|  |
| --- |
| http://zakonst.rada.gov.ua/images/gerb.gif |
| **КАБІНЕТ МІНІСТРІВ УКРАЇНИ**  **РОЗПОРЯДЖЕННЯ** |
| **від 11 липня 2018 р. № 481-р** **Київ** |

**Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України**

1. Затвердити [план заходів на 2018 рік з реалізації Стратегії кібербезпеки України](http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80/print#n13), що додається.

2. Міністерствам, іншим центральним органам виконавчої влади за участю Служби безпеки, Служби зовнішньої розвідки, Національного банку забезпечити:

1) виконання затвердженого цим розпорядженням плану заходів у межах бюджетних призначень, передбачених на поточний рік;

2) формування бюджетних запитів на наступні роки з урахуванням фінансування заходів відповідно до пріоритетів та напрямів, передбачених [Стратегією кібербезпеки України](http://zakon.rada.gov.ua/laws/show/96/2016#n11);

3) подання Адміністрації Державної служби спеціального зв’язку та захисту інформації:

до 10 липня та 15 грудня даних про хід виконання плану заходів, затвердженого цим розпорядженням, для їх узагальнення та інформування зазначеною Адміністрацією Апарату Ради національної безпеки і оборони України та Кабінету Міністрів України;

до 1 вересня пропозицій до плану заходів на 2019 рік з реалізації [Стратегії кібербезпеки України](http://zakon.rada.gov.ua/laws/show/96/2016#n11).

|  |  |
| --- | --- |
| **Прем'єр-міністр України** | **В.ГРОЙСМАН** |
| **Інд. 21** |  |

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖЕНО** **розпорядженням Кабінету Міністрів України** **від 11 липня 2018 р. № 481-р** |

**ПЛАН ЗАХОДІВ**  
**на 2018 рік з реалізації**[**Стратегії кібербезпеки України**](http://zakon.rada.gov.ua/laws/show/96/2016#n11)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Найменування заходу | Відповідальні за виконання | Строк виконання |
| 1. | Підготовка пропозицій стосовно врегулювання на законодавчому рівні питання щодо: |  |  |
|  | розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, вчинені щодо державних та інших інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури та інших об’єктів, а також відповідного розмежування підслідності | Національна поліція  МВС  СБУ (за згодою)  Адміністрація Держспецзв’язку | II квартал |
|  | підвищення рівня відповідальності посадових осіб державних органів, установ та організацій за порушення вимог щодо інформування в установленому порядку про несанкціоновані дії (кібератаки) стосовно державних інформаційних ресурсів | Адміністрація Держспецзв’язку  МВС  Національна поліція  СБУ (за згодою)  Міноборони  Генеральний штаб Збройних Сил (за згодою) | -“- |
|  | визначення Держспецзв’язку органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів | Адміністрація Держспецзв’язку | -“- |
|  | встановлення обов’язкового погодження з Держспецзв’язку завдань (проектів) Національної програми інформатизації, а також проектів (завдань) створення і розвитку інформаційно-телекомунікаційних систем державних органів, підприємств, установ та організацій державної форми власності | Державне агентство з питань електронного урядування  Адміністрація Держспецзв’язку | -“- |
| 2. | Врегулювання питання щодо: |  |  |
|  | заборони державним органам, підприємствам, установам та організаціям державної форми власності, крім закордонних дипломатичних установ України, закуповувати послуги (укладати договори) з доступу до Інтернету в операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації | Адміністрація Держспецзв’язку  Мінекономрозвитку  ДРС  інші суб’єкти забезпечення кібербезпеки | III квартал |
|  | впровадження обов’язкових вимог стосовно здійснення державними органами, підприємствами, установами та організаціями державної форми власності ідентифікації та автентифікації джерел отриманих оновлень до програмного забезпечення, яке використовується для обробки державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та встановлення цілісності таких оновлень | Адміністрація Держспецзв’язку  інші заінтересовані органи виконавчої влади | -“- |
|  | застосування посадовими (службовими) особами державних органів, підприємств, установ та організацій державної форми власності електронного цифрового підпису під час використання електронної пошти для виконання посадових (службових) обов’язків | Адміністрація Держспецзв’язку  Державне агентство з питань електронного урядування  інші заінтересовані органи виконавчої влади | -“- |
|  | визначення порядку передачі, збереження і доступу до резервних копій інформації та відомостей державних електронних інформаційних ресурсів для потреб державних органів, насамперед суб’єктів сектору безпеки і оборони, фінансового, енергетичного, транспортного секторів | Адміністрація Держспецзв’язку  інші заінтересовані органи виконавчої влади | II квартал |
|  | формування переліку об’єктів критичної інформаційної інфраструктури | Адміністрація Держспецзв’язку  СБУ (за згодою)  Генеральний штаб Збройних Сил (за згодою)  Міноборони  інші заінтересовані органи виконавчої влади | липень |
|  | визначення порядку формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури | Адміністрація Держспецзв’язку | -“- |
|  | визначення вимог до проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури | -“- | -“- |
| 3. | Удосконалення взаємодії між суб’єктами забезпечення кібербезпеки шляхом: |  |  |
|  | створення єдиної інтерактивної бази даних про кіберінциденти для потреб Міноборони, Держспецзв’язку, СБУ, Національної поліції, Національного банку, розвідувальних органів | Адміністрація Держспецзв’язку  МВС  Національна поліція  Адміністрація Держприкордонслужби СБУ (за згодою)  Служба зовнішньої розвідки (за згодою)  Національний банк (за згодою)  Генеральний штаб  Збройних Сил (за згодою)  Міноборони  інші заінтересовані органи виконавчої влади | протягом року |
|  | організації обміну інформацією про кібератаки на об’єкти критичної інфраструктури (насамперед енергетики, транспорту, банків) | Адміністрація Держспецзв’язку Міненерговугілля  Мінінфраструктури  МВС  Національна поліція  Національний банк (за згодою)  СБУ (за згодою)  Генеральний штаб Збройних Сил (за згодою)  Міноборони  інші заінтересовані органи виконавчої влади | протягом року |
| 4. | Узгодження проектів (завдань) Національної програми інформатизації, виконання яких передбачено у 2018 році, з Адміністрацією Держспецзв’язку та Державним агентством з питань електронного урядування | Адміністрація Держспецзв’язку  Державне агентство з питань електронного урядування  інші заінтересовані органи виконавчої влади | -“- |
| 5. | Удосконалення нормативно-правової бази шляхом: |  |  |
|  | подальшого впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки | Адміністрація Держспецзв’язку  СБУ (за згодою)  МЗС  Мін’юст  Міноборони  Генеральний штаб Збройних Сил (за згодою)  Національна академія наук (за згодою) | -“- |
|  | імплементації Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради ЄС від 6 липня 2016 р. щодо заходів з підвищення загального рівня безпеки мереж та інформаційних систем в ЄС | Адміністрація Держспецзв’язку  інші заінтересовані органи виконавчої влади  Національна академія наук (за згодою) | II квартал |
| 6. | Розроблення механізму залучення фізичних і юридичних осіб до виконання завдань кіберзахисту державних електронних інформаційних ресурсів у рамках державно-приватного партнерства на умовах аутсорсингу | Адміністрація Держспецзв’язку  інші заінтересовані органи виконавчої влади | -“- |
| 7. | Розвиток Національної телекомунікаційної мережі, врегулювання питань порядку надання послуг та їх тарифікації | Адміністрація Держспецзв’язку | протягом року |
| 8. | Проведення модернізації ситуаційних центрів з кібербезпеки Держспецзв’язку та СБУ шляхом залучення допомоги НАТО в рамках реалізації Трастового фонду Україна - НАТО з кібербезпеки | Адміністрація Держспецзв’язку  СБУ (за згодою)  Мінфін | III квартал |
| 9. | Забезпечення розвитку організаційно-технічної моделі кіберзахисту, зокрема утворення центру реагування на кіберзагрози, а також розвиток системи захищеного доступу державних органів до Інтернету | Адміністрація Держспецзв’язку | протягом року |
| 10. | Опрацювання питання щодо утворення тренінгового кіберцентру в інтересах суб’єктів забезпечення кібербезпеки | Адміністрація Держспецзв’язку  інші суб’єкти забезпечення кібербезпеки | -“- |
| 11. | Вдосконалення механізму взаємодії з Національною академією наук та її профільними установами з метою проведення наукових досліджень та спільних науково-практичних робіт у галузях кібербезпеки та кіберзахисту критичної інфраструктури | Адміністрація Держспецзв’язку  Національна академія наук (за згодою) | -“- |
| 12. | Забезпечення діяльності Центру кіберзахисту Національного банку, удосконалення кіберзахисту і кібербезпеки банківської системи України та у сфері переказу коштів | Національний банк (за згодою)  Адміністрація Держспецзв’язку  СБУ (за згодою) | протягом року |
| 13. | Розроблення методики формування та визначення основних показників ефективності реалізації [Стратегії кібербезпеки України](http://zakon.rada.gov.ua/laws/show/96/2016#n11) з урахуванням досвіду європейських і світових практик | Адміністрація Держспецзв’язку  інші заінтересовані органи виконавчої влади та суб’єкти забезпечення кібербезпеки  Національний інститут стратегічних досліджень (за згодою) | -“- |
| 14. | Участь у заходах щодо зміцнення міжнародного співробітництва шляхом утворення спільних двосторонніх або багатосторонніх груп для здійснення розслідувань кіберзлочинів, а також проведення спільних операцій, обміну інформацією та досвідом | Національна поліція  МВС  Міноборони  Генеральний штаб Збройних Сил (за згодою)  СБУ (за згодою)  Адміністрація Держспецзв’язку  МЗС | -“- |
| 15. | Організація та проведення конференцій, семінарів, форумів, засідань круглих столів, тренінгів, навчань з питань кібербезпеки та кіберзахисту на державному і міжнародному рівнях | Адміністрація Держспецзв’язку  СБУ (за згодою)  Міноборони  Генеральний штаб  Збройних Сил (за згодою)  МЗС  МВС  Національна поліція  інші заінтересовані органи виконавчої влади  Національний банк (за згодою)  Національна академія наук (за згодою) | -“- |
| 16. | Розвиток системи підготовки кадрів у сфері кібербезпеки, зокрема: |  |  |
| підготовка фахівців тактичного та оперативно-тактичного рівня за напрямом “кібербезпека” | Міноборони  Генеральний штаб Збройних Сил (за згодою) | протягом року |
| підготовка, атестація, переатестація та підвищення кваліфікації фахівців у сфері кіберзахисту для потреб державних органів, військових формувань і правоохоронних органів | Адміністрація Держспецзв’язку | -“- |
| 17. | Проектування захищеного дата-центру (центру обробки даних) для потреб державних органів, насамперед суб’єктів сектору безпеки і оборони, фінансового, енергетичного, транспортного секторів | Адміністрація Держспецзв’язку | грудень |
| 18. | Здійснення заходів щодо утворення Національного центру оперативно-технічного управління телекомунікаційними мережами України | Адміністрація Держспецзв’язку  НКРЗІ (за згодою)  Генеральний штаб Збройних Сил (за згодою) | протягом року |