Проєкт

Стратегія кібербезпеки України (2021 – 2025 роки)

БЕЗПЕЧНИЙ КІБЕРПРОСТІР – ЗАПОРУКА УСПІШНОГО РОЗВИТКУ КРАЇНИ

1. КІБЕРБЕЗПЕКА: ГЛОБАЛЬНИЙ КОНТЕКСТ

Стратегія кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Формуючи нову Стратегію кібербезпеки України, ми враховуємо світові тренди в глобальному кіберсередовищі як фактори впливу на розбудову національної системи кібербезпеки.

XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі.

Питома вага кіберзагроз у спектрі загроз національній безпеці країн зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів.

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об’єктів противника шляхом руйнування інформаційних систем, які управляють такими об’єктами.

Водночас все більш активно застосовується поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Зокрема, Російська Федерація активно реалізує концепцію інформаційного протиборства, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України. Країни ЄС, НАТО, провідні міжнародні компанії та експерти одностайно визнають Російську Федерацію і її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її розвідувально-підривна діяльність у кіберпросторі є частиною гібридної війни, яку вона веде проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі, що проявлятимуться, насамперед, у розширенні кола держав, які намагатимуться сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилити державний контроль за національними сегментами мережі Інтернет. При цьому набуватиме поширення розроблення інструментарію, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використовує сучасні досягнення у сфері штучного інтелекту.

Негативною ознакою технологічного розвитку, пов’язаного із всеохоплюючим поширенням цифрових технологій, розширенням Інтернет-середовища, є критично зростаючий технічний рівень інструментарію реалізації кіберзагроз, від чого ландшафт таких загроз охоплює все більше сфер життєдіяльності. Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критично важливій інфраструктурі. Зловмисники зосереджують зусилля на пошуку вразливостей активів (систем управління) і розробляють для цього унікальні за своїми властивостями: багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети, що здійснюють розподілені атаки (DDoS) на операційні мережі, виробничі системи, які використовують хмарні сервіси, атаки на ланцюги поставок. З урахуванням розвитку технологій штучного інтелекту в найближчі 5-10 років масштаби та наслідки таких втручань зростатимуть.

Масштабу глобального тренда набуває використання кіберпростору терористичними організаціями (кібертероризм). Цьому сприятимуть всеохоплююча цифрова трансформація систем управління та життєзабезпечення, що невпинно розширює цільову аудиторію кібертероризму та спектр потенційних об’єктів кібератак. Пріоритетними об’єктами терористичних кібератак вважаються об’єкти атомної енергетики, системи управління електропостачанням, авіа- та залізничним транспортом, потужні сховища стратегічних видів сировини, системи водопостачання, хімічні й біологічні об’єкти.

Нові виклики несе з собою перехід на 5G-мережі, функціонування яких кардинальним чином залежить від коректної роботи програмного забезпечення, що за рахунок новизни технології може мати нові, не повною мірою передбачені загрози. Технології «Інтернет речей», «розширена реальність», «розумне місто» активно доповнюються новими – «гіперавтоматизація», «розумно компонований бізнес», «кібербезпекова сітка», «розподілена хмара», «Інтернет-поведінка» тощо.

Докорінно змінюючи світовий життєустрій, пандемія коронавірусу COVID-19 матиме довготривалий вплив на світовий порядок. Зростає залежність від цифрових комунікацій, що робить вразливим процес обміну інформацією, захисту інформації та персональних даних. Кіберзлочинці, максимально використовуючи тему пандемії, від її початку все більше застосовують нові методи проведення кібератак, що змушує національні уряди впроваджувати додаткові механізми протидії, збереження доступу до необхідних пристроїв, належного функціонування всіх потрібних для життя та роботи електронних ресурсів і систем.

Поширення ландшафту загроз та ускладнення інструментарію їх реалізації спонукає уряди провідних країн удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам. Вносяться зміни до моделі протидії кіберзагрозам, які пов’язані з розумінням недостатньої можливості побудувати абсолютно невразливі системи захисту. Як показує практика, будь-які інформаційно-комунікаційні системи можуть бути уражені внаслідок кібератаки незалежно від рівня їх захисту. Тому набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя.

Ми творимо Україну здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб’єктів забезпечення кібербезпеки на засадах партнерства та співпраці.

2. СТАН РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ НА 2016 – 2020 РОКИ

Прийняття у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері, а отже, сам факт її прийняття є позитивним результатом.

За ці роки було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який є правовим підґрунтям для створення національної системи кібербезпеки та виконання її основними суб'єктами завдань у сфері кібербезпеки.

Удосконалено нормативне забезпечення з питань кіберзахисту критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту.

Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України (Збройних Силах України).

Розбудовується Національна телекомунікаційна мережа, функціонують захищені центри обробки даних (дата-центри), утворюється Національний центр резервування державних інформаційних ресурсів, розпочато функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

З метою покращення координації діяльності суб'єктів забезпечення кібербезпеки було утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері.

Активно розвивається співпраця з іноземними партнерами, поглиблюється співробітництво України з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій.

Започатковано проведення щорічного заходу – місяця кібербезпеки.

Водночас діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Організація і проведення наукових досліджень у сфері кібербезпеки всіма експертами визначаються як недостатні.

Отриманий протягом часу дії Стратегії досвід надав змогу виокремити низку системних проблем, які або ускладнювали, або унеможливлювали її ефективну реалізацію.

Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Реалізація Стратегії була

ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення.

Не були розроблені індикатори виконання Стратегії, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади.

Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично.

Нова Стратегія кібербезпеки України враховує цей досвід і проблеми та визначає механізми реалізації Стратегії на наступний п'ятирічний період.

3. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ: ЗАСАДИ РОЗБУДОВИ

Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток.

Реалізуючи Стратегію кібербезпеки України на 2016 – 2020 роки, держава змогла сформувати ядро національної системи кібербезпеки. Україна наростила потенціал, який дає можливість здійснювати подальшу розбудову національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії.

З цією метою Україна:

посилить спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

набуде здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримуватиме стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

забезпечить розвиток комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом і НАТО та їх державами-

членами, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Розбудова національної системи кібербезпеки на таких засадах дасть можливість розширити запропоновані та рекомендовані дії на всі галузі економіки та сфери діяльності.

З цією метою держава залучить до вирішення завдань щодо забезпечення кібербезпеки в національному масштабі крім основних суб'єктів національної системи кібербезпеки, на яких спиралася на початковій стадії формування національної системи кібербезпеки, широке коло суб'єктів забезпечення кібербезпеки, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки.

Держава розбудовуватиме національну систему кібербезпеки, ґрунтуючись на:

всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України у сфері кібербезпеки;

перманентності заходів з удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо її актуалізації відповідно до безпекових умов, що змінюються;

орієнтованості на суспільство, що сприятиме його економічному і соціальному зростанню;

використанні принципу мінімальної достатності ролі держави у процесах розвитку та забезпечення безпеки кіберпростору, встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет;

збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту, повазі до основоположних цінностей, прав людини і особи на свободу вираження думки, такому самому захисті загальновизнаних основоположних прав в онлайн-середовищі, як і в офлайновому; засудженні практики перевищення встановлених меж необхідності щодо обмеження прав громадян та юридичних осіб під час використання кіберпростору та ІКТ-технологій;

відкритості та створенні умов для активної участі всіх заінтересованих сторін з урахуванням їх потреб і зобов'язань в умовах, коли кібербезпека цифрового середовища набула надважливого значення для держави, суспільства і громадян;

визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності, застосування стимулюючих механізмів та обміну унікальними знаннями і досвідом;

ризик-орієнтованому підході в частині заходів забезпечення кібербезпеки та кіберзахисту;

співпраці та інклюзивному діалозі всіх суб’єктів забезпечення кібербезпеки, зокрема в рамках державно-приватного партнерства, задля досягнення стратегічних цілей, заснування ініціатив, вироблення узгоджених планів та проєктів у сфері кібербезпеки;

впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки, у тому числі тих, що базуються на стратегічному плануванні та управлінні, кризовому управлінні, партнерських відносинах між державою, бізнесом та суспільством;

збалансованому розподілі наявних матеріальних і фінансових ресурсів, а також оптимальному застосуванні для вирішення кожного конкретного завдання у сфері кібербезпеки таких важелів, як законодавство, стандартизація, освітні програми, механізми стимулювання та зміцнення довіри, обмін інформацією і передовим досвідом;

проактивному підході, що передбачає здійснення випереджувальних заходів, зокрема застосування систем попередження кібератак, зміщуючи організаційний та технологічний фокус від боротьби з наслідками до протидії кібератакам на ранніх стадіях;

забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки, а саме дотриманням вимог Конституції і законів України суб'єктами забезпечення кібербезпеки, станом реалізації стратегічних документів, концепцій, державних програм та планів у сфері кібербезпеки, ефективністю використання ресурсів, зокрема бюджетних коштів.

4. НАЦІОНАЛЬНИЙ КІБЕРПРОСТІР: ВИКЛИКИ ТА КІБЕРЗАГРОЗИ

ВИКЛИКИ

Прискорений розвиток та взаємопроникнення інформаційних технологій поряд із потужними соціально значимими перевагами супроводжується масштабуванням кіберзагроз на всі сфери життєдіяльності, їх еволюцією вбік високотехнологічних рішень та урізноманітненням інструментарію реалізації.

Україна має необхідний потенціал для нарощування спроможностей у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.

Викликами для України у сфері кібербезпеки є:

активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, змагальний характер розвитку засобів кібербезпеки та реалізації кіберзагроз у процесі швидких прогресуючих змін інформаційно-комунікаційних технологій, хмарних обчислень, 5G-мереж, великих даних, Інтернету речей, машинного навчання/штучного інтелекту (AI) тощо;

мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї, які дають можливість здійснювати приховане проведення противником кібератак та кібероперацій, віддаленого взяття під контроль

систем управління, завдання шкоди та руйнування критичної інформаційної інфраструктури;

зростання технологічного рівня протиправних посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій;

вплив на економічну діяльність та соціальну поведінку поширення пандемії COVID-19, що спричинило швидку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем. Це посилило загрозу порушення прав громадян під час використання кіберпростору.

Цифрова трансформація, що є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Упровадження нових технологій, цифрових послуг та механізмів взаємодії громадян з державою, включаючи виборчий процес, створює велику кількість прихованих взаємозв'язків на рівні технологій і процесів. Без системного підходу до кібербезпеки та оцінки ризиків існує ймовірність втрати довіри громадян до процесів цифрової трансформації.

ЗАГРОЗИ

Сучасні світові тренди розвитку кібербезпекового середовища, виклики для країни, внутрішні процеси та явища сформували такі загрози кібербезпеці України.

З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об'єкти критичної інфраструктури. Держава-агресор невпинно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей забезпечення кібербезпеки органами сектору безпеки і оборони.

Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед Російської Федерації, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій).

В Україні в останні роки відчутно зросла загроза кібертероризму. Насамперед, це пов'язано з кіберможливостями держави-агресора Російської Федерації, яка веде проти України кібервійну із застосуванням кіберзброї.

Спостерігається використання кіберпростору для фінансування терористичних угруповань. Водночас недостатньою є взаємодія України з міжнародними партнерами щодо опрацювання на взаємовигідній основі механізмів протидії кібертероризму.

Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення інших злочинів (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація ускладнюється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг.

Державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури, які призначені для забезпечення задоволення життєво важливих потреб громадянина, особи, суспільства і держави, є недостатньо захищеними від кібератак.

Державні органи, приймаючи рішення про автоматизацію процесів державного управління, не завжди оцінюють ризики, що виникають у кіберзахисті державних інформаційних ресурсів. Захист інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина службової інформації та персональних даних громадян, не відповідає вимогам законодавства, що посилює ризики втручання в такі системи, загрожує конфіденційності, цілісності та доступності інформації (реєстри, бази даних), яка призначена для задоволення потреб та забезпечення конституційно гарантованих інтересів, громадян, суспільства і держави.

Висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам.

Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі.

Базовий ландшафт інструментарію реалізації окреслених кіберзагроз характеризується зростанням високотехнологічної складової та різноманіттям.

Безперервно збільшується кількість кібератак, спрямованих на викрадення персональних та інших конфіденційних даних громадян та організацій із використанням методів соціальної інженерії.

Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних країні-агресору та іншим країнам.

Збільшення інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах створило глобальний ринок для розвитку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет.

Усе частіше спрямовані кібератаки не здійснюються напряму на уряди та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до великої кількості їх клієнтів та завдання масштабної шкоди.

Популярні веб-сайти, соціальні мережі, реєстри збирають велику кількість ідентифікаційних та персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

Передумови та чинники, які формують окреслені загрози:

недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

5. ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ ТА СТРАТЕГІЧНІ ЦІЛІ

Пріоритетами забезпечення кібербезпеки України є:

убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

захист прав, свобод і законних інтересів громадян України у кіберпросторі;

європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії.

Для формування потенціалу **стримування** (С) до 2026 року маємо досягти таких стратегічних цілей:

Ціль С.1. Дієва кібероборона. Україна має не лише створити та розвивати ефективні (у тому числі кадрово та технологічно) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, що неможливо без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності.

Ціль С.2. Посилення спроможностей у протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму. Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян.

Ціль С.3. Посилення спроможностей у протидії кіберзлочинності. Правоохоронні та державні органи спеціального призначення з правоохоронними функціями набудуть спроможностей для мінімізації загроз кіберзлочинності, посилять свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів.

Ціль С.4. Розвиток асиметричних інструментів стримування. Створимо необхідні умови для забезпечення стримування агресивних дій у

кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору.

Для набуття **кіберстійкості** (К) національною системою кібербезпеки маємо до 2026 року досягти таких стратегічних цілей:

Ціль К.1. Посилення національної кіберготовності та кіберзахист. Запровадити і реалізовувати чіткі та зрозумілі для всіх стейкхолдерів заходи з посилення національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав та свобод кожного українського громадянина. Кіберготовність полягає у здатності всіх стейкхолдерів, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед об’єктів критичної інформаційної інфраструктури.

Ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки. Провести докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Забезпечити збереження наявного кваліфікованого кадрового потенціалу суб’єктів кібербезпеки. Стимулювати дослідження і розробки у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Кібергігієна, цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід’ємними елементами освіти кожного українського громадянина.

Ціль К.3. Безпечні цифрові послуги. Досягнемо балансу між потребами українського суспільства, вітчизняного ринку, економіки держави та необхідністю забезпечити безпеку в кіберпросторі. Забезпечимо надійність та безпеку цифрових послуг з моменту створення та протягом усього їхнього життєвого циклу.

Взаємодія (В) буде вдосконалена досягненням до 2026 року таких стратегічних цілей:

Ціль В.1. Зміцнення системи координації. Держава створить умови для ефективної взаємодії суб’єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів. Скоординуємо діяльність усіх стейкхолдерів задля подолання кризових ситуацій у кібербезпеці.

Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки. Ми запровадимо сервісну модель державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки.

Ціль В.3. Прагматичне міжнародне співробітництво. Спрямуємо відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

6. СТРАТЕГІЧНІ ЗАВДАННЯ

Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

На засадах стримування:

Україна сформує систему дієвої кібероборони шляхом *(ціль С.1):*

утворення у складі Збройних Сил України окремого роду військ – сил кібероборони, забезпечивши його належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору;

запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

забезпечення постійного моніторингу електронних комунікаційних мереж та інформаційних ресурсів домену «ua», здійснення аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій щодо їх функціонування;

розроблення та виконання плану кібероборони як складової частини Плану оборони України;

проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності;

створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею (Military CERT-Network);

забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів та оглядів у сфері кібербезпеки;

запровадження у систему військово-патріотичного виховання та систему територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки.

Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом *(ціль С.2):*

створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури, призначеної для моніторингу кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації, оперативного реагування на цільові та масштабні кібератаки;

удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів;

забезпечення максимального охоплення об'єктів критичної інфраструктури негласною перевіркою стану їх готовності до можливих кібератак та кіберінцидентів з метою превентивного усунення передумов до реалізації кіберзагроз;

забезпечення постійного моніторингу розвитку кіберспроможностей міжнародних терористичних угруповань, спрямованого на своєчасне виявлення і нейтралізацію реальних та потенційних загроз скоєння на території України актів кібертероризму;

посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-галузі, афілійованого з ними середовища, спрямованого на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України у сфері кібербезпеки;

створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності;

вдосконалення нормативно-правового, організаційного та кадрового забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму.

Україна посилить спроможності у протидії кіберзлочинності *(ціль С.3)*, задля цього необхідно:

провести аудит імплементації в українське законодавство положень Конвенції про кіберзлочинність та завершити цей процес шляхом внесення необхідних змін до законів України;

врегулювати на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики та підхід країн-членів ЄС з цих питань;

вдосконалити законодавство України, передбачивши внесення необхідних змін з урахуванням сучасних викликів та тенденцій у сфері кібербезпеки;

запровадити практику проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством, поширенням шкідливого програмного забезпечення або порнографічного контенту, іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах;

розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечити проведення таких досліджень;

розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити всі необхідні умови для її практичної реалізації;

запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

врегулювати на законодавчому рівні правовий статус криптовалют, визначити правові механізми щодо операцій із криптовалютами та створення ринків;

провести спільні з ЄС заходи в рамках Програми з питань розбудови зовнішнього кіберпотенціалу ЄС та підтримки партнерів для підвищення їхньої стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози;

забезпечити підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів;

сприяти розвитку інноваційних методів та технологій цифрової криміналістики;

забезпечити підвищення рівня знань оперативних працівників, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження цифрових (електронних) доказів;

сприяти залученню приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів.

Держава запровадить асиметричні інструменти стримування *(ціль С.4), для цього буде*:

утворено постійно діючу робочу групу з питань кіберрозвідки, налагоджено її ефективну співпрацю з Розвідувальним та ситуативним центром ЄС (INTCEN) з метою просування стратегічної співпраці України у сфері розвідки щодо кіберзагроз та діяльності у сфері кібербезпеки;

удосконалено систему розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці у кіберпросторі;

посилено заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів дипломатичних представництв, консульських установ та об'єктів державної власності України за кордоном;

створено технологічні можливості підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів;

запроваджено гармонізований з євроатлантичною спільнотою підхід до накладання санкцій у відповідь на підривну діяльність у кіберпросторі, розроблено та узгоджено з іноземними партнерами механізм спільних дипломатичних та економічних дій та заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність;

визначено чіткий порядок всебічної дипломатичної реакції із застосуванням доступних на міжнародному рівні інструментів задля протидії зловмисній діяльності у кіберпросторі проти України;

налагоджено систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед країнами-членами ЄС та НАТО, створено платформи такого обміну;

врегульовано на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів із стримування деструктивної діяльності в кіберпросторі;

розроблено дієві механізми залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

На засадах кіберстійкості

Держава у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить досягнення національної кіберготовності та кіберзахисту *(ціль К.1). Для цього необхідно:*

розробити Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування, з подальшим відновленням, на масштабні кібератаки та кіберінциденти щодо об'єктів

критичної інформаційної інфраструктури, у ньому визначити ролі і відповідальність усіх суб'єктів забезпечення кібербезпеки та об'єктів критичної інфраструктури під час надзвичайної ситуації, ключові процеси та заходи для подолання надзвичайної ситуації, критерії віднесення ситуації до надзвичайної, механізми інформування громадян, проведення навчань для перевірки стану готовності до надзвичайних ситуацій;

розробити базові вимоги та рекомендації з питань забезпечення кібербезпеки та кіберзахисту;

розгорнути систему обміну інформацією про кіберінциденти між усіма суб'єктами забезпечення кібербезпеки;

впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури та державних органів, зокрема розробити методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювати на законодавчому рівні обов'язковість здійснення періодичної оцінки ризиків на підставі розроблених методик;

впровадити систему сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;

забезпечити розвиток організаційно-технічної моделі кіберзахисту, впровадити механізми своєчасної ідентифікації загроз, інструменти виявлення кібератак для оперативного реагування на них та швидкого відновлення стабільної роботи під час та після кібератак;

завершити процеси визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створити і забезпечити функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійно переглядати та оновлювати вимоги до їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;

запровадити загальнонаціональну програму виявлення вразливостей інформаційно-комунікаційних систем, проводити на регулярній основі аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

запровадити постійну оцінку стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів, встановити заохочення, обов'язковість та періодичність проведення такої оцінки з урахуванням категорій критичності об'єктів, передбачити можливість участі у цих заходах фахівців з кібербезпеки приватного сектору;

впровадити систему аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначити механізми та базові методики проведення незалежних аудитів, встановити вимоги до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності

проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;

забезпечити розвиток систем технічного і криптографічного захисту інформації, пріоритетність використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

популяризувати застосування вітчизняних засобів криптографічного захисту інформації в інтересах приватних компаній;

проводити щорічні командно-штабні кібернавчання стратегічного рівня за участю представників державного та приватного секторів;

забезпечити розвиток мережі галузевих (секторальних) центрів реагування на кібератаки та кіберінциденти;

створити Національний центр резервування державних інформаційних ресурсів, провести модернізацію системи захищеного доступу державних органів до мережі Інтернет;

завершити розгортання Національної телекомунікаційної мережі, збільшити її пропускну здатність, передбачити під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації.

В Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення *(ціль К.2), для чого буде:*

забезпечено стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, 5G, штучного інтелекту, Інтернету речей, технологій хмарних і квантових обчислень, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки;

проведено аналіз та оцінено поточний стан підготовки фахівців у сфері кібербезпеки, розроблено на основі проведеного аналізу пропозиції щодо реформування системи підготовки та підвищення кваліфікації таких фахівців, схвалено відповідну концепцію;

розроблено Загальнонаціональну програму кібергігієни, спрямовану на підвищення рівня кіберграмотності населення України;

утворено центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері;

встановлено вимоги щодо необхідності підвищення кваліфікації співробітників суб'єктів сектору безпеки і оборони, об'єктів критичної інфраструктури та державних службовців з питань кібербезпеки та

кіберзахисту із запровадженням коротко- та довгострокових курсів і програм з цих питань;

забезпечено періодичне проведення навчання, у тому числі за рахунок держави, та отримання принаймні одного сертифіката (а також нового кожні три роки) з кібербезпеки для фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, а також співробітників освітніх закладів, що безпосередньо здійснюють підготовку фахівців з кібербезпеки;

створено механізми підготовки фахівців з кібербезпеки як на рівні вищої освіти, так і на рівнях середньої та професійно-технічної освіти;

забезпечено періодичне проведення з урахуванням відомчої специфіки атестації (переатестації) фахівців, що відповідають за забезпечення кібербезпеки та кіберзахисту державних органів та об'єктів критичної інфраструктури;

забезпечено матеріальне стимулювання фахівців у сфері кібербезпеки, які проходять військову, державну службу (у тому числі державну службу особливого характеру), службу в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі;

започатковано проведення щорічних національних кіберзмагань для школярів старших класів навчання та студентів як інструменту відбору найкращих молодих фахівців у сфері кібербезпеки;

забезпечено включення кібербезпекової складової до програми підготовки шкільних вчителів у вищих навчальних закладах усіх рівнів акредитації при одночасному запровадженні підвищення кваліфікації діючого педагогічного складу з питань кібербезпеки;

включено питання кібергігієни, цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до програм середньої, професійно-технічної та вищої освіти;

забезпечено координацію наукового співтовариства під час проведення наукових розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

визначено довгострокові напрями проведення досліджень та розробок у сфері кібербезпеки, а також розроблено дієву програму державної підтримки (на основі проєктного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень з питань кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

долучено основних суб’єктів національної системи кібербезпеки до програм навчання і підвищення кваліфікації персоналу, що проводяться за підтримки ЄС, зокрема Агентства ЄС з кібербезпеки (ENISA), поступово охоплюючи такими заходами інших суб’єктів забезпечення кібербезпеки.

Визнаючи безпечні цифрові послуги запорукою економічного розвитку, держава здійснюватиме такі заходи *(ціль К.3):*

зміцнюватиме довіру приватного сектору та окремих громадян до цифрових послуг, які надаються державою, безумовно виконуючи вимоги щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформуючи громадськість про їх безпечність та надійність;

впроваджуватиме цифрові послуги для населення та розвиватиме національну інформаційну інфраструктуру, передбачаючи виділення коштів на заходи кібербезпеки та кіберзахисту в розмірі не менше ніж 5% від загальної вартості відповідного об'єкта інформаційної інфраструктури (інформаційно-комунікаційної системи);

розробить нові національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів;

створюватиме органи з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг;

запровадить електронні довірчі послуги на основі кваліфікованого сертифіката автентифікації веб-сайту;

розбудовуватиме систему органів оцінки відповідності інформаційно-комунікаційних технологій, що використовуються для створення таких систем, вимогам з безпеки, управління інформаційною безпекою суб'єктами, що надають цифрові послуги;

створить необхідні передумови (нормативні, організаційні, технологічні) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) з використанням технологій електронної ідентифікації та/або електронних довірчих послуг;

підвищить ефективність системи захисту персональних даних громадян, визначивши базові вимоги до їх зберігання та обробки та посиливши відповідальність за порушення цих вимог, гармонізує вітчизняне законодавство з відповідним законодавством ЄС.

<u>На засадах взаємодії</u>

Національний координаційний центр кібербезпеки забезпечить скоординовану діяльність усіх стейкхолдерів у процесі розбудови та функціонування національної системи кібербезпеки *(ціль В.1) шляхом:*

розроблення та затвердження порядку проведення огляду стану національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії;

запровадження обов'язкового надання в режимі реального часу інформації про кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки або кіберзахисту до Національного координаційного центру кібербезпеки;

забезпечення розгляду найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, рішення якого є обов'язковими для виконання всіма суб'єктами забезпечення кібербезпеки;

розширення мережі обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз на базі технологічної платформи Національного координаційного центру кібербезпеки, охопивши всі державні органи та об'єкти критичної інфраструктури, уніфікації форматів обміну інформацією;

запровадження за досвідом країн-членів ЄС скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем під егідою Національного координаційного центру кібербезпеки;

розроблення та запровадження механізмів заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки держави;

забезпечення щорічного оприлюднення основними суб'єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності.

Держава у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі *(ціль В.2), здійснюючи такі заходи:*

врегулює на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проєктів у цій сфері;

запровадить на регулярній основі проведення консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічно сприятиме їх розвитку;

залучатиме на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення нормативно-правових актів, нормативних документів та стандартів у цій сфері;

підвищить ефективність залучення громадськості до прийняття рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їх результатів на інформаційних ресурсах Національного

координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки;

стимулюватиме розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об’єктах критичної інформаційної інфраструктури;

впровадить програму розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання;

розробить систему оцінки новітніх технологій, що безпосередньо мають вплив на кіберстійкість країни, створить інструменти (стандарти, протоколи, сертифікати тощо) з оцінки ефективності використання новітніх технологій з протидії кібератакам;

запровадить пілотні менторські програми підвищення кваліфікації фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору;

продовжить практику щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, академічних і освітніх установ, а також громадського та приватного секторів, закріпивши необхідність його проведення відповідним нормативно-правовим актом;

сприятиме, зокрема шляхом надання організаційно-технічної підтримки, функціонуванню у всіх регіонах України постійно діючих діалогових майданчиків (конференцій, семінарів, форумів тощо), діяльність яких спрямована на розбудову довіри між суб’єктами забезпечення кібербезпеки;

сприятиме впровадженню на підприємствах, в установах і організаціях незалежно від форми власності культури кібербезпеки, що полягає у постійному підвищенні кіберобізнаності їх керівників та працівників;

сприятиме взаємному визнанню результатів оцінки відповідності та сертифікації з кібербезпеки, здійснених відповідними органами як в Україні, так і за кордоном;

впровадить механізм оцінки втрат суб’єктів господарювання внаслідок кібератак для можливості їх відшкодування та як елемент подальшого впровадження системи кіберстрахування.

Україна розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України *(ціль В.3). Для цього:*

забезпечимо участь України у роботі міжнародної платформи Програми дій із заохочення відповідальної поведінки держав у кіберпросторі

Генеральної Асамблеї ООН та Групи урядових експертів ООН з питань інформаційної безпеки (UNGGE);

забезпечимо участь України у доопрацюванні Другого додаткового протоколу до Будапештської конвенції Ради Європи про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших країнах;

розширимо шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю (ЕС3), до телекомунікаційної системи Інтерполу I-24/7 (за технологією FIND);

продовжимо співробітництво з Агентством ЄС з кібербезпеки (ENISA), зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради Європи (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (NIS Директиви) як елементу євроінтеграції України;

поглибимо співпрацю з Міжнародним союзом електрозв'язку (ITU) у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах;

налагодимо співпрацю з Інтернет-корпорацією з присвоєння імен та номерів (ICANN) щодо вироблення державної політики у мережі Інтернет;

розширимо в межах Організації за демократію та економічний розвиток ГУАМ взаємодію з питань кібербезпеки;

вивчимо можливість приєднання України до стратегії ЄС з диверсифікації розпізнавання імен DNS, надання підтримки ініціативі «DNS4EU» з метою уникнення екстремальних сценаріїв реалізації кібератак на глобальну кореневу систему DNS, її ієрархічну та делеговану систему зон;

забезпечимо імплементацію Україною Положення ЄС про обмеження строку дії IPv4 для управління ринком, що прискорить впровадження в Україні IPv6, а також інших усталених стандартів безпеки в Інтернеті, передових практик розпізнавання імен DNS, маршрутизації та безпеки електронної пошти;

розвиватимемо міжнародне співробітництво у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблюючи діалог України з Європейським Союзом, Організацією Північноатлантичного договору, Організацією з безпеки і співробітництва в Європі щодо зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої співпраці;

створимо постійно діючу робочу групу з питань взаємодії із провідними ІТ-компаніями, світовими провайдерами цифрових послуг, соціальними

мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України;

визначимо та затвердимо перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

7. НАПРЯМИ ЗОВНІШНЬОПОЛІТИЧНОЇ ДІЯЛЬНОСТІ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Україна приділятиме особливу увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти, розвиватиме на договірній основі з партнерськими спецслужбами країн-членів ЄС і НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовуватиме кращі світові практики, активно здійснюватиме інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки.

Україна співпрацюватиме з міжнародними партнерами, організаціями та іншими заінтересованими сторонами, які поділяють наше спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного та безпечного, в основі якого дотримання прав людини, основних свобод та демократичних цінностей, що є запорукою соціально-економічного та політичного розвитку України.

Україна продовжить активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов’язкових норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна буде не лише учасником, але й ініціатором та організатором.

Виходячи з того, що Інтернет давно став суспільним надбанням, істотно вийшов за межі суто національних інтересів, держава максимально підтримуватиме мультистейкходерську (багатосторонню) модель управління Інтернетом, сприяючи міжнародним, регіональним та національним дискусіям з цього питання, сприяючи залученню до цього процесу приватного сектору, наукових та освітніх кіл, громадянського суспільства. Спроби окремих авторитарних держав суверенізувати Інтернет суперечать

довгостроковим інтересам України та її моделі соціально-економічного розвитку.

Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у галузі прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього держава активізує свою участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширить представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері.

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури Інтернету Україна виходить з того, що Інтернет має залишатися глобальним та відкритим, технології повинні орієнтуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас у зв’язку з ускладненням міжнародної безпеки в кіберпросторі Україна займатиме більш активну позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері кібербезпеки, зменшуючи небезпеки мілітаризації кіберпростору.

Ураховуючи взаємопов’язаність сучасного віртуального простору та з метою розвитку співпраці між державою, приватним сектором економіки, науковими і освітніми колами та громадянським суспільством у сфері кібербезпеки, Україна розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний і, насамперед, безпечний, що є запорукою успішного розвитку країни.

Протягом реалізації Стратегії Україна зробить кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна розвиватиме мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва.

8. МЕХАНІЗМИ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ТА ЗАБЕЗПЕЧЕННЯ ВІДКРИТОСТІ

Стратегія діє на період 2021 – 2025 років. Координатором реалізації Стратегії є робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Основним критерієм результативності Стратегії є досягнення мети та стратегічних цілей шляхом виконання визначених стратегічних завдань.

Національний координаційний центр кібербезпеки у визначених законодавством формах забезпечує (на весь період дії Стратегії) планування заходів з реалізації Стратегії, координує їх проведення і контролює стан виконання та ефективність.

Загальний план, розроблений Національним координаційним центром кібербезпеки та схвалений Радою національної безпеки і оборони України, є основою для формування Кабінетом Міністрів України щорічних планів заходів з реалізації Стратегії, а також для здійснення дієвого контролю за виконанням запланованих завдань і відповідних заходів.

Ефективність реалізації Стратегії визначається у проведених у встановленому порядку оглядах стану:

національної системи кібербезпеки;

кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Результати оглядів можуть стати підставою для внесення змін до загального плану та/або щорічних планів заходів з реалізації Стратегії, що обумовлено необхідністю адаптації до змін у безпековому середовищі, усунення та мінімізації негативних тенденцій у сфері кібербезпеки.

Стратегія є основою для розроблення інших нормативно-правових актів у сфері кібербезпеки України, а також для обґрунтування розподілу необхідних матеріальних, кадрових та інших ресурсів.

Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків, передбачених Державним бюджетом України для сектору безпеки і оборони, які розглядатимуться Радою національної безпеки і оборони України в порядку, визначеному Бюджетним кодексом України. Відповідно до законодавства державні органи, підприємства, установи та організації передбачатимуть у своїх планах фінансові витрати на кібербезпеку. У рамках державно-приватного партнерства, міжнародної технічної допомоги залучатимуться інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки.

Щороку Національний координаційний центр кібербезпеки оприлюднює публічний звіт про стан реалізації Стратегії за загальними оцінками.

Процес реалізації Стратегії має бути максимально прозорим, відкритим та супроводжуватися демократичним цивільним контролем. З цієї метою основними суб’єктами національної системи кібербезпеки в межах компетенції додатково буде здійснюватися щорічне інформування громадськості через власні офіційні сайти про стан реалізації ними Стратегії та стан фінансування відповідних заходів.

9. ВИМІРИ УСПІХУ (МЕТРИКИ)

Першочерговим завданням для України є розроблення та запровадження індикаторів стану кібербезпеки на основі системного моніторингу виявлення

і прогнозування кіберзагроз, що надасть змогу фіксувати досягнення або недоліки функціонування системи кібербезпеки.

Крім того, буде розроблено інтегральну систему оцінки новітніх технологій, що безпосередньо мають вплив на кіберстійкість держави, створення інструментів (стандарти, протоколи, сертифікати тощо) з оцінки ефективності використання новітніх технологій з протидії кібератакам.

Ефективність реалізації Стратегії буде визначатися через постійний моніторинг її виконання та спиратися на чітку систему індикаторів стану кібербезпеки, які буде розроблено протягом першого року реалізації Стратегії.

Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації Стратегії з таких питань, як:

виконання стратегічних завдань у межах цілей, визначених Стратегією (за кожним завданням);

досягнення стратегічних цілей, визначених Стратегією (за кожною ціллю);

ступінь впливу заходів, що здійснюються в межах Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави.

Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства і держави. Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за такими критеріями:

підвищення рівня довіри населення до держави щодо безпечності кіберпростору;

формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки крім державних інституцій залучені приватні суб'єкти та громадяни;

позитивний вплив на захист національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією Російської Федерації проти України).

За допомогою розгалуженої системи індикаторів буде визначатися стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Система індикаторів буде включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дасть можливість комплексно оцінювати результативність та ефективність реалізації Стратегії.