ЗАТВЕРДЖЕНО
розпорядженням Кабінету Міністрів України
від 7 березня 2025 р. № 204-р

# ПЛАН
заходів на 2025 рік з реалізації Стратегії кібербезпеки України

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 1. Створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору | 1) розроблення правової, організаційної, технологічної моделей функціонування кібервійськ та їх застосування | розроблено відповідні моделі функціонування кібервійськ | II квартал 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |
| | 2) формування необхідної організаційної структури кібервійськ із урахуванням досвіду провідних держав — членів НАТО | сформовано відповідну організаційну структуру кібервійськ | III квартал 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |
| | 3) забезпечення кібервійськ належними фінансовими, кадровими і технічними ресурсами | забезпечено кібервійська належними ресурсами | IV квартал 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |
| 2. Запровадження ефективних механізмів взаємодії основних суб’єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони | розроблення та внесення на розгляд Кабінету Міністрів України проекту нормативно-правового акта про затвердження порядку (механізму) взаємодії основних суб’єктів | внесено на розгляд Кабінету Міністрів України відповідний проект акта | IV квартал 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Адміністрація Держспецзв’язку<br>СБУ (за згодою)<br>Національна поліція |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (щодо політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі) | | | Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби |
| 3. Розроблення та забезпечення виконання плану кібероборони як складової частини плану оборони України | уточнення в разі потреби плану кібероборони з метою оновлення політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі | уточнено план кібероборони | протягом 2025 року | Генеральний штаб Збройних Сил (за згодою)<br>Міноборони<br>Адміністрація Держспецзв'язку<br>СБУ (за згодою)<br>Національна поліція<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 4. Забезпечення проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав — членів НАТО для досягнення оперативної сумісності | 1) проведення переговорів і консультацій із партнерами з метою підвищення рівня професійної компетентності кіберфахівців основних суб'єктів національної системи кібербезпеки за стандартами освіти НАТО | проведено відповідні переговори та консультації | протягом 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Адміністрація Держспецзв'язку<br>СБУ (за згодою)<br>Національна поліція<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| | 2) забезпечення участі представників основних суб'єктів забезпечення кібербезпеки у спільних тематичних навчаннях із відповідними підрозділами держав — членів НАТО для досягнення оперативної сумісності | взято участь представниками України у відповідних заходах (у разі запрошення) | протягом 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Адміністрація Держспецзв'язку<br>СБУ (за згодою)<br>Національна поліція<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 5. Посилення спроможностей щодо проведення негласних перевірок стану готовності об’єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, поступове охоплення такими заходами всіх об’єктів | здійснення запланованих заходів із проведення негласних перевірок стану готовності об’єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, зокрема шляхом здійснення пошуку та виявлення потенційних вразливостей інформаційно-комунікаційних систем об’єктів критичної інфраструктури | проведено заплановані негласні перевірки стану готовності об’єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, зокрема шляхом здійснення пошуку та виявлення потенційних вразливостей інформаційно-комунікаційних систем об’єктів критичної інфраструктури | IV квартал 2025 року | СБУ (за згодою) |
| 6. Посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, що спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку у сфері кібербезпеки | посилення технічних спроможностей для здійснення запланованих заходів із контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, що спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку у сфері кібербезпеки | посилено технічні спроможності для здійснення запланованих заходів із контррозвідувального захисту у відповідній сфері | IV квартал 2025 року | СБУ (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 7. Завершення імплементації в законодавство України положень Конвенції про кіберзлочинність | імплементація в законодавство України положення Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних | імплементовано в законодавство України положення Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних | IV квартал 2025 року | Національна поліція<br>МВС<br>Мін'юст<br>СБУ (за згодою) |
| 8. Запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у разі, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур щодо звернення до правоохоронних органів | забезпечення розміщення на офіційних веб-сайтах державних органів інформації про алгоритм дій громадян у разі, коли вони стикаються із кібершахрайством та іншими кіберзлочинами | розміщено на офіційних веб-сайтах державних органів відповідну інформацію про алгоритм дій громадян у разі, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, яка постійно оновлюється та актуалізується | протягом 2025 року | МВС<br>Національна поліція<br>Мінсоцполітики<br>МОН<br>МКСК<br>СБУ (за згодою)<br>Національний банк (за згодою) |
| 9. Здійснення спільних із державами — членами ЄС і НАТО заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність і реагувати на кіберзагрози | 1) проведення навчальних семінарів, практичних занять, робочих груп з питань боротьби із кіберзлочинністю та реагування на кіберзагрози в рамках проекту Ради Європи "CyberUA" і спільного проекту | здійснено відповідні міжнародні спільні заходи із державами — членами ЄС і НАТО | протягом 2025 року | МЗС<br>Апарат Ради національної безпеки і оборони України (за згодою)<br>Адміністрація Держспецзв'язку<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | Європейського Союзу та Ради Європи “CyberEast+” | | | СБУ (за згодою)<br>Національна поліція<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| | 2) взяття участі в міжнародних заходах держав — членів ЄС і НАТО, на які запрошено Українську Сторону, що спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність і реагувати на кіберзагрози | взято представниками України участь у відповідних міжнародних заходах | протягом 2025 року | Апарат Ради національної безпеки і оборони України (за згодою)<br>Адміністрація Держспецзв’язку<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>СБУ (за згодою)<br>Національна поліція<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 10. Удосконалення системи розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці в кіберпросторі | нарощення технічних спроможностей шляхом модернізації та закупівлі необхідного обладнання, інструментів упередження загроз і нарощення кадрового потенціалу шляхом підвищення кваліфікації персоналу | посилено технічні та кадрові спроможності в частині упередження загроз національній безпеці | протягом 2025 року | Служба зовнішньої розвідки (за згодою) |
| 11. Посилення заходів щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об’єктів державної власності України за кордоном | посилення захисту 15 закордонних дипломатичних установ України та об’єктів державної власності України за кордоном шляхом запровадження системного рішення щодо доступу до Інтернету та службового листування із використанням централізованого захищеного вузла доступу | запроваджено системне рішення щодо доступу 15 закордонних дипломатичних установ України та об’єктів державної власності України за кордоном до Інтернету та службове листування із використанням централізованого захищеного вузла доступу (на рівні МЗС) | IV квартал 2025 року | МЗС<br>Служба зовнішньої розвідки (за згодою)<br>СБУ (за згодою)<br>Міноборони<br>Адміністрація Держспецзв’язку |
| 12. Застосовування всіх доступних інструментів дипломатії та міжнародного права для протидії зловмисній | вжиття уповноваженими представниками закордонних дипломатичних установ України заходів до запровадження державами — | вжито відповідних заходів, а також ініційовано виключення Російської Федерації з усіх груп і підгруп із кібербезпеки | протягом 2025 року | МЗС |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| діяльності проти України в кіберпросторі | членами ЄС і НАТО обмежувальних заходів у вигляді спеціальних економічних та інших обмежувальних заходів (санкцій) проти Російської Федерації, юридичних і фізичних осіб Російської Федерації у зв'язку із провадженням зловмисної діяльності проти України в кіберпросторі, застосування механізмів міжнародного судочинства для притягнення Російської Федерації до відповідальності за кіберзлочини проти України, а також продовження роботи щодо виключення Російської Федерації з усіх груп і підгруп із кібербезпеки ключових міжнародних організацій | ключових міжнародних організацій | | |
| 13. Налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі із міжнародними партнерами, | забезпечення обміну інформацією про деструктивну діяльність у кіберпросторі із державами — членами НАТО | забезпечено регулярний обмін інформацією | протягом 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>СБУ (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| насамперед державами — членами НАТО, створення платформи для такого обміну | | | | |
| 14. Розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі | створення кіберрезерву та відпрацювання механізму його мобілізації | створено кіберрезерв і відпрацьовано механізм його мобілізації | IV квартал 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Адміністрація Держспецзв’язку<br>СБУ (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби |
| 15. Забезпечення проведення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень до цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування | продовження здійснення заходів із проведення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень до цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування | здійснено відповідні заходи | протягом 2025 року | Апарат Ради національної безпеки і оборони України (за згодою)<br>Адміністрація Держспецзв’язку<br>МВС<br>Національна поліція<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>СБУ (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Національний банк (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | | | | інші центральні органи виконавчої влади |
| 16. Впровадження ризик-орієнтованого підходу в частині заходів із 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, забезпечення нормативного врегулювання питань щодо впровадження обов’язкового проведення періодичної оцінки кіберризиків на підставі розроблених методик | 1) розроблення та затвердження методики ідентифікації та оцінки кіберризиків на національному рівні | розроблено та затверджено відповідну методику | IV квартал 2025 року | Адміністрація Держспецзв’язку<br>Апарат Ради національної безпеки і оборони України (за згодою)<br>Національна поліція<br>СБУ (за згодою)<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| | 2) нормативне врегулювання питань щодо впровадження обов’язковості проведення періодичної оцінки кіберризиків | внесено на розгляд Кабінету Міністрів України відповідні проекти актів | IV квартал 2025 року | Адміністрація Держспецзв’язку<br>Апарат Ради національної безпеки і оборони України (за згодою)<br>Національна поліція<br>СБУ (за згодою)<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | | | | Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| 17. Забезпечення розвитку систем криптографічного та технічного захисту інформації, пріоритетності використання засобів криптографічного та технічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури | 1) проведення державної експертизи у сфері криптографічного та технічного захисту інформації | проведено всі заплановані експертизи у сфері криптографічного та технічного захисту інформації | протягом 2025 року | Адміністрація Держспецзв’язку |
| | 2) ліцензування господарської діяльності у галузі криптографічного та технічного захисту інформації | видано ліцензії на провадження господарської діяльності у галузі криптографічного та технічного захисту інформації | протягом 2025 року | Адміністрація Держспецзв’язку |
| 18. Проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань і тренінгів за участю представників державного та приватного сектору | 1) проведення командно-штабних кібернавчань стратегічного рівня | проведено щонайменше одне командно-штабне кібернавчання | протягом 2025 року | Апарат Ради національної безпеки і оборони України (за згодою)<br>Адміністрація Держспецзв’язку<br>СБУ (за згодою)<br>Національна поліція<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | | | | Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| | 2) проведення тематичних кібертренінгів за участю представників державного та приватного сектору | проведено не менше п’яти тематичних кібертренінгів | протягом 2025 року | Апарат Ради національної безпеки і оборони України (за згодою)<br>Адміністрація Держспецзв’язку<br>СБУ (за згодою)<br>Національна поліція<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| 19. Забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти | 1) посилення технічних спроможностей системи центрів забезпечення кібербезпеки СБУ з метою її сталого функціонування на | посилено технічні спроможності регіональних центрів забезпечення кібербезпеки СБУ | IV квартал 2025 року | СБУ (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | національному та регіональному рівні | | | |
| | 2) забезпечення створення галузевого (секторального) центру реагування на інциденти з кібербезпеки в системі МВС | створено галузевий (секторальний) центр реагування на інциденти з кібербезпеки в системі МВС | IV квартал 2025 року | МВС<br>Національна поліція |
| | 3) забезпечення створення регіонального центру реагування на інциденти з кібербезпеки | створено регіональний центр реагування на інциденти з кібербезпеки | IV квартал 2025 року | Адміністрація Держспецзв’язку |
| 20. Забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до Інтернету | 1) закупівля обладнання (разом із ліцензіями) для модернізації підсистем захисту системи захищеного доступу державних органів до Інтернету від DDoS-атак | придбано та встановлено обладнання в повному обсязі | IV квартал 2025 року | Адміністрація Держспецзв’язку |
| | 2) закупівля обладнання для модернізації та розвитку інформаційної системи “Програмна платформа для розгортання та супроводження державних електронних реєстрів” | посилено спроможності інформаційної системи “Програмна платформа для розгортання та супроводження державних електронних реєстрів” | IV квартал 2025 року | Адміністрація Держспецзв’язку |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 21. Удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки та захисту інформації | 1) розроблення стандартів вищої освіти у сфері кібербезпеки та захисту інформації | розроблено та затверджено стандарти вищої освіти освітніх ступенів бакалавра та магістра у сфері кібербезпеки та захисту інформації | IV квартал 2025 року | МОН<br>Адміністрація Держспецзв'язку<br>СБУ (за згодою)<br>Національна поліція<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |
| | 2) удосконалення системи підготовки та підвищення кваліфікації військових фахівців у сфері кібербезпеки | внесено відповідні зміни до переліку та змісту курсів підготовки фахівців із кіберзахисту Збройних Сил | IV квартал 2025 року | Генеральний штаб Збройних Сил (за згодою)<br>Міноборони |
| | 3) забезпечення розроблення програм, тренінгів із підвищення рівня знань, умінь і навичок за професійними стандартами: "Адміністратор безпеки мереж і систем", "Аудитор інформаційних технологій (з кібербезпеки)", | затверджено відповідні програми | IV квартал 2025 року | Адміністрація Держспецзв'язку |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| | “Фахівець з оцінки заходів захисту інформації (кібербезпеки)”, “Фахівець з реагування на інциденти кібербезпеки”, “Фахівець сфери захисту інформації” | | | |
| | 4) забезпечення підвищення кваліфікації державних службовців і посадових осіб місцевого самоврядування з питань кібербезпеки | проведено навчання не менше ніж 1 000 осіб державних службовців і посадових осіб місцевого самоврядування з питань кібербезпеки | IV квартал 2025 року | НАДС<br>інші органи виконавчої влади |
| 22. Створення центрів, що здійснюватимуть узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій і вітчизняних розробок у зазначеній сфері | забезпечення виконання завдань з аналізу та обміну інформацією про кіберзагрози регіональним центром реагування на інциденти з кібербезпеки | проведено аналіз і обмін інформацією про кіберзагрози регіональним центром реагування на інциденти з кібербезпеки | IV квартал 2025 року | Адміністрація Держспецзв’язку<br>Апарат Ради національної безпеки і оборони України (за згодою)<br>СБУ (за згодою)<br>Національна поліція<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Служба зовнішньої розвідки (за згодою)<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 23. Залучення суб’єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу | забезпечення участі представників Міноборони та Збройних Сил у навчаннях і підвищенні кваліфікації за міжнародними програмами | залучено до навчання та заходів із підвищення кваліфікації не менше 20 представників Міноборони та Збройних Сил | протягом 2025 року | Міноборони<br>Генеральний штаб Збройних Сил (за згодою) |
| 24. Розроблення національних стандартів у сфері кібербезпеки, організаційних і технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, із урахуванням європейських і міжнародних стандартів | розроблення пропозицій до проектів національних стандартів у сфері кіберзахисту, гармонізованих із європейськими, міжнародними стандартами у сфері кібербезпеки | подано відповідні пропозиції державному підприємству “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” | IV квартал 2025 року | Адміністрація Держспецзв’язку |
| 25. Розроблення та затвердження порядку проведення огляду національної системи кібербезпеки із забезпеченням його проведення не менше ніж раз на рік протягом строку реалізації Стратегії кібербезпеки України | розроблення пропозицій до порядку проведення огляду національної системи кібербезпеки | подано відповідні пропозиції Національному координаційному центру кібербезпеки | IV квартал 2025 року | Адміністрація Держспецзв’язку<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>МВС<br>Національна поліція<br>Апарат Ради національної безпеки і оборони України (за згодою) |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 26. 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 і приватного сектору | 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 і приватного сектору | проведено місяць кібербезпеки в Україні | III квартал 2025 року | Адміністрація Держспецзв’язку<br>Апарат Ради національної безпеки і оборони України (за згодою)<br>СБУ (за згодою)<br>Міноборони<br>Генеральний штаб Збройних Сил (за згодою)<br>Національна поліція<br>Адміністрація Держприкордонслужби<br>Національний банк (за згодою)<br>МВС<br>Служба зовнішньої розвідки (за згодою) |
| 27. Забезпечення участі України в міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі | складання постійним представництвом України при ООН календарного плану заходів ООН щодо заохочення відповідальної поведінки держав у кіберпросторі, а також забезпечення участі представників України в заходах | забезпечено участь представників України в усіх відповідних міжнародних заходах ООН | протягом 2025 року | МЗС |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| 28. Розвиток практичного співробітництва із НАТО щодо питань кібероборони, налагодження тісної взаємодії з цих питань із відповідними органами 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) | забезпечення практичного співробітництва із НАТО з питань кібероборони | взято участь представниками Міноборони та Збройних Сил у заходах НАТО з питань кібероборони | протягом 2025 року | Міноборони Генеральний штаб Збройних Сил (за згодою) |
| 29. Продовження практики проведення двосторонніх кібердіалогів із державами-партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку | проведення двосторонніх кібердіалогів із державами-партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між | проведено мінімум один кібердіалог | протягом 2025 року | МЗС |

| Найменування завдання | Найменування заходу | Індикатор виконання | Строк виконання | Відповідальні за виконання |
|---|---|---|---|---|
| комунікації між заінтересованими державними органами України та іноземних держав, розширення кола держав-партнерів, із якими проводяться кібердіалоги, ініціювання питання про укладення двосторонніх договорів про співпрацю у сфері кібербезпеки | заінтересованими державними органами України та іноземних держав, розширення кола держав-партнерів, із якими проводяться кібердіалоги, ініціювання питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки | | | |