До відома читачів

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ:
“БЕЗПЕЧНИЙ КІБЕРПРОСТІР – ЗАПОРУКА УСПІШНОГО РОЗВИТКУ КРАЇНИ”:

Указ Президента України від 26 серпня 2021 року № 447/2021

1. Кібербезпека: глобальний контекст

Забезпечення кібербезпеки 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.

XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій.

Питома вага кіберзагроз 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 нову безпекову ситуацію. 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. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні 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. Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед Російської Федерації, міжнародних хакерських угруповань для реалізації кібервпливу.

Зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси.

Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо.

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 передбачені загрози.

Пандемія COVID-19 матиме довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних. Це вимагає забезпечення належного рівня їх захищеності та змушує державу і бізнес впроваджувати додаткові механізми і заходи щодо належного функціонування і захисту всіх необхідних для життєдіяльності інформаційних ресурсів і систем.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним. 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, передбачивши нові можливості для цифровізації всіх сфер суспільного життя.

Україна має бути 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, яка ґрунтується на довірі.

У такій ситуації актуальним є затвердження нової Стратегії кібербезпеки України, яка визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Стратегія ґрунтується на положеннях Конституції України, законів України "Про національну безпеку України" та "Про основні засади забезпечення кібербезпеки України", Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні, затвердженої Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів.

2. Стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96

Затвердження у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері.

За роки реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, 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 визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Удосконалено нормативне забезпечення з питань кіберзахисту об'єктів 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, утворюється Національний центр резервування державних інформаційних ресурсів, забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, 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 у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Федеративною Республікою Німеччина, Королівством Нідерланди, Японією тощо), поглиблюється співробітництво 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 кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки.

Отриманий досвід надав змогу виокремити низку системних проблем.

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 кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, заплановані заходи не завжди корелювалися із визначеними нею завданнями. Реалізація зазначеної 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 кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань. Участь у реалізації названої Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучалися заклади освіти та наукові установи.

Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, не були виконані, зокрема: не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично.

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

3. Національний кіберпростір: виклики та кіберзагрози

Викликами для України у сфері кібербезпеки є:

активне використання кіберзасобів у міжнародній конкуренції;

змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;

мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Загрозами кібербезпеці України є:

гібридна агресія Російської Федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності;

кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо;

організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію;

використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності.

Ураховуючи виклики та загрози, що постали перед Україною у кіберпросторі, критично зростає роль кібербезпеки в процесах цифрової трансформації держави.

Передумови та чинники, які формують окреслені загрози:

висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, відсутність системи оцінки відповідності такої продукції вимогам з безпеки, що підвищує ступінь уразливості інформаційної інфраструктури від незадекларованих функцій та звужує спроможності протидії кіберзагрозам;

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

відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом;

відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;

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, низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту;

відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом.

4. Національна система кібербезпеки: засади розбудови

Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави.

Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

посилення 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);

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

забезпечення розвитку 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, Сполученими Штатами Америки та іншими державами-членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Україна, крім основних суб'єктів національної системи кібербезпеки, залучить до вирішення завдань у цій сфері більш широке коло учасників, 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.

Україна розбудовуватиме національну систему кібербезпеки, ґрунтуючись на:

всеохоплюючому розумінні та постійному аналізі глобальних трендів кібербезпекового середовища, неухильному захисті національних інтересів України у сфері кібербезпеки;

перманентності заходів з перегляду та уточнення повноважень і відповідальності суб'єктів забезпечення кібербезпеки держави, удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо його актуалізації відповідно до безпекових умов, що змінюються;

пріоритетності економічного і соціального розвитку суспільства;

збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина;

чіткому визначенні ролей та механізмів взаємодії під час розв'язання завдань кібербезпеки, стимулюванні до обміну інформацією, знаннями і досвідом;

ризик-орієнтованому підході до забезпечення кібербезпеки;

співпраці та інклюзивному діалозі всіх суб'єктів забезпечення кібербезпеки, зміцненні довіри, зокрема в рамках державно-приватного партнерства;

впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки;

збалансованому розподілі наявних матеріальних, фінансових та інших ресурсів;

проактивному підході до нейтралізації кіберзагроз;

забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

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 цієї Стратегії.

Для формування потенціалу стримування (С) необхідним є досягнення таких стратегічних цілей:

ціль С.1. Дієва кібероборона – Україна створить та забезпечить розвиток (у тому числі кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформує належну правову, організаційну, технологічну модель їх функціонування та застосування, забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності;

ціль С.2. Ефективна протидія 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. Ефективна протидія кіберзлочинності – Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів;

ціль С.4. Розвиток асиметричних інструментів стримування – Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору.

Для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей:

ціль К.1. Національна кіберготовність та надійний кіберзахист – Україна запровадить і реалізує чіткі та зрозумілі для всіх заінтересованих сторін заходи щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Україна посилить кіберготовність, що полягатиме у здатності всіх заінтересованих сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури. Україна створить національну систему управління інцидентами;

ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки – Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок 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. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним стануть невід'ємними елементами освіти кожного громадянина України;

ціль К.3. Безпечні цифрові послуги – Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність та безпеку цифрових послуг протягом усього їхнього життєвого циклу.

Для вдосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей:

ціль В.1. Зміцнення системи координації – Україна 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, скоординує діяльність усіх заінтересованих сторін задля подолання надзвичайних (кризових) ситуацій у кіберпросторі.

ціль В.2. Формування нової моделі відносин у сфері кібербезпеки – Україна запровадить 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 – Україна спрямує 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. Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Забезпечення координації з міжнародними партнерами здійснюватиметься Міністерством закордонних справ України.

6. Стратегічні завдання

Розбудова національної системи кібербезпеки на засадах стримування, кіберстійкості та взаємодії має здійснюватися шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Для досягнення цілі С.1 Україна сформує систему дієвої кібероборони шляхом:

утворення у системі Міністерства оборони України кібервійськ та забезпечення їх 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;

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;

забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

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

Для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом:

створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури;

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

посилення спроможностей у проведенні негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об'єкти;

посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, 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.

Для досягнення цілі С.3 Україна посилить спроможності у протидії кіберзлочинності шляхом:

завершення імплементації в законодавство України положень Конвенції про кіберзлочинність;

врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав-членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки;

розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних вебсайтах;

розроблення методики проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечення проведення таких досліджень;

розроблення методики комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створення необхідних умов для її практичної реалізації;

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

врегулювання на законодавчому рівні правового статусу криптовалют;

проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози;

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

забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

залучення 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.

Для досягнення цілі С.4 Україна запровадить асиметричні інструменти стримування шляхом:

удосконалення системи розвідувального забезпечення кібербезпеки в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці у кіберпросторі;

посилення заходів щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном;

створення технологічних можливостей підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів;

запровадження гармонізованого з євроатлантичною спільнотою підходу до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, розроблення та узгодження з іноземними партнерами механізму спільних дипломатичних та економічних дій і заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність;

застосуванням усіх доступних інструментів дипломатії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України;

налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами-членами ЄС та державами-членами НАТО, створення платформи такого обміну;

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

розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

Для досягнення цілі К.1 Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом:

розроблення Національного плану реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення;

створення національної системи управління інцидентами, розроблення та впровадження стандартних операційних процедур для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності;

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

запровадження планування видатків на кібербезпеку за окремими бюджетними програмами;

розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик;

налагодження на основі взаємної довіри системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікації форматів обміну інформацією;

впровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичної оцінки ризиків на підставі розроблених методик;

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

забезпечення розвитку організаційно-технічної моделі кіберзахисту;

завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійного перегляду та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;

запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

впровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначення механізмів та базових методик проведення аудитів, встановлення вимог 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;

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

впровадження вітчизняних рішень із захисту інформації;

проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів;

забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти;

завершення розгортання Національної телекомунікаційної мережі, збільшення її пропускної здатності, передбачення під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації;

забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до мережі Інтернет;

створення національного сервісу доменних імен (DNS).

Для досягнення цілі К.2 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 шляхом:

забезпечення координації наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

визначення довгострокових напрямів проведення досліджень і розробок у сфері кібербезпеки, а також розроблення дієвої програми державної підтримки (на основі проектного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони;

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

удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки;

розроблення Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти;

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

забезпечення матеріального стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі 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;

залучення суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу.

Для досягнення цілі К.3 Україна спрямує зусилля на забезпечення надійності та безпеки цифрових послуг шляхом:

зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформування громадськості про їх безпечність та надійність;

впровадження цифрових послуг для населення та розвитку національної інформаційної інфраструктури;

розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів;

створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг;

створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг;

підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог.

Для досягнення цілі В.1 Національний координаційний центр кібербезпеки забезпечить скоординовану діяльність усіх заінтересованих сторін у процесі розбудови та функціонування національної системи кібербезпеки шляхом:

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

запровадження обов'язкового негайного, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки;

забезпечення розгляду найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, системного контролю за станом виконання його рішень;

запровадження скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем;

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

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

Для досягнення цілі В.2 Україна у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі, шляхом:

врегулювання 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 проектів у цій сфері;

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

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

підвищення ефективності 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;

стимулювання 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;

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

продовження практики щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору;

запровадження системи страхування від кіберризиків, зокрема механізму оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування;

розроблення фінансових та нефінансових механізмів для сприяння впровадженню сучасних технологій кібербезпеки у державному і приватному секторі, включаючи страхування, лізинг, пільги тощо.

Для досягнення цілі В.3 Україна розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України, шляхом:

забезпечення участі України у міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі;

забезпечення участі України у доопрацюванні Другого додаткового протоколу до Конвенції 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 державах;

розширення шляхом діалогу з міжнародними партнерами доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7;

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

поглиблення співпраці з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах;

поглиблення співпраці з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства;

розвитку міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України;

продовження практики проведення двосторонніх кібердіалогів з державами-партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між заінтересованими державними органами України та іноземних держав, розширення кола держав-партнерів, з якими проводяться кібердіалоги, ініціювання питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки;

створення постійно діючої робочої групи 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;

визначення та затвердження переліку пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

7. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки

Україна у сфері кібербезпеки забезпечить 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 держав-членів ЄС і держав-членів 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 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, а й ініціатором та організатором.

Україна максимально підтримуватиме мультистейкхолдерську (багатосторонню) модель управління Інтернетом, сприяючи міжнародним, регіональним та національним дискусіям з цього питання, залученню до цього процесу представників приватного сектору, наукових та освітніх кіл, інститутів 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 сфері прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього Україна 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, її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження 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 небезпеку мілітаризації кіберпростору.

Україна розвиватиме мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва.

8. Механізми реалізації стратегії та забезпечення відкритості

Координатором реалізації цієї Стратегії є робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Реалізація Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

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 реалізації Стратегії, координує і контролює стан її виконання та ефективність.

План реалізації Стратегії, розроблений Національним координаційним центром кібербезпеки та затверджений в установленому порядку, є основою для щорічного планування суб'єктами забезпечення кібербезпеки заходів з реалізації Стратегії.

Кабінет Міністрів України в установленому порядку забезпечує необхідними силами, засобами і ресурсами виконання заходів з реалізації Стратегії.

Результати виконання запланованих заходів з реалізації Стратегії подаються суб'єктами забезпечення кібербезпеки до Національного координаційного центру кібербезпеки.

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

національної системи кібербезпеки;

кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Результати оглядів можуть стати підставою для внесення змін до Плану реалізації Стратегії 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 обґрунтування розподілу необхідних для забезпечення кібербезпеки матеріальних, кадрових та інших ресурсів.

Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків, передбачених Державним бюджетом України та з інших джерел, не заборонених законодавством. У порядку координації Національний координаційний центр кібербезпеки під час підготовки матеріалів до засідань Ради національної безпеки і оборони України щодо проекту Закону України про Державний бюджет України та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням національної безпеки і оборони України, аналізує пропозиції суб'єктів забезпечення кібербезпеки України щодо фінансування заходів з кібербезпеки, передбачених положеннями Стратегії кібербезпеки України, та надає відповідні пропозиції.

Згідно із законодавством 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 вебсайти про стан реалізації ними Стратегії та стан фінансування відповідних заходів.

9. Виміри успіху (метрики)

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);

рівень 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:

рівень 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;

рівень захищеності 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 змогу комплексно оцінювати результативність та ефективність реалізації Стратегії.

Україна розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний та безпечний задля захисту суверенітету держави, соціального і економічного розвитку суспільства.

За результатами реалізації Стратегії Україна у співпраці з приватним сектором та із залученням міжнародних партнерів забезпечить:

стійкість до кіберзагроз, підвищивши здатність державних органів, бізнесу і громадян захищати себе та реагувати на кіберзагрози;

спроможність до ефективної протидії недружнім діям у кіберпросторі, забезпечивши їх швидке виявлення та розслідування, створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі;

розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам.

Керівник Офісу Президента України А.ЄРМАК

URL: //www.president.gov.ua/documents/4472021-40013

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~