України: 5 ключових висновків про кіберстійкість країни зі звіту ЄС. URL: https://cybersec.net.ua/statti/932 (дата публікації: 6 листопада 2025).
[62] РНБО України. Підписання меморандуму між НКЦК та ECCC. URL: https://www.rnbo.gov.ua (дата доступу: квітень 2026).
[63] Наразі проект має назву «Проєкт США "Кібербезпека критично важливої інфраструктури України"»
[64] CRDF Global. Програми підвищення кіберстійкості для громад України. Цит. за матеріалами заходу АММУ, грудень 2025. URL: https://atu.net.ua/news/kiberstijkist-gromad-strategy-innovation-summit
[65] Асоціація малих міст України. Кіберстійкість громад: Strategy & Innovation Summit. URL: https://atu.net.ua/news/kiberstijkist-gromad-strategy-innovation-summit (дата публікації: грудень 2025).
[66] Міністерство цифрової трансформації України. Стартував новий етап проєкту DT4UA. URL: https://thedigital.gov.ua/news/technologies/tsyfrovizuyemo-razom-z-yes-startuvav-novyy-etap-proyektu-dt4ua (дата публікації: 31 жовтня 2025).
[67] Дія.Освіта. Базові знання з кібергігієни; Кіберняні. URL: https://osvita.diia.gov.ua (дата доступу: квітень 2026).

спеціальну цільову групу, а доступні платформи, орієнтовані на мобільні та цифрові канали, передбачають умови підключення, що для мешканців прифронтових районів і тимчасового житла можуть бути проблематичними[68]. Кіберосвітні програми 2025 року охоплюють переважно економічно активне міське населення з базовими цифровими компетенціями; групи, що відчувають найбільші труднощі з доступом – літні люди, мешканці периферійних районів, ВПО, – залишаються на периферії охоплення, і жодне з аналізованих відомств не артикулювало це як стратегічну проблему, що потребує цільового вирішення.

Не менш суттєвим є дефіцит незалежних досліджень кіберстійкості на рівні громад. Самостійного корпусу таких досліджень у 2025 році публічно зафіксовано не було: діагностична робота відбувалася переважно через адміністративні інструменти – інформаційний аудит та самооцінювання. Найближчим до дослідницького формату є системний інформаційний аудит, ініційований однією з обласних військових адміністрацій, що у 2025 році відбувся вже втретє і поширився на рівень громад[69], проте він стосується передусім управління відкритими даними, а не кіберстійкості в технічному розумінні. Дослідження рівня цифрових навичок українців, що проводиться раз на два роки, було представлено на профільному форумі у листопаді 2025 року, однак повне оприлюднення його результатів до кінця звітного року не відбулося[70]. Наявні дослідження оперують або технічними показниками (кількість зафіксованих інцидентів CERT-UA), або освітніми (кількість проходжень курсів), але не соціологічними вимірами фактичної поведінки та обізнаності конкретних спільнот. Дефіцит незалежних досліджень є наслідком як ресурсних обмежень НУО і академічних установ, так і складності польової роботи в умовах воєнного стану.

Серед інших помітних подій 2025 року – проведення у грудні тематичного заходу за участі НКЦК при РНБО, представників місцевого самоврядування та міжнародних партнерів, де обговорювалися стратегії кіберзахисту на муніципальному рівні та перспективи розбудови мережі центрів обміну інформацією про кіберзагрози на кшталт регіональних ISAC. Ця ідея, запозичена зі світової практики, передбачає горизонтальну координацію кіберзахисту між громадами; її інституційне оформлення залишається питанням майбутнього. Щодо реального тестування кіберстійкості громад: жодного публічно задокументованого випадку, де кіберінцидент виявив рівень підготовленості громади і призвів до задокументованих висновків, у відкритих джерелах за 2025 рік не виявлено.

IX. КІБЕРДИПЛОМАТІЯ

У 2025 році міжнародна співпраця України у сфері кібербезпеки набула системного та багаторівневого характеру. Україна не лише отримувала допомогу, але й виступала активним експортером практичного досвіду протидії кібератакам в умовах війни.

В рамках співпраці з Європейським Союзом у Києві було проведено четвертий раунд кібердіалогу Україна–ЄС, зосередженого на операційній взаємодії та кіберстійкості. Під час діалогу сторони обговорили поточні кіберзагрози, узгодження політик кібербезпеки, імплементацію директиви NIS2, захист критичної інфраструктури та розвиток кібероборони. Особливу увагу було приділено інтеграції України у європейську кіберекосистему, доступу до Кіберрезерву ЄС, створенню національних Кіберсил і розвитку державно-приватної взаємодії, питанню запровадження кіберсанкцій проти держав і структур, причетних до зловмисних кібероперацій. Також в рамках діалогу було організовано, за сприяння НКЦК, командно-штабні навчання з партнерами, під час яких моделювалися спільні дії України та ЄС у разі масштабної кібератаки.

---

[68] OCHA / CCCM Cluster. Оцінка вразливостей в місцях тимчасового проживання ВПО. URL: https://www.cccmcluster.org (дата публікації: грудень 2024).

[69] Львівська ОВА. Розпочато плановий інформаційний аудит. URL: https://loda.gov.ua/news/141236 (дата публікації: липень 2025).

[70] Міністерство цифрової трансформації України. Як підвищити кіберстійкість країни: презентуємо проєкт Національної стратегії кібергігієни.

У 2025 році також в перше пройшов кібердіалог між Україною та Нідерландами.

Крім цього слід відмітити посилення узгодженості політичних заяв щодо атрибуції кібератак із державами-партнерами ЄС та НАТО та співпрацю щодо посилення режиму кіберсанкцій проти рф у відповідь на зловмисну діяльність в кіберпросторі.

Відбулося розширення співпраці з ENISA (обмін аналітикою, участь у тренуваннях, доступ до методологій). Посиленню співпраці сприяло те, що вперше національний експерт від України – представник НКЦК, був відряджений до ENISA на довгостроковій основі. Також у 2025 році українська команда дебютувала на найбільших європейських кіберзмаганнях, організованих ENISA – European Cybersecurity Challenge, що відбулися у жовтні у м. Варшава. Під час змагань Україна подала заявку на проведення ECSC 2026, яку підтримали ENISA та виконавчий комітет ECSC.

Була започаткована взаємодія із Європейським центром компетенції в сфері кібербезпеки (ECCC), меморандум з яким було підписано Україною в особі НКЦК у березні 2025 року. А у червні цього ж року представники України вперше взяли участь у засіданні Керівної ради ECCC та зустрічі мережі національних координаційних кіберцентрів ЄС, в ході яких подали запит щодо партнерської участі України в ECCC, долучення до реалізації проєктів Digital Europe Programme та створення національного осередку NCC-UA на базі НКЦК.

Також тривало започаткування співробітництва в сфері кібербезпеки із країнами Східної Європи та Близького Сходу. Представники України на запрошення азербайджанської сторони у жовтні 2025 року взяли участь у масштабній конференції Critical Infrastructure Defense Challenge, що пройшла у м. Баку; долучилися до Конференції з кібербезпеки у Румунії та інших країн.

А у липні 2025 року у м. Чернівці за ініціативи НКЦК відбулися консультації з партнерами щодо створення регіонального кіберальянсу Україна-Румунія-Молдова, який поставив на меті практичну взаємодію у протидії кібер та гібридним загрозам, насамперед з боку рф. Очікується, що Альянс посилить співпрацю України, Румунії та Республіки Молдова у обміні інформацією про кіберзагрози, спільній розробці та впровадженні рішень на основі ШІ, підготовці фахівців, зокрема для проведення спільних заходів кібероборони, підвищенні стійкості критичної інфраструктури та захисті демократичних інституцій. Формування кіберальянсу стало важливим кроком на виконання домовленостей Президентів України, Румунії та Молдови за результатами четвертого саміту Україна – Південно-Східна Європа.

Слід відмітити, що якщо у попередні роки основним донором міжнародної допомоги для України у сфері кібербезпеки виступали США, зокрема така допомога реалізовувалася через CRDF Global та USAID, то у зв’язку із зміною зовнішньополітичної позиції Сполучених Штатів щодо тимчасового припинення та у подальшому обмеження гуманітарної допомоги іншим країнам, зокрема Україні, а також ліквідацією USAID, американська допомога у 2025 році у сфері кібербезпеки зменшилася. Це обумовило більш активну роль та залученість європейських країн та власне ЄС, а також активізацію інших партнерів, таких як Канада та Великобританія. Наприклад, традиційно у 2025 році під егідою НКЦК проходили засідання Національного кластеру кібербезпеки, які на відміну від попередніх років замість США були профінансовані Канадою у межах Талліннського механізму, який став одним з ключових інструментів міжнародної допомоги Україні у сфері кібербезпеки. В цілому, у 2025 році Канада виділила 92 млн. гривень у стратегічні ініціативи у сфері кібербезпеки, серед яких – захист критичної інфраструктури, навчальні програми та постачання обладнання.

2025 рік став і роком суттєвої активізації міжнародної співпраці та залучення країн-учасниць у межах Талліннського механізму (ТМ), який було започатковано в грудні 2023 року як міжнародну відповідь на постійно зростаючі загрози в кіберпросторі та агресію росії. Він покликаний посилити захист України від кібератак, зробивши міжнародну підтримку максимально ефективною та скоординованою між країнами-партнерами. Станом на квітень 2026 року до ініціативи доєдналося 14 країн: Велика Британія, Данія, Естонія, Італія, Канада, Нідерланди, Німеччина, Норвегія, Польща, США, Франція, Чехія, Швеція та Фінляндія.

НАТО, ЄС та Світовий банк долучилися як офіційні спостерігачі. Франція навіть включила Талліннський механізм у свою національну кіберстратегію[71].

Для забезпечення прозорості та централізованої взаємодії з донорами й реципієнтами в квітні 2025 року створено Проєктний офіс Талліннського механізму (Tallinn Mechanism Project Office, TMPO). Він виконує функцію постійного координаційного центру між міжнародними партнерами та українськими установами, супроводжує реалізацію проєктів і забезпечує узгодженість дій усіх сторін. Проєкти, які реалізуються у межах Талліннського механізму, обирають[72]:

- Технічна робоча група, що оцінює проєкти за технічною спроможністю та відповідністю пріоритетам.
- Міжвідомча робоча група, яка визначає стратегічну важливість ініціатив.

Таким чином забезпечується прозора система відбору та координація імплементації проєктів у межах Талліннського механізму. Станом на квітень 2026 року чотири проекти були завершені, ще 25 перебували на різних етапах реалізації. ТМ показує помітні здобутки у залученні коштів міжнародної донорської підтримки для вирішення українських кібербезпекових питань. Зокрема, Швеція оголосила про виділення близько 593 млн грн (135 млн шведських крон)[73] на посилення кіберстійкості України, Канада - 92 млн грн (3 млн канадських доларів)[74], Норвегія – 2,1 млн євро[75], Італія – 1 млн євро[76]. Крім окремих проєктів, у межах Талліннського механізму впроваджується низка інших ініціатив – від оцінки кібербезпеки об'єктів критичної інфраструктури до програм розвитку спроможностей і професійного навчання українських фахівців (більше інформації в наступному розділі).

Загалом, серед основних країн-партнерів України сфері кібербезпеки у 2025 році можна відзначити ЄС, Естонію, Канаду, США, Великобританію, Японію. Серед недержавного сектору та структур-імплементаторів – CRDF Global, ESTDEV, EGA, EU4DigitalUA GIZ, USAID, DAI, JICA та інші.

Україна поступово стає активним учасником ключових міжнародних конференцій та інших заходів у сфері кібербезпеки, а також технічних кібербезпекових змагань. Що свідчить про визнання та поступове масштабування унікального українського досвіду у цій галузі. Зокрема, в ході щорічної Мюнхенської конференції з кібербезпеки, яка проходила у лютому 2025 року, було організовано окрему панельну дискусію за участі виключно українських представників державного і приватного секторів, які ділилися досвідом щодо побудови кіберстійкості в умовах війни. А у квітні 2025 року українська команда вперше здобула перемогу на щорічному хакатоні НАТО, що проходив у Франції.

Також Україна вже самостійно виступає організатором заходів міжнародного масштабу у сфері кібербезпеки. Зокрема у березні 2025 року в столиці України відбувся другий Київський міжнародний форум кіберстійкості 2025 під гаслом «На захисті демократії». Захід під егідою Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України об'єднав українських та міжнародних лідерів думок, представників державного сектору, міжнародних організацій, бізнесу, кіберспільноти, технологічних компаній і провідних експертів галузі для обговорення ключових викликів кібербезпеки.

Загалом захід зібрав понад 1000 учасників з 35 країн, ставши головною подією в сфері кібербезпеки в Україні та Східній Європі. Київський міжнародний форум з кіберстійкості 2025 ще раз довів: Україна не лише перемагає у кібервійні проти рф, а вже є регіональним лідером в сфері кібербезпеки та готова формувати спільно з партнерами майбутнє глобальної кіберстійкості.

[71] https://www.sgdsn.gouv.fr/files/files/National%20cybersecurity%20strategy_ENG.pdf
[72] https://platform-tm.com/project-implementation
[73] https://platform-tm.com/news/sweden-allocates-sek-135-million-to-improve-ukraines-civilian-cybersecurity
[74] https://platform-tm.com/news/canada-allocates-cad-3-million-to-strengthen-ukraines-cyber-resilience
[75] https://platform-tm.com/news/norway-joins-the-tallinn-mechanism-to-support-ukraines-cyber-resilience
[76] https://platform-tm.com/news/italy-contributes-nearly-euro1-million-to-strengthen-cybersecurity-in-ternopil-region

X. КАДРОВЕ ТА НАУКОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Кадрове забезпечення залишається одним із найбільш системних та гостро відчутних викликів для суб'єктів національної системи кібербезпеки України у 2025 році. Узагальнена картина, що складається на основі самооцінок ключових державних органів, є неоднорідною: якщо частина відомств оцінює свій кадровий потенціал як достатній для виконання базових функцій, більшість фіксує суттєві обмеження – насамперед у кількості та якості фахівців вузькопрофільних напрямів (SOC, DevSecOps, криміналістика, threat intelligence). Серед оборонних структур центральна проблема – укомплектування підрозділів кіберзахисту фахівцями, здатними ефективно протидіяти актуальним загрозам в умовах безперервного збройного конфлікту.

Визначальною причиною кадрового дефіциту виступає структурний дисбаланс між умовами оплаті праці в державному та приватному секторах. Конкуренція з боку ринку, де кваліфікований спеціаліст може отримати значно вищу винагороду, призводить до відтоку кадрів із державних органів і ускладнює рекрутинг. Існуючий механізм бюджетного фінансування не передбачає ефективних інструментів матеріального стимулювання, що унеможливлює застосування селективних підходів до підбору персоналу у сфері кіберзахисту. Наслідком є зниження конкурентоспроможності державних органів на ринку праці та, відповідно, зниження загального рівня спроможностей.

Для державних наукових і академічних установ ситуація є ще більш критичною. Навіть утримання фахівців за профільними напрямами (SOC, DevSecOps) описується як сильно обмежене, а формування кадрового резерву – як максимально обмежене через неможливість забезпечити гідну оплату. У підпорядкованих структурах ці проблеми виражені ще гостріше: матеріально-технічне забезпечення більшості з них перебуває на мінімально прийнятному рівні, а спроможності щодо протидії кіберзагрозам оцінюються як низькі.

Водночас окремі суб'єкти оцінюють рівень кадрового забезпечення як достатній для виконання основних функцій кіберзахисту, хоча й супроводжують цю оцінку застереженнями щодо постійного підвищення навантаження на персонал. Такі оцінки, однак, можуть не відображати реальних потреб у ситуації постійної ескалації кіберагресії. Дефіцит кіберфахівців у масштабах країни може сягати до 100 тисяч осіб, хоча ця цифра є приблизною в умовах відсутності надійної статистичної бази. Суперечливість наявних оцінок - від кількох тисяч до ста тисяч - сама по собі є індикатором інформаційної прогалини, що унеможливлює системне стратегічне планування у кадровій сфері.

Системна робота зі стандартизації кваліфікацій у сфері кібербезпеки, розпочата ще у 2021 році, у 2025 році перейшла до якісно нового етапу - функціонування повноцінного кваліфікаційного центру та нарощування переліку чинних профстандартів. Було затверджено три нові професійні стандарти, що регламентують діяльність фахівців у сфері захисту критичної інфраструктури, чим розширено сукупний перелік затверджених стандартів до рівня, що охоплює основні кваліфікаційні позиції галузі.

Кваліфікаційний центр інформаційних технологій та кібербезпеки у 2025 році розширив перелік акредитацій до десяти додаткових кваліфікацій, охоплюючи позиції аудиторів та провідних спеціалістів[77]. На початку 2025 року 11 випускників Центру успішно склали атестацію та отримали перші в Україні сертифікати за стандартом «Адміністратор мереж і систем», а до кінця першого кварталу - ще чотири аналогічних сертифіката[78]. У лютому 2025 року Кваліфікаційний центр отримав акредитацію від Національного агентства кваліфікацій з термінами дії сертифікатів акредитації до 2030 року[79].

[77] Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки // qc.csi.cip.gov.ua. URL: https://qc.csi.cip.gov.ua/uk/posts/10 (дата доступу: 05.04.2026).
[78] Випуск Кваліфікаційного центру – сертифікати отримали четверо адміністраторів мереж і систем // qc.csi.cip.gov.ua. 19 березня 2025. URL: https://qc.csi.cip.gov.ua/uk/posts/19-03-25 (дата доступу: 05.04.2026).
[79] Порядок присвоєння та підтвердження // qc.csi.cip.gov.ua. URL: https://qc.csi.cip.gov.ua/uk/pages/assigning-confirmation (дата доступу: 05.04.2026).

Розробка нових профстандартів відбувається з метою формування повноцінної Національної рамки кваліфікацій у сфері кібербезпеки та імплементації таких рамок, як NICE NIST та ECSF ENISA[80]. На 2026 рік заплановано розробку ще трьох профстандартів організаційно-правового спрямування, що свідчить про безперервність реформи попри складні умови воєнного часу.

Паралельно здійснюється апробація єдиного державного кваліфікаційного іспиту (ЄДКІ) для бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації» як обов'язкового компоненту атестації. У 2025 році іспит відбувся 29 квітня, порогове значення балу для зарахування встановила фахова комісія МОН за результатами психометричного аналізу[81]. За підсумками іспиту 2025 року поріг не подолали 15,35% студентів (361 здобувач освіти)[82]. Необхідно зазначити, що проект стандарту вищої освіти за спеціальністю 125 на третьому (освітньо-науковому) рівні у 2025 році перебував на стадії розробки, що вказує на незавершеність нормативної бази для підготовки докторів філософії за оновленими вимогами[83].

Між джерелами наявна певна суперечність: попри системну роботу з розробки стандартів, ряд відомств фіксує потребу у цільовому фінансуванні для повноцінного впровадження Рамки кваліфікацій з кібербезпеки та захисту інформації у власну операційну діяльність, що свідчить про розрив між наявністю нормативних документів та їх практичним застосуванням.

У 2025 році за даними Єдиної державної електронної бази з питань освіти (ЄДЕБО) заклади фахової передвищої та вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» здійснили підготовку 3541 особи. З них докторів філософії – 17 осіб, магістрів - 1192 особи, бакалаврів - 2263 особи, молодших бакалаврів – 2 особи, фахових молодших бакалаврів – 67 осіб.

Щодо вступної кампанії на спеціальність F5 «Кібербезпека та захист інформації» у 2025 році: для здобуття ступеня бакалавра подано 22 735 заяв, магістра – 3 916 заяв, доктора філософії – 215 заяв. Фактично зараховано на освітній ступінь бакалавра – 3753 особи, магістра – 1353 особи, доктора філософії – 74 особи. Ці дані свідчать про значний розрив між кількістю поданих заяв та реальним зарахуванням на рівні бакалаврату (співвідношення приблизно 6:1), що відображає як конкурсний характер вступу, так і обмежену ліцензійну ємність програм.

За рейтингом популярності серед вступників 2025 року кібербезпека стабільно входить до пріоритетних напрямів серед технічних спеціальностей. На окремих університетських програмах конкурс сягав понад 9 заяв на місце. Серед десяти найпопулярніших серед вступників закладів за спеціальністю F5 – університети Львова, Києва та Вінниці[84]. Незважаючи на воєнний стан і пов'язані з ним труднощі (евакуація, мобілізація студентів, руйнування інфраструктури окремих закладів), інтерес до спеціальності залишається стабільно високим.

В системі відомчої підготовки окремі органи забезпечують підготовку фахівців через профільні навчальні інститути за спеціальністю F5. Зокрема, упродовж 2025 року 51 особа

---

[80] Ставка на освіту: Україна посилює стійкість у кіберпросторі через професійну підготовку // qc.csi.cip.gov.ua. URL: https://qc.csi.cip.gov.ua/uk/posts/stavka_osvita (дата доступу: 05.04.2026).

[81] Встановлено пороговий бал ЄДКІ за спеціальністю 125 Кібербезпека // mon.gov.ua. 12 травня 2025. URL: https://mon.gov.ua/news/vstanovleno-porohovyi-bal-iedki-za-spetsialnistiu-125-kiberbezpeka (дата доступу: 05.04.2026).

[82] ЄДКІ 2026 зі спеціальності «Кібербезпека та захист інформації»: дати проведення й поради з підготовки // education.ua. 10 листопада 2025. URL: https://www.education.ua/news/2025/11/10/yedki-2026-zi-spetsialnosti-kiberbezpeka-ta-zakhyst-informatsii-daty-provedennia-y-porady-z-pidhotov/ (дата доступу: 05.04.2026).

[83] Проєкт стандарту вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» на третьому (освітньо-науковому) рівні вищої освіти // cybersec.net.ua. URL: https://cybersec.net.ua/normatyvni-dokumenty.html (дата доступу: 05.04.2026).

[84] Кібербезпека та захист інформації: все про спеціальність F5 (125) // education.ua. URL: https://www.education.ua/news/2024/03/29/kiberbezpeka-ta-zakhyst-informatsii-vse-pro-spetsialnist-125/ (дата доступу: 05.04.2026).

підвищила кваліфікацію з питань кібербезпеки на платній основі, ще 33 поєднували службову діяльність зі здобуттям вищої освіти за ІТ-спеціальностями. Крім того, 11 осіб у рамках безкоштовних програм пройшли підготовку в різних акредитованих закладах – з тематики кібердипломатії, стратегічного лідерства, загальних курсів кібербезпеки та захисту персональних даних. Новий напрям підготовки керівників – CISO Campus, відкритий у листопаді 2025 року на базі CDTO Campus[85] – орієнтований на масштабування підготовки керівників з кібербезпеки (CISO) по всіх державних установах, де посаду CISO було запроваджено законодавчо.

Освітні програми у сфері кібербезпеки зазнають активної модернізації, хоча сам процес характеризується суттєвою нерівномірністю між закладами. Ключова вимога, яку зафіксували більшість стейкхолдерів та підтверджує міжнародна практика, – підвищення частки практичної складової підготовки. За оцінками, у середньому цей показник для бакалаврських та магістерських програм не перевищує 30%, тоді як потреби ринку праці та реальна природа кіберзагроз вимагають значно глибших практичних компетенцій. Бракує кіберполігонів, актуальних курсів із реагування на інциденти, форензіки та threat intelligence.

Одним із найбільш помітних зрушень стала системна переорієнтація освітніх програм на відповідність затвердженим профстандартам. Урядові структури рекомендували університетам інтегрувати стандарти у навчальні плани та використовувати їх для запровадження спеціалізацій[86]. Освітні програми окремих університетів вже відображають ці зміни – зокрема, магістерські програми з «Кібербезпеки» орієнтуються на вимоги Професійного стандарту «Адміністратор мереж і систем» та суміжних стандартів.

В умовах воєнного стану освіта зіткнулася з рядом нових виклики: відтік студентів і викладачів за кордон, мобілізація персоналу (особливо серед фахівців-практиків, яких залучали до викладання), скорочення контингенту у деяких регіонах. Ці фактори чинять тиск на якість підготовки та наповненість ринку праці.

У сфері міжнародного партнерства у 2025 році продовжував реалізовуватися проєкт USAID «Кібербезпека критично важливої інфраструктури України», у рамках якого здійснювалося підвищення практичних компетенцій викладачів в закордонних організаціях за напрямками реагування на інциденти, цифрової форензіки, безпеки кіберфізичних систем, аудиту, аналізу шкідливого програмного забезпечення тощо[87]. Заклади вищої освіти – учасники проєкту отримували також лабораторне обладнання та ліцензійне програмне забезпечення для розгортання практичних кіберполігонів. Загальна кількість університетів, охоплених проєктом, – більше 12, кількість охоплених викладачів - близько 300[88].

Одним із конкретних прикладів міжнародної освітньої діяльності у 2025 році стало замовлення наукових досліджень щодо підходів провідних держав світу до розвитку штучного інтелекту та принципів відповідальності за результати його використання, а також щодо міжнародних кіберстратегій у їх регіональному розрізі.

Окремою ініціативою у сфері освіти стало відкриття Держспецзв'язку у 2025 році безкоштовного онлайн-курсу «Кіберзахист для організацій» на платформі Києво-Могилянської академії, орієнтованого на широке коло учасників – від ІТ-фахівців до HR та

---

[85] Запускаємо CISO Campus - національну платформу підготовки керівників із кібербезпеки // thedigital.gov.ua. 18 листопада 2025. URL: https://thedigital.gov.ua/news/education/zapuskayemo-ciso-campus-natsionalnu-platformu-pidhotovky-kerivnykiv-iz-kiberbezpeky (дата доступу: 05.04.2026).

[86] Перший в Україні Кваліфікаційний центр інформаційних технологій та кібербезпеки розпочав сертифікацію спеціалістів // qc.csi.cip.gov.ua. 25 липня 2024. URL: https://qc.csi.cip.gov.ua/uk/posts/the-first-information-technology (дата доступу: 05.04.2026).

[87] Проєкт USAID «Кібербезпека критично важливої інфраструктури України» // ice.nure.ua. URL: https://ice.nure.ua/ua/international-cooperation/proiekt-usaid-kiberbezpeka-krytychno-vazhlyvoi-infrastruktury-ukrainy/ (дата доступу: 05.04.2026).

[88] Нові освітні програми з кібербезпеки в українських вишах мають базуватися на міжнародних стандартах та бути орієнтованими на здобуття практичних навичок – МОН // mon.gov.ua. URL: https://mon.gov.ua/news/novi-osvitni-programi-z-kiberbezpeki-v-ukrainskikh-vishakh-mayut-bazuvatisya-na-mizhnarodnikh-standartakh (дата доступу: 05.04.2026).

управлінців[89]. Ця ініціатива доповнює систему формальної вищої освіти та розширює доступ до кібербезпекових знань для фахівців без профільної підготовки.

Постійною лишається підтримка міжнародних партнерів в сфері розвитку кадрових ресурсів. У грудні 2025 року відбувся хакатон «Стратегічне планування та управління кібербезпекою» за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США[90], що свідчить про продовження активної двосторонньої співпраці у навчальній сфері. Також CRDF Global допоміг провести курс «Управління вразливостями» (VDP) – наразі ця програма об'єднала та посилила кіберзахист більше 300 організацій, а також програму IRD 4.0 для відпрацювання практичних сценаріїв реагування на кіберзагрози.

За підтримки Естонії (e-Governance Academy (eGA), CybExer Technologies та Estonian Centre for International Development (ESTDEV) та спільно з НКЦК було започатковано проєкт «UA-EE Cyber Shield via Tallinn Mechanism»[91] із підвищення практичних навичок 500 українських кіберфахівців державного сектору та ОКІ для запобігання, виявлення та реагування на кіберзагрозиЗа підтримки ЄС було організовано перший чемпіонат України з CTF. Японське агенство міжнародного співробітництва JICA виступило спонсором триденних інтегрованих кібернавчань Hackwave Reloaded 2025 для представників об'єктів критичної інфраструктури, енергетичного і телекомунікаційного секторів.

Важливим учасником цього процесу став і Талліннський механізм, який також системно підтримує розвиток кадрового капіталу у сфері кібербезпеки. За участі міжнародних партнерів проводяться тренінгові програми та навчальні заходи для державних службовців і фахівців із кібербезпеки. Зокрема, в 2025 році на базі CDTO Campus були організовані навчальні програми за підтримки Франції (у співпраці з Expertise France) та Німеччини (у співпраці з Monarch)[92].

Незважаючи на всі ці зусилля ситуація з науковим забезпеченням сфери кібербезпеки лишається надзвичайно складною. Загальна картина відображає значну фрагментарність: частина державних органів замовляє дослідження і планує їх імплементацію, інша - прямо вказує на відсутність будь-яких замовлень у 2025 році, ще одна – фіксує труднощі з трансфером результатів до практичної діяльності.

Серед тематичних кластерів замовлених досліджень виокремлюються два основні. По-перше, оборонна проблематика: проводились дослідження щодо загроз, пов'язаних із використанням шпигунського комерційного програмного забезпечення (spyware), результати яких розпочато імплементувати у практичну діяльність. По-друге, міжнародна стратегічна аналітика: замовлено дослідження за двома пов'язаними темами – підходи провідних держав до розвитку штучного інтелекту та відповідальності за його використання, а також порівняльний аналіз кіберстратегій та стратегій кіберстійкості в регіональному розрізі.

У сфері освітньої науки у 2025 році виконувались три ініціативні науково-дослідні роботи з метою оновлення змісту навчальних дисциплін та освітніх програм. Паралельно проводились дослідження у сферах кіберзахисту, штучного інтелекту та криптографії, однак їх імплементація в державні системи (SIEM, SOC, Kubernetes/OpenShift-платформи) залишається обмеженою і потребує вдосконалення механізмів трансферу технологій. Без ініціативного принципу та відповідного фінансування практичне використання наукових результатів залишається слабким місцем системи.

Ряд стейкхолдерів прямо повідомляє про відсутність замовлених або проведених досліджень у 2025 році. Водночас зафіксовано, що станом на початок 2026 року практично неможливо оцінити стан вітчизняних досліджень у сфері кібербезпеки через відсутність дієвої

[89] Долучайтеся до онлайн-курсу «Кіберзахист для організацій» // cip.gov.ua. URL: https://cip.gov.ua/ua/news/doluchaitesya-do-onlain-kursu-kiberzakhist-dlya-organizacii (дата доступу: 05.04.2026).
[90] НКЦК продовжує проводити навчальні заходи для державного сектору країни // rnbo.gov.ua. URL: https://www.rnbo.gov.ua/ua/Diialnist/4758.html (дата доступу: 05.04.2026).
[91] Про план реалізації Стратегії кібербезпеки України // rnbo.gov.ua. URL: https://www.rnbo.gov.ua/ua/Diialnist/5235.html (дата доступу: 05.04.2026).
[92] https://www.cdto-campus.com/en/faculties/tallinn-cybersecurity-mechanism

моделі координації. Окремі позитивні спроби реалізувати таку координацію на базі Міністерства освіти і науки у 2024–2025 роках не мали помітного продовження.

На рівні системної організації досліджень важливою є діяльність Національного фонду досліджень України (НФДУ). У 2025 році НФДУ оголосив конкурс «Наука для зміцнення обороноздатності і національної безпеки України» (терміни подання заяв: березень–квітень 2025 року, реалізація проєктів: 2025–2026 роки), у рамках якого кібербезпека – зокрема, кіберстійкість критичної інфраструктури та адаптивні системи кібербезпеки – визначена як один із пріоритетних напрямів[93]. За підсумками конкурсу переможцями стали 33 проєкти із 109 поданих заявок[94]. Паралельно НФДУ проводив конкурс прикладних досліджень «Передова наука» (заявки – квітень–травень 2025 року)[95], що відкриває фінансові можливості й для кібербезпекових досліджень.

Серед системних прогалин - відсутність національних досліджень у сфері штучного інтелекту, квантових технологій та постквантової криптографії. Окремою проблемою є відсутність дієвого координаційного механізму, здатного готувати регулярні звіти про стан наукового супроводу галузі та представляти інтереси наукового середовища у процесах формування державної кібербезпекової політики. Ця ситуація є проблемним сигналом для науково-технологічного розвитку галузі в перспективі.

Гендерний аспект кадрового забезпечення кібербезпеки набув у 2025 році якісно нового статусу: з периферійної теми він перетворився на предмет системної державної ініціативи. Активна роль у цьому належить Національному координаційному центру кібербезпеки, який розвиває відповідну Національну ініціативу із посилення ролі жінок в кібербезпеці, започатковану рішенням НКЦК у вересні 2024 року[96]. У вересні 2025 року за підтримки Консультативної місії ЄС відбувся воркшоп «Шлях жінок у кібербезпеці: історії, виклики, успіх», у рамках якого вперше в Україні були проведені жіночі кіберзмагання CTF for Women[97]. У листопаді 2025 року CDTO Campus оголошував набір на спеціальну програму для жінок з кібербезпеки[98].

Кількісні показники присутності жінок у сфері кібербезпеки відображають картину, типову для більшості країн: серед усього персоналу кібербезпекових підрозділів опитаних державних організацій жінки складають меншість. Водночас у їхньому середовищі вищою є частка тих, хто перебуває на управлінських і вищих посадах, ніж можна було б очікувати від стереотипних уявлень про галузь. У профільних підрозділах та особливо на керівних позиціях представленість жінок залишається нижчою, ніж у загальноорганізаційному вимірі.

Результати якісного дослідження з вибіркою із тридцяти жінок-фахівчинь виявили кілька стійких патернів кар'єрних викликів. Передусім – це гендерна динаміка на робочому місці: непряма дискримінація, прояви якої часто не усвідомлюються як дискримінація (мікроагресія, знецінення думки, підвищені вимоги до підтвердження компетентності порівняно з чоловіками-колегами). Значна частина учасниць дослідження також вказувала на

[93] Національний фонд досліджень України оголошує конкурс «Наука для зміцнення обороноздатності і національної безпеки України» // mon.gov.ua. 1 березня 2025. URL: https://mon.gov.ua/news/natsionalnyi-fond-doslidzhen-ukrainy-oholoshuie-konkurs-nauka-dlia-zmitsnennia-oboronozdatnosti-i-natsionalnoi-bezpeky-ukrainy (дата доступу: 05.04.2026).

[94] NRFU Scientific Council approved the rating list of projects of the Call 'Science to Strengthen Defense Capabilities of Ukraine' // nrfu.org.ua. 26 червня 2025. URL: https://nrfu.org.ua/en/news-en/scientific-council-of-the-nrfu-approved-the-rating-list-of-projects-submitted-to-the-call-science-to-strengthen-defense-capabilities-of-ukraine/ (дата доступу: 05.04.2026).

[95] Умови конкурсу «Передова наука» 2025 // nrfu.org.ua. 25 квітня 2025. URL: https://nrfu.org.ua/wp-content/uploads/2025/04/umovi_peredova_nauka_2025.pdf (дата доступу: 05.04.2026).

[96] Наталія Ткачук: НКЦК започатковує ініціативу з посилення ролі жінок у кібербезпеці // rnbo.gov.ua. URL: https://www.rnbo.gov.ua/ua/Diialnist/7042.html (дата доступу: 05.04.2026).

[97] Сила жіночого лідерства: НКЦК змінює українську кіберспільноту // rnbo.gov.ua. 5 вересня 2025. URL: https://www.rnbo.gov.ua/ua/Diialnist/7271.html (дата доступу: 05.04.2026).

[98] У CDTO Campus триває набір на дві програми для жінок: лідерство в цифровізації та кібербезпека // spacemag.com.ua. 8 квітня 2025. URL: https://spacemag.com.ua/fashion/news/u-cdto-campus-tryvaye-nabir-na-dvi-programy-dlya-zhinok-liderstvo-v-czyfrovizacziyi-ta-kiberbezpeka/ (дата доступу: 05.04.2026).

необґрунтовані затримки у кар'єрному просуванні та відчуття «скляної стелі» при просуванні до керівних позицій[99].

Сімейні обставини – зокрема, материнство – становлять окремий блок викликів. Відсутність гнучких умов праці та достатньої підтримки для батьків у більшості державних установ примушує жінок робити вибір між кар'єрою та родинними обов'язками, причому тягар цього вибору лягає непропорційно більше на жінок. Ця проблема загострилася в умовах воєнного стану, коли жінки нерідко стали єдиними опікунами дітей.

Доступ до навчання, сертифікацій та можливостей кар'єрного розвитку є менш рівноправним для жінок у ряді відомств. Участь у публічних заходах, конференціях, відрядженнях стикається зі специфічними обмеженнями та неформальними упередженнями. Водночас жінки-фахівчині виявляють помітну стійкість і адаптивність в умовах воєнного стану, часто займаючи активну позицію у питаннях розвитку власних компетенцій і побудові горизонтальних професійних зв'язків.

Ключовою системною рекомендацією, що формулюється за результатами досліджень, є потреба у прозорих і рівних процедурах кар'єрного просування, запровадженні менторських програм, підтримці материнства та гнучкості зайнятості, а також посиленні видимості жіночих рольових моделей у сфері кібербезпеки, особливо для студентської аудиторії.

Окрім описаних вище системних вимірів, 2025 рік відзначився кількома суттєвими подіями та тенденціями. У листопаді 2025 року набули чинності нові норми закону № 4336-IX, що встановлюють зобов'язання для державних установ щодо проведення регулярних інструктажів та тренінгів з кібергігієни для персоналу[100]. Відповідний урядовий порядок, що визначає чіткий порядок та відповідальних, набрав чинності у жовтні 2025 року, що фактично формалізує обов'язкову освітню діяльність у сфері кібергігієни для всього державного сектору.

У вересні 2025 року відбувся фінал Першого чемпіонату України з кіберзмагань у форматі CTF. Проведення таких заходів є важливим елементом позауніверситетської системи виявлення та розвитку кіберталантів. Водночас, за висновками аналітичних досліджень, позауніверситетська система підготовки кіберкадрів загалом не вирішує стратегічних проблем – вона виявляє таланти, однак не формує систематичну пропозицію кваліфікованих фахівців для державного сектору.

На рівні міжнародних партнерств у 2025 році зафіксована активна взаємодія з широким колом партнерів. Активно тривала співпраця з США (USAID, CRDF Global, Державний департамент), ЄС (Консультативна місія, Horizon Europe).

Слід зазначити структурну проблему, яку відображають джерела і яка залишається невирішеною: незважаючи на значний обсяг міжнародної допомоги та власні зусилля, Україна не має надійної статистичної бази щодо кіберкадрів. Без системного моніторингу кількості фахівців, їх кваліфікаційної структури, динаміки внутрішнього і зовнішнього відтоку довгострокове планування підготовки кадрів залишається орієнтовним і не може бути обґрунтовано підкріплено конкретними цільовими показниками.

ВИСНОВКИ

Принципова інституційна новація 2025 року в архітектурі Національної системи кібербезпеки полягає у включенні Міністерства закордонних справ до складу її основних суб'єктів – до цього МЗС не мало формального місця в системі, попри те що кібердипломатія як напрям фактично вже реалізовувалась. Це рішення є логічним наслідком зростання ролі

99 https://www.facebook.com/SvitlanaDubovaCADEP/posts/pfbid0rq2AMLqZPyhYhDyDXkCP9eMKq8igVEuLidqdbxjZSRJHH2gRYV3a87iwELXRCmjgl

100 Кіберстійкість через обізнаність: як Закон № 4336-IX змінює підходи до навчання у держсекторі // cip.gov.ua. 13 листопада 2025. URL: https://cip.gov.ua/ua/news/kiberstiikist-cherez-obiznanist-yak-zakon-4336-ikh-zminyuye-pidkhodi-do-navchannya-u-derzhsektori (дата доступу: 05.04.2026).

кібербезпекового виміру в зовнішній політиці України: атрибуція атак, координація санкційних заходів із партнерами, участь у міжнародних нормотворчих процесах потребували чіткого інституційного статусу виконавця. В усьому іншому архітектура системи залишилась практично незмінною: склад суб'єктів, розподіл їхніх повноважень і координаційна роль НКЦК зберігають наступність із попереднім періодом.

Разом із тим нормативна реформа 2025 року є найбільш масштабною в історії української системи кібербезпеки: Закон № 4336-IX разом із дев'ятьма постановами КМУ утворили якісно новий регуляторний каркас. Серед змін, що мають принципове значення, – відмова від КСЗІ на користь ризик-орієнтованого підходу на основі профілів безпеки, законодавче закріплення інституту CISO з прямою забороною суміщати цю роль із функцією цифрової трансформації, а також вперше введений у національне право термін «стратегічні кібероперації» з відповідним механізмом координації через НКЦК. Водночас реформа має два системних обмеження, які визначатимуть якість її реалізації. По-перше, сім із дев'яти підзаконних актів набули чинності у листопаді–грудні, що фактично унеможливило їх повноцінне впровадження у звітному році. По-друге, незавершеність ключових елементів – таксономії інцидентів, стандартизованих форм повідомлень, цифрової платформи обміну інформацією – утворює прямий розрив між законодавчо закріпленим обов'язком повідомляти про інциденти і практичним інструментом для цього. Окремо варто зафіксувати концентрацію в одному органі – Держспецзв'язку – регуляторних, операційних, стандартизаційних і контрольних функцій одночасно: така конструкція є структурно нестандартною і потребує осмисленого підходу з точки зору інституційних стримувань. Понад чотирирічна відсутність правової основи для Кіберсил ЗСУ, за наявності активного збройного конфлікту, є не технічною прогалиною, а стратегічним дефіцитом, який жодна підзаконна реформа не компенсує.

Загальна операційна динаміка 2025 року є позитивною за всіма основними напрямами. Кількість інцидентів критичного та високого рівня скоротилась із 59 до 12, показник реалізації Стратегії кібербезпеки зріс до 86%. Система Protective DNS із підключенням понад 500 провайдерів заблокувала близько 72 тисяч фішингових ресурсів, захист кінцевих точок охопив 46,5 тисяч серверів і робочих станцій. Організаційно нарощено спроможності кібероборони ЗСУ, виокремлено кіберзахисні підрозділи в МЗС і Мінцифри, розпочато формування регіональних центрів Держспецзв'язку. Проведено близько 100 навчальних заходів. Через Талліннський механізм мобілізовано понад 61 млн євро технічної допомоги, укладено 9 нових меморандумів із країнами-партнерами, вперше направлено національного експерта до ENISA на постійній основі, ініційовано створення Кіберальянсу Україна–Румунія–Молдова.

Загрозовий ландшафт ускладнився одночасно за кількома вимірами. Російські APT-групи змістили пріоритет із масованих деструктивних атак на тривале стратегічне закріплення в системах – з акцентом на сектор безпеки і оборони, електронні комунікації, енергетику, логістику та підприємства оборонно-промислового комплексу і виробників безпілотних систем. Окремим вектором стало зміщення атак на регіональний рівень – місцеві органи влади та комунальну інфраструктуру прифронтових областей. Група UAC-0001/APT28 почала застосовувати LLM безпосередньо у шкідливому програмному забезпеченні для генерації коду в реальному часі, що суттєво ускладнює виявлення традиційними засобами захисту. Передача державних кіберінструментів, зокрема ПЗ Pegasus, підконтрольним злочинним групам означає неконтрольоване поширення засобів, що раніше були доступні виключно державним акторам. Конфлікт вийшов за межі двостороннього: зафіксовано спільне використання інфраструктури групами Gamaredon і Lazarus для атак на оборонні підприємства Європи та українських виробників безпілотних систем. Кампанія «Чорна зима» унаочнила усталену доктрину противника – синхронізацію ракетних ударів по енергетиці з кібератаками та дезінформаційними операціями як єдиного комплексу впливу.

До Реєстру об'єктів критичної інфраструктури внесено відомості про понад 4600 об'єктів –- з них 2046 додано протягом року; погоджено 1306 паспортів безпеки. Ситуаційний центр СБУ обробив майже 290 млрд подій безпеки, нейтралізував 1169 загроз високого рівня та припинив 3010 критичних інцидентів; система ДЦКЗ Держспецзв'язку попередила 730

інцидентів на 97 підключених організаціях. CSIRT-NBU проаналізував близько 2 тисяч зразків шкідливого ПЗ і надіслав 340 повідомлень через платформу MISP-NBU до 60 банків.

Окремим структурним викликом залишається те, що частина приватних підприємств критичної інфраструктури свідомо уникає отримання статусу ОКІ або штучно занижує категорію критичності, щоб уникнути регуляторного навантаження.

Загальний показник реалізації Стратегії кібербезпеки склав 86% у порівнянні з 32% у 2022 році. З 93 оцінених завдань 64 виконано повністю; 38% завдань мають прострочені терміни виконання. У розрізі напрямів найвищий показник демонструє «Кіберстійкість» – 97%. Напрям «Вдосконалення взаємодії» реалізовано на 88%. Напрям «Стримування» має найнижчий показник – 76%, хоча продемонстрував найвищий приріст за рік – 35%; його ключовим невиконаним завданням залишається законодавче забезпечення Кіберсил ЗСУ. Серед системних причин неповного виконання планових заходів: недостатність бюджетного фінансування; неузгодженість між документами стратегічного планування і урядовими планами дій; виклики правового режиму воєнного стану.

Закон № 4336-IX вперше законодавчо закріпив обов'язок органів місцевого самоврядування призначати відповідальних за кіберзахист. Реалізація цієї вимоги відбувається нерівномірно: більшість ОМС здійснили формальне призначення, тоді як затверджені плани реагування на кіберінциденти у відкритих джерелах не виявлені. На платформі Дія.Освіта загальна кількість реєстрацій перевищила 3 млн, близько 1 млн громадян пройшли навчання з кіберграмотності, тема кібергігієни набрала 1,1 млн переглядів. Демографічний профіль платформи показує, що 70,9% користувачів навчаються зі смартфонів, домінуюча вікова група – 31–60 років; сегмент 65+, внутрішньо переміщені особи та мешканці прифронтових районів залишаються поза охопленням, і жодне з відомств не визначило це як окрему стратегічну проблему. Представлено проєкт Національної стратегії кібергігієни з горизонтом до 2030 року. Самостійного корпусу незалежних досліджень кіберстійкості на рівні громад не зафіксовано: наявні дані оперують технічними або освітніми показниками, але не соціологічними вимірами фактичної поведінки та обізнаності конкретних спільнот. НУО-сектор залишається фінансово нестабільним і проєктно залежним переважно від американських та канадських донорів без гарантованого продовження програм.

Кібердипломатія розвивалась одночасно у кількох напрямах. З ЄС проведено четвертий раунд кібердіалогу з фокусом на імплементацію NIS2, доступ до Кіберрезерву ЄС та запровадження кіберсанкцій; вперше відбувся кібердіалог з Нідерландами. Підписано меморандум з ЕССС, Україна вперше взяла участь у засіданні його Керівної ради і подала запит на членство та залучення до програми Digital Europe. Українська команда дебютувала на European Cybersecurity Challenge і подала заявку на проведення ECSC 2026; у квітні вперше перемогла на хакатоні НАТО. Створено проєктний офіс Талліннського механізму Tallinn Mechanism Project Office (TMPO). Структурно значущою є зміна донорського балансу: внаслідок ліквідації USAID та обмеження американської допомоги роль основного донора перейшла до європейських партнерів і Канади – зокрема, Канада виділила 92 млн грн на стратегічні ініціативи. Другий Київський міжнародний форум кіберстійкості зібрав понад 1000 учасників із 35 країн.

Кадровий дефіцит у сфері кібербезпеки залишається структурно невирішеною проблемою. Його оцінки варіюються від кількох тисяч до 100 тисяч осіб – сама ця розбіжність свідчить про відсутність надійної статистичної бази, без якої довгострокове планування підготовки кадрів залишається орієнтовним. Визначальною причиною дефіциту є структурний дисбаланс оплати праці між державним і приватним секторами. На бакалаврат подано 22 735 заяв при зарахуванні 3753 осіб – співвідношення 6:1 відображає обмежену ліцензійну ємність програм. Практична складова підготовки в бакалаврських та магістерських програмах у середньому не перевищує 30%, бракує кіберполігонів і курсів з реагування на інциденти, форензіки та threat intelligence. За результатами ЄДКІ поріг не подолали 15,35% студентів-бакалаврів. Відкрито CISO Campus для підготовки керівників з кібербезпеки в державних установах.

Науковий вимір є найбільш проблемним: частина відомств не замовляла жодних досліджень, механізм трансферу результатів у практичну діяльність відсутній, координаційна функція на рівні системи не реалізована, а національні дослідження у сферах штучного інтелекту, квантових технологій та постквантової криптографії відсутні.

Гендерний вимір перейшов від декларативного до інституційного: в рамках Національної ініціативи з посилення ролі жінок в кібербезпеці, започаткованій НКЦК, проведено перші жіночі кіберзмагання CTF for Women; відкрито окрему програму підготовки для жінок; якісне дослідження 30 жінок-фахівчинь зафіксувало стійкі патерни непрямої дискримінації, «скляної стелі» та непропорційного тягаря материнства в умовах воєнного стану, що вказує на потребу системних змін на національному рівні.

РЕКОМЕНДАЦІЇ ТА НАСТУПНІ КРОКИ

Організаційно-правові заходи

- Оновити Стратегію кібербезпеки України з урахуванням актуального ландшафту кіберзагроз, пріоритетів та потреб розвитку національної системи кібербезпеки;
- Вдосконалити механізми відповідальності за порушення вимог у сфері кібербезпеки;
- Унормувати підходи до забезпечення безпеки ланцюгів постачання;
- Прийняти нормативно-правові акти, необхідні для створення та забезпечення функціонування в Україні кіберсил;
- Унормувати організаційні питання взаємодії та координації суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям, а також реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки;
- Завершити гармонізацію законодавства України із законодавством ЄС у сфері кібербезпеки;
- Імплементувати Регламент ЄС про цифрові послуги (Digital Services Act), ратифікувати Другий додатковий протокол до Конвенції про кіберзлочинність, імплементувати європейські норми щодо захисту персональних даних (GDPR);
- Унормувати питання державно-приватного партнерства у сфері кібербезпеки;
- Узгодити норми законодавства та термінологію у сфері кіберзахисту та захисту інформації в ІКС, у тому числі щодо систем, де циркулює державна таємниця.

Разом із тим, з урахуванням прийняття у 2025 році значної кількості НПА, спрямованих на посилення кібербезпеки України та створення для цього відповідних нормативно-організаційних інструментів, одним із ключових викликів залишається організація та проведення практичних та методологічних навчань для відповідальних посадових осіб державного сектору та ОКІ з метою забезпечення їх правильного розуміння та застосування.

Міжнародне співробітництво

- Закріпити регіональне лідерство України у сфері кібербезпеки як окремий стратегічний пріоритет в оновленій Стратегії кібербезпеки України, формалізувавши її роль як експортера кіберекспертизи та невід'ємного елемента європейської кіберекосистеми;
- Формалізувати участь України у European Cyber Competence Centre (ECCC) та забезпечити отримання НКЦК статусу NCC-UA як національного координатора у мережі координаційних центрів з кібербезпеки ЄС;
- Масштабувати співпрацю у сфері кібербезпеки на Східну Європу, Балкани та Близький Схід;
- Забезпечити розвиток регіонального кіберальянсу «Україна – Румунія – Молдова»;

- Запустити спільні кібернавчання (ТТХ, CTF) з країнами-партнерами на базі української інфраструктури, практичного досвіду та експертного потенціалу;
- Розвивати спільну атрибуцію кібератак та координацію кіберсанкцій з метою посилення санкційного тиску на рф;
- Консолідувати підтримку партнерів щодо проведення у 2026 році Міжнародного київського форуму кіберстійкості;
- Створити за підтримки країн-партнерів в Україні Міжнародний центр компетенції з кіберстійкості як платформу міжнародної взаємодії у сфері кібербезпеки.

Освіта та наука, розвиток кадрового потенціалу

- Сформувати Національну стратегію розвитку кіберкадрів до 2030 року із чіткими прогнозами потреб державного сектору, оборонної сфери, критичної інфраструктури та регіонального рівня. Запровадити щорічний національний звіт про стан кіберкадрів і наукового забезпечення кібербезпеки, як інструмент стратегічного управління та корекції державної політик;
- Запровадити конкурентні механізми оплати праці у державному секторі, включно зі спеціальними надбавками для критично важливих кіберпосад, гнучкими контрактами, преміальними моделями та програмами утримання ключових фахівців;
- Завершити формування Національної рамки кваліфікацій у сфері кібербезпеки, синхронізованої з NICE NIST та ECSF ENISA, а також забезпечити її обов'язкове використання у державних органах під час добору кадрів і планування навчання;
- Модернізувати освітні програми ЗВО, збільшивши частку практичної підготовки щонайменше до 50%, із розвитком кіберполігонів, лабораторій, стажувань, дуальної освіти та участі роботодавців у формуванні навчальних планів;
- Розширити державне замовлення на спеціальність F5 "Кібербезпека та захист інформації" з орієнтацією на потреби державного сектору, а також запровадити цільові стипендії та контракти із подальшим працевлаштуванням;
- Посилити науковий компонент кібербезпеки, створивши національну програму прикладних досліджень за пріоритетами: штучний інтелект, постквантова криптографія, безпека критичної інфраструктури, кіберстійкість державних систем, безпека defense tech;
- Розвивати гендерну інклюзивність у галузі, зосередившись на менторських програмах, прозорому кар'єрному просуванні, підтримці батьківства/материнства, спеціальних освітніх програмах для жінок та популяризації жіночих рольових моделей у кібербезпеці;
- Масштабувати програми кібергігієни для всього державного сектору, забезпечивши обов'язкове щорічне навчання персоналу, тестування знань та симуляції фішингових атак;
- Розвивати систему раннього виявлення талантів, підтримуючи CTF-змагання, хакатони, шкільні та студентські ліги, регіональні кібертабори та програми залучення молоді до кіберпрофесій.

Посилення кіберстійкості

- Посилити захист військових систем управління, зв'язку та ситуаційної обізнаності, шляхом впровадження сегментації мереж, резервних каналів зв'язку, захисту польових цифрових систем та безпечного використання месенджерів військовослужбовцями;
- Створити окрему програму кіберзахисту оборонно-промислового комплексу та виробників БПЛА, що передбачатиме аудит безпеки, захист ланцюгів постачання, перевірку програмного забезпечення та безпеку виробничих майданчиків;

- Підвищити кіберстійкість критичної інфраструктури шляхом впровадження обов'язкових планів безперервності діяльності, резервного управління, аварійного відновлення, автономних резервних копій та регулярних кризових навчань;
- Зосередити додаткові ресурси на регіональному рівні, особливо у прифронтових областях, створивши регіональні центри кіберстійкості для підтримки місцевої влади, ОКІ, комунальних підприємств та локальних операторів зв'язку;
- Прискорити заміну застарілих IT та OT/ICS/SCADA систем, насамперед у критичній інфраструктурі, із пріоритетом для енергетики, водопостачання, транспорту та зв'язку;
- Заборонити використання неліцензійного ПЗ та неконтрольованих особистих пристроїв у державному секторі, впровадивши політики BYOD, MDM-рішення та централізований контроль кінцевих точок;
- Створити національну систему протидії ШІ-загрозам, включаючи виявлення AI-фішингу, дипфейків, автоматизованих кампаній впливу та шкідливого ПЗ із елементами ШІ;
- Інтегрувати штучний інтелект у кіберзахист держави, використовуючи його для аналізу журналів подій, виявлення аномалій, автоматизації SOC-процесів та прогнозування атак;
- Розпочати підготовку до постквантового переходу, створивши дорожню карту міграції державних криптографічних систем на постквантові алгоритми та інвентаризацію критичних криптозалежних сервісів;
- Посилити захист ланцюгів постачання у сфері кібербезпеки та цифрових послуг, зокрема постачальників програмного забезпечення, хмарних сервісів, операторів телекомунікацій і критично важливих ІКТ-підрядників;
- Сформувати довгострокову стратегію цифрового суверенітету України, спрямовану на зменшення критичної залежності від вузького кола зовнішніх постачальників технологій, хмарної інфраструктури та безпекових сервісів.

Проактивна кібероборона

- Завершити формування та набуття спроможностей Кіберсилами Збройних Сил України;
- Забезпечити стратегічне планування та дієву координацію наступальних кібероперацій стратегічного рівня;
- Розвивати проактивну кібероборону та активне полювання на загрози (threat hunting), зосередившись на ранньому виявленні проникнень у державні системи, військові мережі, енергетику, транспорт та телекомунікації;
- Створити кіберрезерв, як кадрову основу для національної системи кібербезпеки та кризового реагування;
- Забезпечити скоординованість проактивних заходів інформаційного та кібердоменів;
- Розробити національні інструменти для проведення проактивних кібероперацій, зокрема з інтеграцією можливостей ШІ;
- Забезпечити підготовку фахівців в інтересах проактивної кібероборони шляхом розробки та впровадження відповідних навчальних програм для суб'єктів сектору безпеки і оборони – основних суб'єктів кібербезпеки;
- Масштабувати кібернавчання воєнного типу із обов'язковим включенням кіберкомпоненти.

Державно-приватне партнерство

- Розробити та впровадити Концепцію розвитку державно-приватного партнерства у сфері кібербезпеки та план її реалізації із визначенням чітких кроків та індикаторів виконання;
- Забезпечити обов'язкове залучення українських компаній до реалізації проєктів міжнародної технічної допомоги у сфері кібербезпеки;

- Забезпечити стале державне замовлення для вітчизняних IT- та кібербезпекових компаній;
- Сприяти розвитку експортного потенціалу українсього IT- та кібербезпекового бізнесу, зокрема шляхом адвокації української експертизи та технологій на міжнародній арені, залучення інвестицій, започаткування спільних міждержавних проєктів;
- Розробити механізм сталої підтримки неурядових організацій з метою зменшення їхньої повної залежності від іноземного грантового фінансування.