# ІНДИКАТОРИ ВИКОНАННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

1. Розробити систему індикаторів стану кібербезпеки, що включатиме: 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Служба безпеки України, Національна академія наук України, Національний інститут стратегічних досліджень |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Розроблено та представлено НКЦК систему індикаторів стану кібербезпеки.*** |

# Ціль С.1. Дієва кібероборона

2. Створити у системі Міністерства оборони України кібервійська, забезпечивши їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство оборони України |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Внесено зміни до законів України «Про Збройні Сили України», «Про оборону України», «Про національну безпеку України», «Про чисельність Збройних Сил України» та до Кримінального кодексу України щодо визначення завдань Кібервійськ Збройних Сил України, збільшення чисельності Збройних Сил України, надання права застосовувати кіберзброю в мирний час та в особливий період, уточнення (доповнення) термінології, встановлення засад військово-цивільного партнерства із фахівцями та суб’єктами господарювання під час організації та проведення кібероперацій.***  ***Кібервійська Збройних Сил України забезпечено ресурсами за відповідними показниками: персонал, озброєння та військова техніка, запаси, навченість.***  ***Кібервійська як окремий рід військ Збройних Сил України набули спроможностей до виконання завдань за призначенням.*** |

3. Запровадити ефективні механізми взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони.

|  |  |
| --- | --- |
|  | Міністерство оборони України, Генеральний штаб Збройних Сил України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Міністерством оборони України внесено на розгляд Кабінету Міністрів України проект акта Уряду про затвердження механізму (порядку) взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі).*** |

4. Розробити та забезпечити виконання плану кібероборони як складової частини плану оборони України.

|  |  |
| --- | --- |
|  | Генеральний штаб Збройних Сил України, Міністерство оборони України, інші основні суб'єкти національної  системи кібербезпеки |
|  | *Розробка – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***План кібероборони України як складова частина Плану оборони України розроблено та затверджено.***  ***Забезпечено скоординоване виконання заходів Плану кібероборони України.***  ***Забезпечено щорічне (за необхідності) уточнення Плану кібероборони України з метою оновлення політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі.*** |

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

|  |  |
| --- | --- |
|  | Міністерство оборони України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | **Проведено щонайменше двічі на рік тематичні навчання, учасниками кожного з яких були представники держав-членів НАТО.** |

6. Створити MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею.

|  |  |
| --- | --- |
|  | Міністерство оборони України, Генеральний штаб Збройних Сил України |
|  | *Перше півріччя 2024 року* |
| ***Індикатор виконання*** | **У Міністерстві оборони України створено MIL.CERT-UA.**  **Укладено угоди (меморандуми) щодо співпраці з європейською військовою CERT-мережею.** |

7. Забезпечити оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки та оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

|  |  |
| --- | --- |
|  | Міністерство оборони України, Генеральний штаб Збройних Сил України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Щороку, починаючи з 2023 року  (за попередній рік), та під час проведення відповідних оглядів* |
| ***Індикатор виконання*** | ***Кожний із проведених оглядів (оборонних оглядів; оглядів національної системи кібербезпеки; оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом) містить окремий розділ, в якому надано оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони.*** |

8. Запровадити у системі військово-патріотичного виховання та системі територіальної оборони навчальні програми підготовки та проводити практичні навчання у сфері кібербезпеки.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство оборони України, Генеральний штаб Збройних Сил України, місцеві органи виконавчої влади спільно з органами місцевого самоврядування |
|  | *Запровадження – перше півріччя  2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***До кінця першого півріччя 2022 року в навчальних програмах систем військово-патріотичного виховання та територіальної оборони закріплено вимоги до знань слухачів в частині питань кібербезпеки.***  ***В подальшому щорічно не менше 25 відсотків учасників цих систем мають бути охоплені такими курсами і здобути практичні навички у сфері кібербезпеки.*** |

# Ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму

9. Створити відповідно до схвалених концептуальних засад загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури.

|  |  |
| --- | --- |
|  | Служба безпеки України, Кабінет Міністрів України |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Розроблено, погоджено із зацікавленими сторонами та впроваджено загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури.*** |

10. Удосконалити аналітичне і криміналістичне забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів.

|  |  |
| --- | --- |
|  | Служба безпеки України |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Розроблено, погоджено із зацікавленими сторонами та затверджено методики обробки та оцінки цифрових даних, формування електронних доказів.*** |

11. Посилити спроможності у проведенні негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об'єкти.

|  |  |
| --- | --- |
|  | Служба безпеки України |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Удосконалено нормативно-правову базу щодо проведення негласних перевірок, забезпечено необхідний технічний, апаратно-програмний інструментарій, кадрові спроможності для їх проведення, до кінця 2025 року реалізовано такі перевірки щодо інформаційно-комунікаційних систем всіх об'єктів критичної інфраструктури, ключових державних електронних інформаційних ресурсів, єдиних державних реєстрів та баз даних.*** |

12. Посилити контррозвідувальний захист сфери електронних комунікацій, IT-сфери, афілійованого з ними середовища, спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України у сфері кібербезпеки.

|  |  |
| --- | --- |
|  | Служба безпеки України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Забезпечено попередження та своєчасне реагування на потенційні загрози національній безпеці, пов’язані із розвідувально-підривною діяльністю спецслужб іноземних держав, спрямованих на сферу електронних комунікацій та IT-сферу.*** |

13. Створити технологічні можливості 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.

|  |  |
| --- | --- |
|  | Служба безпеки України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Міністерство внутрішніх справ України, Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Розроблено та затверджено необхідну нормативно-правову базу, інтегровано апаратно-програмні засоби для автоматичного виявлення кібератак у режимі реального часу та їх блокування в загальнодержавні інформаційно-комунікаційні системи та на окремі об'єкти критичної інфраструктури, забезпечено автоматизований інформаційний обмін щодо отриманих даних між відповідальними державними органами, формалізовано механізм блокування кібератак.*** |

14. Вдосконалити нормативно-правове, організаційне та кадрове забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму.

|  |  |
| --- | --- |
|  | Служба безпеки України, Кабінет Міністрів України |
|  | *Перше півріччя 2024 року* |
| ***Індикатор виконання*** | ***Протидія та реагування на кібератаки, що створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою здійснюється в рамках правового режиму боротьби з тероризмом.*** |

# Ціль С.3. Ефективна протидія кіберзлочинності

15. Завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Всі положення Конвенції про кіберзлочинність імплементовано в українське законодавство, створено достатню правову базу для безперешкодної взаємодії із країнами-підписантами Конвенції для ефективної протидії кіберзлочинності в рамках цього міжнародного документу.*** |

16. Забезпечити унормування в установленому порядку 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Вітчизняне законодавство забезпечує можливість ефективно використовувати електронні докази у цивільному, адміністративному та кримінальному судочинстві у відповідності до кращих практик Сполучених Штатів Америки, держав – членів ЄС.*** |

17. Розробити концептуальні підходи щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей).

|  |  |
| --- | --- |
|  | Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Національна поліція України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Чинна державна політика спрямована та сприяє забезпеченню конституційних прав та свобод людини і громадянина під час використання кіберпростору. Розроблено та впроваджено ефективні механізми захисту персональних даних громадян, забезпечення права на повагу до гідності людини і громадянина, свободи слова, недопущення булінгу та використання кіберпростору для сексуальної експлуатації дітей, доведення до самогубства, а також здійснення інших злочинів проти волі, честі та гідності особи, інших прав і свобод людини і громадянина.*** |

18. Запровадити практику 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.

|  |  |
| --- | --- |
|  | Міністерство внутрішніх справ України, Національна поліція України, Міністерство цифрової трансформації України, Міністерство соціальної політики України, Міністерство освіти і науки України, Міністерство культури та інформаційної політики України, Служба безпеки України, Національний банк України |
|  | *Запровадження – друге півріччя  2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***Створено нормативні і організаційно-технічні умови для проведення загальнонаціональних інформаційних роз'яснювальних кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами.***  ***Інформація щодо алгоритму таких дій є загальнодоступною та розміщена на сторінках офіційних Інтернет представництв основних суб’єктів національної системи кібербезпеки.***  ***Забезпечено функціонування цілодобової гарячої лінії, на яку кожен громадянин може звернутися і отримати роз’яснення щодо дій у випадку, якщо він став жертвою кіберзлочину.*** |

19. 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.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Розробка – друге півріччя 2023 року Реалізація – щороку* |
| ***Індикатор виконання*** | ***Адміністрацією Держспецзв’язку розроблено та затверджено Методику збору кіберстатистики. Основними суб'єктами національної системи кібербезпеки збирається кіберстатистика у відповідності до розробленої Адміністрацією Держспецзв’язку методики. Раз на рік на їх офіційних сайтах публікується інформація щодо кіберінцидентів, кібератак та заходів протидії.*** |

20. 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний інститут стратегічних досліджень |
|  | *Розробка – друге півріччя 2024 року Реалізація – щороку* |
| ***Індикатор виконання*** | ***Методика проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, розроблена Держспецзв'язку та затверджена Урядом. Кабінетом Міністрів України організовано щорічне проведення таких досліджень, починаючи з 2024 року.*** |

21. Розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити необхідні умови для її практичної реалізації.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Служба безпеки України, Національний інститут стратегічних досліджень |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Розроблено та затверджено протокольним рішенням НКЦК методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам.***  ***Зазначена методика використовується на практиці для комунікування між державою і суспільством.*** |

22. Запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний банк України |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Чинні організаційно-правові механізми забезпечують ідентифікацію суб'єктів електронної комерції у кіберпросторі.*** |

23. Забезпечити в установленому порядку врегулювання правового статусу криптовалют.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний банк України |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Розроблено та внесено на розгляд Верховної Ради України законопроект щодо врегулювання правового статусу криптовалют у вітчизняному законодавстві, а також підготовлено відповідні зміни до інших законів та підзаконних нормативно-правових актів.*** |

24. Проводити спільні з ЄС та НАТО заходи, спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Представники України беруть участь не менш ніж у 90% міжнародних заходів ЄС та НАТО у сфері кібербезпеки, на які запрошено українську сторону.***  ***Україна виступає ініціатором та організатором не менш ніж 7 міжнародних заходів у сфері кібербезпеки щорічно, що проводяться спільно з ЄС та НАТО.*** |

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

|  |  |
| --- | --- |
|  | Міністерство юстиції України, Міністерство внутрішніх справ України, Служба безпеки України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Організовано не менш ніж 5 програм підвищення кваліфікації (тренінгів, семінарів тощо) щорічно із охопленням не менш ніж 80% судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів.***  ***Проведено оцінку потреб щодо необхідного апаратно-програмного та іншого забезпечення в інтересах проведення судових експертиз за вказаними напрямами та здійснено його подальшу закупівлю або організоване отримання в рамках міжнародної допомоги.*** |

26. Забезпечити 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.

|  |  |
| --- | --- |
|  | Міністерство внутрішніх справ України, Національна поліція України, Служба безпеки України, Державна судова адміністрація України, Офіс Генерального прокурора |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Організовано не менш ніж 7 програм підвищення кваліфікації (тренінгів, семінарів тощо) щорічно із охопленням не менш ніж 60% співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів, які працюють у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів.*** |

27. Залучати 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.

|  |  |
| --- | --- |
|  | Міністерство юстиції України, Міністерство внутрішніх справ України, Національна поліція України, Служба безпеки України, Державна судова адміністрація України, Офіс Генерального прокурора |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Нормативно-правова база забезпечує можливість повноцінного залучення приватних експертів.***  ***У щонайменше 50% випадках проведення розслідувань комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів та у випадках відсутності необхідної кваліфікації та/або технічних можливостей у відповідних державних, у т.ч. правоохоронних органів, було залучено приватних експертів.*** |

# Ціль С.4. Розвиток асиметричних інструментів стримування

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

|  |  |
| --- | --- |
|  | Служба зовнішньої розвідки України, інші розвідувальні органи України |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Посилено кадрові та технічні спроможності структурних підрозділів розвідувальних органів, що відповідають за напрям кіберрозвідки та протидії кіберзагрозам національній безпеці.*** |

29. Посилити заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Служба зовнішньої розвідки України, Служба безпеки України, Міністерство оборони України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Перше півріччя 2024 року* |
| ***Індикатор виконання*** | ***Впроваджено централізовану систему управління кіберінцидентами в структурі МЗС, орієнтовану на забезпечення кіберзахисту інфраструктури та інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном, створено протоколи її спільного використання (МЗС, СБУ, СЗРУ та Держспецзв'язку за загальною координацією НКЦК).*** |

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

|  |  |
| --- | --- |
|  | Служба безпеки України, розвідувальні органи України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації |
|  | *Перше півріччя 2024 року* |
| ***Індикатор виконання*** | ***Налагоджено взаємодію з постачальниками електронних комунікаційних мереж та послуг, забезпечено інтероперабільність наявного у розвідувальних та контррозвідувальних органів технічного обладнання з обладнанням та відповідними протоколами обміну інформацією систем зазначених суб'єктів для підключення технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів.*** |

31. Запровадити гармонізований з євроатлантичною спільнотою підхід 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.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Міністерство економіки України, Служба безпеки України, розвідувальні органи України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Країнами ЄС та США в рамках підтримки України та гармонізованого підходу до санаційної політики запроваджено санкції у відповідь на деструктивну кіберактивність проти України щодо суб'єктів, до яких запроваджено санкції Україною.***  ***Аналогічні санкції введено Україною щодо суб'єктів, на які накладено санкції Країнами ЄС та США за деструктивну кіберактивність проти цих країн.*** |

32. Застосовувати усі доступні інструменти дипломатії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Забезпечено застосування санкцій євроатлантичною спільнотою на рф, юридичних та фізичних осіб рф за зловмисну діяльність у кіберпросторі проти України, застосовано механізм міжнародного судочинства для притягнення рф до відповідальності за кіберзлочини проти України, ініційовано виключення рф з усіх груп та підгруп з кібербезпеки ключових міжнародних організацій (ООН, ОБСЄ, ISO тощо).*** |

33. Налагодити систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами – членами ЄС та державами – членами НАТО, створити платформи такого обміну.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Створення платформ – перше півріччя 2023 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***Забезпечити автоматизований обмін інформацією в режимі наближеному до реального часу між НКЦК і СERT-UA з боку України та компетентними органами країн ЄС і НАТО щодо кібератак, виявлених вразливостей систем кіберзахисту національного значення, планів та намірів зловмисників щодо реалізації кібероперацій.*** |

34. Забезпечити розроблення законопроекту, спрямованого на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Законопроект, спрямований на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі, розроблено та внесено на розгляд Верховної Ради України.*** |

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

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України, розвідувальні органи України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Декриміналізовано несанкціоноване втручання в роботу інформаційно-комунікаційних систем з боку фахівців приватного сектору, що здійснюється для стримування та протидії агресії проти України в кіберпросторі у відповідності до вимог закону.***  ***Створено кіберрезерв та відпрацьовано механізм його мобілізації.***  ***Створено спільноту українських IT-спеціалістів, для нейтралізації ворога в кіберпросторі.*** |

# Ціль К.1. Національна кіберготовність та надійний кіберзахист

36. Розробити Національний план 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний  центр кібербезпеки, основні  суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Розроблено та затверджено Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі.*** |

37. Створити національну систему управління інцидентами,   
розробити та впровадити стандартні операційні процедури для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний  центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Створено національну систему управління інцидентами (прийняті відповідні нормативно-правові документи, протестовано функціональність системи).***  ***Розроблено та впроваджено стандартні операційні процедури для реагування на різні види подій у кіберпросторі.*** |

38. Забезпечити постійний моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Створено нормативні, організаційні та технологічні умови для проведення 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.***  ***Забезпечено на постійній основі обмін інформацією про виявлені в режимі реального часу аномалії функціонування національних електронних комунікаційних мереж та інформаційних ресурсів.*** |

39. Передбачати у проекті закону про Державний бюджет України на відповідний рік видатки на кібербезпеку за окремими бюджетними програмами.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України, Служба зовнішньої розвідки України |
|  | *Щороку* |
| ***Індикатор виконання*** | ***У щорічному Законі України «Про Державний бюджет України» передбачено видатки на кібербезпеку за окремими бюджетними програмами.*** |

40. Розробити базові (визначатимуть мінімальний обов'язковий рівень) вимоги та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Розроблені, обговорені із заінтересованими сторонами та затверджені базові вимоги та рекомендації з питань забезпечення кібербезпеки.*** |

41. Налагодити на основі взаємної довіри системний обмін інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікувати формати обміну інформацією.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Уніфіковано формати обміну інформацією (відповідні формати нормативно закріплені).***  ***Станом на перше півріччя 2023 року щонайменше раз на тиждень відбувається обмін інформацією, учасниками якого є не лише основні суб’єкти національної системи кібербезпеки.*** |

42. Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розробити методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Розроблено та затверджено методику ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави.***  ***Нормативно врегулювано питання щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик.*** |

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

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Внесено зміни до переліку сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання.***  ***Створено та акредитовано в Національному агентстві з акредитації України орган з сертифікації продукції, процесів та послуг, орган оцінки відповідності у сфері електронних довірчих послуг та орган з оцінки відповідності у сфері криптографічного захисту інформації. Забезпечено функціонування зазначених органів та випробувальної лабораторії.***  ***Розширено сфери акредитації органу з сертифікації продукції у сфері кіберзахисту.*** |

44. Забезпечити розвиток організаційно-технічної моделі кіберзахисту.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Затвердження моделі – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***До завершення 2022 року розроблено перелік нормативно-правових актів, необхідних для розвитку організаційно-технічної моделі кіберзахисту.***  ***У першому півріччі 2023 року визначено необхідні заходи, етапи їх реалізації та відповідальні суб’єкти, які забезпечують розвиток елементів організаційно-технічної моделі кіберзахисту у різних інфраструктурах та їх рівнях.***  ***У 2024 – 2025 роках забезпечено впровадження складових частин організаційно-технічної моделі кіберзахисту.*** |

45. 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національний банк України, інші суб'єкти національної системи захисту критичної інфраструктури |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Затверджено Перелік об'єктів критичної інфраструктури.***  ***Затверджено Перелік об'єктів критичної інформаційної інфраструктури.***  ***Через два місяці після затвердження Преліку ОКІ прийнято, розроблено в рамках міжнародної технічної допомоги спеціалізоване програмне та апаратне забезпечення Реєстру ОКІІ.***  ***Створено макет Реєстру ОКІІ, затверджено технічне завдання на КСЗІ інфрамаційно-комунікаційної системи (ІКС) «Реєстр ОКІІ»***  ***І півріччя 2023 року***  ***Проведено тестову експлуатацію та усунено недоліки макету ІКС «Реєстр ОКІ».***  ***Розроблено експлуатаційну документацію, проведено навчання персоналу адміністраторів Реєстру ОКІІ, створено та підтверджено відповідність КСЗІ ІКС «Реєстру ОКІІ».***  ***ІІ півріччя 2023 року***  ***ІКС «Реєстр ОКІ» уведено в експлуатацію наказом розпорядника Національного реєстру ОКІ.***  ***І півріччя 2024 року***  ***Впроваджено подання поточних профілів кіберзахисту ОКІІ до Реєстру ОКІІ, створено поточний профіль кіберзахисту ІКС «Реєстр ОКІІ».***  ***ІІ півріччя 2022 року***  ***Розроблено зміни до Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518, в яких запроваджено вимоги щодо оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.***  ***Переглянуто та за необхідності оновлено вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.*** |

46. Запровадити на постійній основі оцінку стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановити обов'язковість та періодичність проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювати участь у цих заходах фахівців з кібербезпеки приватного сектору.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України |
|  | *Розробка змін до законодавства – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***Нормативно визначено* обов’язковість та періодичність проведення оцінки ста*ну захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, а також порядок залучення до таких заходів фахівців з кібербезпеки приватного сектору.*** |

47. Впровадити систему аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначити механізми та базові методики проведення 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Прийнято постанову Кабінету Міністрів України “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури”.***  ***Затверджено наказами Адміністрації Держспецзв'язку Методичні рекомендації щодо проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури; Вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та Порядок атестації (переатестації) аудиторів інформаційної безпеки на об’єктах критичної інфраструктури.*** |

48. 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.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України. |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Розроблено та прийнято нормативний документ, що створює передумови пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва.***  ***Щорічно кількість засобів ТЗІ/КЗІ вітчизняного виробництва з підтвердженою відповідністю збільшується.***  ***Щорічно зростає експорт вітчизняних засобів ТЗІ/КЗІ.*** |

49. Впровадити вітчизняні рішення із захисту інформації.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***В органах державної влади та на об’єктах критичної інформаційної інфраструктури за умови існування декількох рішень із захисту інформації з однаковим характеристиками пріоритетність віддана вітчизняним.*** |

50. Проводити командно-штабні кібернавчання стратегічного рівня,   
а також тематичні кібернавчання та тренінги за участю представників державного та приватного секторів.

|  |  |
| --- | --- |
|  | Національний координаційний  центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щонайменше раз на рік проводяться командно-штабні кібернавчання стратегічного рівня.***  ***Щонайменше раз на 2 роки проводяться тематичні кібернавчання та тренінги за участю представників державного та приватного секторів.*** |

51. Забезпечити розвиток мережі центрів реагування на кібератаки та кіберінциденти.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Щорічно вводиться в роботу щонайменше один новий центр (секторальний або відомчий) реагування на кібератаки та кіберінциденти.*** |

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

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Завершено розгортання Національної телекомунікаційної мережі.***  ***Збільшено пропускну здатність транспортної платформи Національної телекомунікаційної мережі шляхом нарощування її оптичного сегмента за рахунок:***  ***збудовано п’ять вузлів Національної телекомунікаційної мережі для чотирьох центральних органів виконавчої влади та Головного управління урядового фельд’егерського зв’язку Держспецзв’язку;***  ***спроектовано та збудовано ВОЛЗ транспортної платформи Національної телекомунікаційної мережі до адміністративних будівель територіальних органів державної влади, складових сектору безпеки і оборони в обласних центрах України (за окремим планом).*** |

53. Забезпечити функціонування та розвиток Національного центру резервування державних інформаційних ресурсів, провести модернізацію системи захищеного доступу державних органів до мережі Інтернет.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Постійно Модернізація системи захищеного доступу державних органів до мережі Інтернет – друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***Забезпечено функціонування та розвиток Національного центру резервування державних інформаційних ресурсів.***  ***Розроблено технічне завдання та проведено модернізацію системи захищеного доступу державних органів до мережі Інтернет.*** |

54. Створити національний сервіс доменних імен (DNS).

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний  центр кібербезпеки |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Створено та введено в експлуатацію національний сервіс доменних імен (DNS).*** |

# Ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки

55. Забезпечити координацію наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Міністерство освіти і науки України, Національна академія наук України, Національний інститут стратегічних досліджень |
|  | *Створення механізму координації – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***До кінця другого півріччя 2022 року створено (розроблено загальне бачення та реалізовано на практиці) координаційний механізм.***  ***Координаційні заходи відбуваються не рідше 4 разів на рік.***  ***Річні результати координаційних заходів подаються до НКЦК.*** |

56. Визначити довгострокові напрями проведення досліджень   
і розробок у сфері кібербезпеки, а також розробити дієву програму 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Міністерство освіти і науки України, Національна академія наук України, Національний інститут стратегічних досліджень |
|  | *Визначення довгострокових напрямів – друге півріччя 2022 року Розроблення програми – перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***До кінця другого півріччя 2022 року визначено та передано до НКЦК перелік (з короткою анотацією) довгострокових напрямів*** ***проведення досліджень і розробок у сфері кібербезпеки.***  ***До кінця першого півріччя 2023 року розроблено Концепцію державної цільової програми підтримки стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони.*** |

57. Забезпечити 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Національна академія наук України |
|  | *Розроблення механізму стимулювання – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***До кінця другого півріччя 2022 року розроблено (створено концептуальне бачення, затверджено необхідні нормативно-правові документи та проведено пілотне застосування) механізму стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій.***  ***Щорічно механізм забезпечує стимулювання мінімум одного нового дослідження чи розробки в наступних категоріях: технології хмарних та квантових обчислень, 5G-мережі, Інтернет речей, штучний інтелект, нові засоби реалізації кіберзагроз, створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки.***  ***Щорічно до НКЦК подається довідкова інформація про результативність застосування механізму.*** |

58. Удосконалити систему підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство освіти і науки України, Національне агентство України з питань державної служби, основні суб'єкти національної системи кібербезпеки |
|  | *Розроблення концепції системи – друге півріччя 2022 року Реалізація концепції – друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***До кінця другого півріччя 2022 року розроблено та публічно презентовано Концепцію системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки.***  ***До кінця другого півріччя 2025 року Концепція офіційно прийнята, має затверджений план реалізації та впроваджується щонайменше в пілотному режимі.*** |

59. Розробити Загальнонаціональну програму кіберграмотності, спрямовану 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство освіти і науки України, Міністерство цифрової трансформації України, основні суб'єкти національної системи кібербезпеки |
|  | *Розробка програми – перше півріччя 2023 року Реалізація програми – постійно* |
| ***Індикатор виконання*** | ***До кінця першого півріччя 2023 року розроблено деталізовану Загальнонаціональну програму кіберграмотності.***  ***Щорічно програма охоплює щонайменше на 10% цільових аудиторій більше, ніж у попередньому році.*** |

60. Утворити центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національна академія наук України, основні суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Створено щонайменше 3 центри (відомчі, секторальні, наукові або інші), які на постійній основі здійснюють узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері (або хоча б одне з цих завдань).*** |

61. Забезпечити матеріальне 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, основні суб'єкти національної системи кібербезпеки |
|  | *Перше півріччя 2022 року* |
| ***Індикатор виконання*** | ***Розроблено та прийнято акт(и) Кабінету Міністрів України, що забезпечать матеріальне 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.*** |

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

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно ініціюється (направлено запит, проведено консультації) приєднання України до щонайменше однієї нової міжнародної програми навчання і підвищення кваліфікації персоналу.***  ***Щорічно щонайменше 5 представників основних суб’єктів національної системи кібербезпеки та ОКІ проходять навчання/підвищення кваліфікації за міжнародними програмами.*** |

# Ціль К.3. Безпечні цифрові послуги

63. Зміцнювати довіру приватного сектору та 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.

|  |  |
| --- | --- |
|  | Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші центральні та місцеві органи виконавчої влади, Національний банк України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічне проведення роз’яснювальних інформаційних кампаній, що охоплюють до 20% представників цільових аудиторій.*** |

64. Забезпечити впровадження цифрових послуг для населення та розвиток національної інформаційної інфраструктури.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство цифрової трансформації України, Національний банк України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно впроваджується щонайменше 5 нових цифрових послуг.***  ***95% закладів соціальної інфраструктури та органів місцевого самоврядування підключені до широкосмугового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с.*** |

65. Розробити 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.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України,  Міністерство економіки України, основні суб'єкти національної системи кібербезпеки |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Розроблено та прийнято національні стандарти, гармонізовані із європейськими/міжнародними стандартами у сфері кібербезпеки в частині безпеки інтернету речей, застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень.*** |

66. Створити органи з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації України, Національний банк України |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Створено (прийнята необхідна нормативно-правова база, забезпечено організаційні, технічні, кадрові та фінансові спроможності) щонайменше два органи з оцінки відповідності надавачів електронних довірчих послуг.*** |

67. Створити необхідні передумови (нормативні, організаційні, технологічні) 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.

|  |  |
| --- | --- |
|  | Міністерство цифрової трансформації України |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Створено та впроваджено*** ***інтегровану систему електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг.*** |

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

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Уповноважений Верховної Ради України з прав людини (за згодою) |
|  | *Друге півріччя 2023 року* |
| ***Індикатор виконання*** | ***До національного законодавства імплементовано положення GDPR.*** |

# Ціль В.1. Зміцнення системи координації

69. Розробити та затвердити порядок проведення огляду національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки |
|  | *Затвердження порядку – друге півріччя 2022 року Проведення огляду – щороку, починаючи з 2023 року* |
| ***Індикатор виконання*** | ***Протокольним рішенням НКЦК затверджено порядок проведення огляду національної системи кібербезпеки. Кабінетом Міністрів України спільно з НКЦК організовано щорічне проведення такого огляду відповідно до затвердженого порядку.*** |

70. Запровадити обов'язкове негайне, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Встановлення вимог та відповідальності щодо інформування – друге півріччя 2022 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***Усі відомчі та галузеві (секторальні) центри кібербезпеки (кіберзахисту) повідомили НКЦК про 100% кібератак, які були виявлені ними протягом всього періоду виконання Стратегії відповідно до наступних параметрів:***  ***відомчі та галузеві (секторальні) центри кібербезпеки (кіберзахисту) невідкладно, не пізніше 30 хвилин з моменту виявлення, інформують Національний координаційний центр кібербезпеки про виявлену кібератаку або кіберінцидент, що потенційно може мати критичні наслідки для кібербезпеки держави із зазначенням об’єкта кібератаки (кіберінциденту), часу її здійснення та іншої наявної інформації. Протягом 12 годин після виявлення такої кібератаки/кіберінцидента у встановленому порядку НКЦК надається технічна інформація (індикатори компрометації, тип атаки, особливості механізму реалізації тощо), а також інформація щодо можливого джерела, потенційних наслідків, додаткових обставин, вжитих та запланованих заходів реагування.*** |

71. Забезпечити розгляд найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, системний контроль за станом виконання його рішень.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Засідання Національного координаційного центру кібербезпеки, а також його робочих груп проводяться на системній основі, але не рідше одного разу на квартал. На засіданнях розглядаються найважливіші питання у сфері кібербезпеки України та приймаються стратегічні рішення. Контроль за їх виконанням забезпечено Апаратом РНБО України.*** |

72. Запровадити скоординоване виявлення та розкриття вразливостей інформаційно-комунікаційних систем.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Впровадження системи управління вразливостями – друге півріччя  2023 року Реалізація – постійно* |
| ***Індикатор виконання*** | ***Створено нормативно-правову базу та організаційні механізми щодо скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем, впроваджено систему управління вразливостями. Виявлення та розкриття вразливостей інформаційно-комунікаційних систем здійснюється на системній основі відповідальними суб’єктами забезпечення кібербезпеки із залученням приватного сектору.*** |

73. Розробити та запровадити механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, основні суб'єкти національної системи кібербезпеки, Національний інститут стратегічних досліджень |
|  | *Перше півріччя 2024 року* |
| ***Індикатор виконання*** | ***Розроблено та впроваджено організаційно-правові механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки.*** |

74. Забезпечити щорічне оприлюднення основними суб'єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Щороку, починаючи з 2022 року  (за попередній рік)* |
| ***Індикатор виконання*** | ***Публічні звіти про стан кібербезпеки за сферами відповідальності щорічно оприлюднюються на офіційних веб-сайтах основних суб'єктів національної системи кібербезпеки****.* |

# Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки

75. Забезпечити розроблення законопроекту, спрямованого на врегулювання питань 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Розроблено та внесено на розгляд Верховної Ради України законопроект.*** |

76. Запровадити 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, всебічно сприяти їх розвитку.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Створено механізм проведення консультацій, який застосовується на постійній основі.*** |

77. Залучати 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно до розробки проектів НПА, нормативних документів та стандартів у цій сфері залучається мінімум один новий (такий, що не залучався до того протягом реалізації Стратегії)*** ***представник наукових установ/ громадських організацій/незалежний експерт.*** |

78. Підвищити 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.

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно на сайті НКЦК розміщується щонайменше одна нова анкета (опитування) з актуальних питань кібербезпеки.*** |

79. Стимулювати 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Запроваджено (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) механізм стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом.***  ***Щорічно надається підтримка щонайменше трьом вітчизняним програмним продуктам, що використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури.*** |

80. Впровадити програму розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України |
|  | *Друге півріччя 2024 року* |
| ***Індикатор виконання*** | ***Розроблено та впроваджено (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) програму розвитку ринку товарів і послуг у сфері кібербезпеки.*** |

81. Продовжити практику 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки |
|  | *Щороку у жовтні* |
| ***Індикатор виконання*** | ***Щорічно проводяться заходи, присвячені місяцю кібербезпеки в Україні.***  ***Щорічно за результатами проведення місяця кібербезпеки готується інформаційна довідка, яка відображає: коло залучених профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору.*** |

82. Запровадити систему страхування від кіберризиків, зокрема механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України |
|  | *Друге півріччя 2025 року* |
| ***Індикатор виконання*** | ***Розроблено та прийнято НПА, що дозволяє реалізувати в Україні систему страхування від кіберризиків, зокрема механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування.***  ***Запроваджено щонайменше один пілотний проект.*** |

83. Розробити фінансові та нефінансові механізми для сприяння впровадженню сучасних технологій кібербезпеки у державному і приватному секторі, включаючи страхування, лізинг, пільги тощо.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний  центр кібербезпеки |
|  | *Перше півріччя 2025 року* |
| ***Індикатор виконання*** | ***Розроблені та запроваджені (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) фінансові та нефінансові механізми.***  ***Хоча б один з механізмів функціонує в пілотному режимі.*** |

# Ціль В.3. Прагматичне міжнародне співробітництво

84. Забезпечити участь України у міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно забезпечується участь представників України у 100% заходів ООН щодо заохочення відповідальної поведінки держав у кіберпросторі.***  ***Щорічно надається перелік заходів із зазначеного питання, які відбувались під егідою ООН та хто і в якому статусі приймав в них участь від України.*** |

85. Забезпечити участь 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.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Представник(и) України постійно приймають участь у заходах із доопрацювання Другого додаткового протоколу до Конвенції про кіберзлочинність.***  ***Щорічно надається інформація про кількість заходів, а також хто і в якому статусі приймав в них участь від України.*** |

86. Розширити шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу І-24/7.

|  |  |
| --- | --- |
|  | Національна поліція України, Служба безпеки України, Міністерство закордонних справ України |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Правоохоронні органи України, з числа основних суб’єктів національної системи кібербезпеки, мають постійний доступ до ресурсів Європейського центру боротьби з кіберзлочинністю та до телекомунікаційної системи Інтерполу І‑24/7.*** |

87. Продовжити співробітництво 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Служба безпеки України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно проводяться щонайменше одні консультації між представниками України та Агентства Європейського Союзу з питань мережевої та інформаційної безпеки.*** |

88. Поглибити співпрацю з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах.

|  |  |
| --- | --- |
|  | Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації |
|  | *Друге півріччя 2022 року* |
| ***Індикатор виконання*** | ***Забезпечено участь у заходах Міжнародного союзу електрозв’язку у сферах кібербезпеки та електронних комунікацій щодо питань стандартизації і удосконалення національної системи електронних комунікацій.*** |

89. Розвивати практичне співробітництво з НАТО щодо питань кібероборони, налагодити тісну взаємодію з цих питань із відповідними структурами Альянсу, зокрема Радою управління з кібероборони (NATO Cyber Defence Management Board), Центром операцій у кіберпросторі (Cyberspace Operations Centre), Центром можливостей з реагування на комп'ютерні інциденти (NATO Computer Incident Response Capability), Об'єднаним центром передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence).

|  |  |
| --- | --- |
|  | Національний координаційний центр кібербезпеки, Міністерство оборони України, Генеральний штаб Збройних Сил України, основні суб'єкти національної системи кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Україна має офіційне представництво у всіх вказаних структурах (або підписані угоди (меморандуми) про співробітництво).***  ***З кожною організацією визначено коло питань для практичної співпраці.***  ***З кожною організацією є щонайменше один спільний реалізований проект станом на кінець 2025 року.*** |

90. Поглибити співпрацю з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства.

|  |  |
| --- | --- |
|  | Міністерство цифрової трансформації України, Національна поліція України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Спільно з міжнародними партнерами щорічно проводиться не менше 5 заходів, спрямованих на захист дітей від сексуального онлайн-насильства.***  ***Щорічно реалізується щонайменше один пілотний проект.*** |

91. Забезпечити розвиток міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України, Національний координаційний центр кібербезпеки |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно Україна підтримує щонайменше одну міжнародну ініціативу.*** |

92. Продовжити практику 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, розширити коло держав – партнерів, з якими проводяться кібердіалоги, ініціювати питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки.

|  |  |
| --- | --- |
|  | Міністерство закордонних справ України |
|  | *Постійно* |
| ***Індикатор виконання*** | ***Щорічно проводяться кібердіалоги з наявними партнерами, а також щорічно додається щонайменше одна країна для таких діалогів.*** |

93. Створити 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.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки |
|  | *Перше півріччя 2023 року* |
| ***Індикатор виконання*** | ***Створено постійно діючу робочу групу, проведено щонайменше одне засідання робочої групи.*** |

94. Визначити та затвердити перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

|  |  |
| --- | --- |
|  | Кабінет Міністрів України, Національний координаційний центр кібербезпеки |
|  | *Друге півріччя 2022 року*. |
| ***Індикатор виконання*** | ***Підготовлено та затверджено список пріоритетних напрямів, проведено щонайменше одні консультації щодо їх підтримки за рахунок міжнародної технічної допомоги.*** |