Прим. № 1

# ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

05.06.2019 № 05/02-526

Державна регуляторна служба України
вул. Арсенальна, 9/11, м. Київ, 01011

Щодо погодження проекту
постанови КМУ

Направляємо на погодження проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» підготовлено Адміністрацією Державної служби спеціальної зв'язку та захисту інформації України на виконання вимог підпункту "г" підпункту 3 пункту 2 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32, та пункту 2 Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р.

Просимо погодити зазначений проект згідно з положеннями статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Додатки: 1. Проект постанови Кабінету Міністрів України на 11 арк., тільки на адресу.
2. Пояснювальна записка до проекту постанови Кабінету Міністрів України на 5 арк., тільки на адресу.
3. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України на 6 арк., тільки на адресу.
4. Повідомлення про оприлюднення проекту нормативно-правового акта на 1 арк., тільки на адресу.

Голова Служби Л.О. Євдоченко

Пахомченко О.В. 281-67-02

0.31

Проект

Прим. №__

**КАБІНЕТ МІНІСТРІВ УКРАЇНИ**

**ПОСТАНОВА**

від 2019 р. №

Київ

**Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків**

Відповідно до підпункту "г" підпункту 3 пункту 2 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32, Кабінет Міністрів України **п о с т а н о в л я є**:

1. Затвердити Протокол спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків, що додається.

2. Для реалізації завдань, визначених Протоколом, міністерствам, іншим центральним органам виконавчої влади визначити (створити) підрозділи (команди, центри, групи), які забезпечуватимуть кіберзахист та реагування на кіберзагрози щодо об'єктів критичної інформаційної інфраструктури у відповідній галузі або сфері діяльності та/або покласти функції з кіберзахисту на підрозділи із захисту інформації.

3. Державним органам, органам місцевого самоврядування, органам управління Збройними Силами, іншим військовим формуванням, утвореним відповідно до законів, правоохоронним органам, підприємствам, установам та організаціям, у власності чи розпорядженні яких є об'єкти критичної інформаційної інфраструктури та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) таких об'єктів, організувати створення або створити на таких об'єктах підрозділи кіберзахисту та/або покласти функції з кіберзахисту на підрозділи із захисту інформації.

Прем'єр-міністр України В. ГРОЙСМАН

*Л.О. Євдоченко*

Проект

Затверджено
постановою Кабінету Міністрів
України від _____ 2019 р. №_____

# ПРОТОКОЛ
## спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків

1. Цей Протокол встановлює перелік взаємно пов'язаних у часі та за цілями обов'язкових дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак і кіберінцидентів та усунення їхніх наслідків.

Особливості взаємодії основних суб'єктів забезпечення кібербезпеки в умовах особливого періоду, правового режиму воєнного та надзвичайного стану, а також в районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії та проведення антитерористичної операції визначається спільними наказами основних суб'єктів забезпечення кібербезпеки.

2. Терміни, що використовуються у цьому Протоколі:

власник (розпорядник) об'єктів критичної інформаційної інфраструктури (суб'єкт/оператор критичної інформаційної інфраструктури) – державний орган, підприємство, установа або організація, юридична та/або фізична особа, які на правах власності, оренди або на інших законних підставах має право розпоряджатися об'єктом критичної інформаційної інфраструктури, що використовується для виконання життєво-важливих функцій або надання життєво-важливих послуг за призначенням у відповідних секторах (галузях) економіки або сферах діяльності;

життєво-важливі послуги – послуги, які забезпечуються підприємствами, установами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до настання негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;

життєво-важливі функції – функції, які виконують державні органи, підприємства, установи та організації будь-якої форми власності, порушення яких призводить до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;

суб'єкти кіберзахисту – суб'єкти господарювання незалежно від форми власності, що провадять діяльність та/або надають послуги, пов'язані з

кіберзахистом, які мають команди (центри, групи) реагування на кіберінциденти (CERT, CSIRT, CSIRT-NBU, MCSIRT, CSOC тощо).

Інші терміни вживаються у значеннях, наведених у Законі України «Про основні засади забезпечення кібербезпеки України».

3. Основними суб'єктами забезпечення кібербезпеки щодо виконання дій, встановлених цим Протоколом, є Держспецзв'язку, Міністерство оборони України та Генеральний штаб Збройних Сил України, СБУ, Національна поліція, розвідувальні органи України.

4. Під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків взаємодіють основні суб'єкти забезпечення кібербезпеки, суб'єкти кіберзахисту та суб'єкти/оператори критичної інформаційної інфраструктури (далі – суб'єкти взаємодії).

5. Протоколом встановлюються чотири фази взаємодії:

Фаза 0 – попередження кіберінцидентів та кібератак, превентивні заходи суб'єктів взаємодії щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури;

Фаза 1 – виявлення спроб та/або фактів вчинення кібератак та кіберінцидентів, стримування кібератак, обмін інформацією між суб'єктами взаємодії щодо таких фактів;

Фаза 2 – припинення та усунення наслідків кібератак та кіберінцидентів, відновлення сталого функціонування об'єктів критичної інформаційної інфраструктури;

Фаза 3 – аналіз виявлених кібератак та кіберінцидентів, проведених заходів, надання рекомендацій щодо попередження реалізації кіберзагроз.

У випадку отримання випереджувальної інформації про підготовку та безпосередню загрозу проведення кібератак та кіберінцидентів проти об'єктів критичної інформаційної інфраструктури держави з метою випереджувального реагування, нарощування готовності відповідних сил та засобів рішення про введення необхідних фаз приймається Національним координаційним центром кібербезпеки при РНБО України.

У випадку раптового початку проведення кібератак проти об'єктів критичної інформаційної інфраструктури держави рішення про введення відповідної фази приймаються керівництвом суб'єкта забезпечення кібербезпеки, силами та засобами якого виявлено факти проведення зазначених протиправних дій в кіберпросторі (кібератак, кіберінцидентів тощо), про що невідкладно інформуються інші суб'єкти забезпечення кібербезпеки.

6. Під час Фази 0 (попередження кіберінцидентів та кібератак, превентивні заходи суб'єктів взаємодії щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури):

1) Держспецзв'язку:

координує діяльність інших суб'єктів взаємодії щодо кіберзахисту;

здійснює оцінку стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах та виявляє можливі уразливі місця програмно-апаратних засобів, які використовуються для обробки інформації (місця, використовуючи які зловмисник може порушити

цілісність, доступність, конфіденційність інформації або спостережність системи);

надає рекомендації (у тому числі, шляхом розміщення на своєму офіційному веб-сайті), консультативно-методичну і практичну допомогу суб'єктам/операторам критичної інформаційної інфраструктури з питань протидії кіберзагрозам та кіберзахисту, зокрема щодо усунення вразливостей, виявлених за результатами проведення оцінок стану захищеності державних інформаційних ресурсів;

накопичує та проводить аналіз даних про кіберінциденти, а також веде інтерактивну базу даних про кіберінциденти (державний реєстр кіберінцидентів);

інформує інших суб'єктів взаємодії про кіберзагрози;

організує та проводить практичні семінари з питань кіберзахисту для суб'єктів взаємодії;

взаємодіє з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST;

розробляє, супроводжує і поширює між основними суб'єктами забезпечення кібербезпеки модель технічних розвідок іноземних держав, що здійснюють свою діяльність у кіберпросторі.

2) Міністерство оборони України та Генеральний штаб Збройних Сил України:

здійснюють заходи із підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), координують діяльність державних органів та органів місцевого самоврядування щодо підготовки та ведення кібероборони;

отримують від основних суб'єктів забезпечення кібербезпеки та узагальнюють інформацію щодо об'єктів критичної інформаційної інфраструктури воєнної сфери та сфери оборони держави;

проводять інформаційно-аналітичну діяльність та прогнозування розвитку обстановки у воєнній сфері, пов'язану з кіберзагрозами та кіберпростором;

підтримують сили та засоби для дій в кіберпросторі в готовності до виконання завдань за призначенням, здійснюють адекватне нарощування їх готовності в залежності від рівня загроз та ступенів реагування на них;

забезпечують несення бойового чергування визначених сил та засобів в інтересах підготовки та ведення кібероборони;

здійснюють підготовку та застосування Збройних Сил в кіберпросторі щодо виконання ними завдань за призначенням та безпечного використання ними кіберпростору;

здійснюють розвиток необхідних спроможностей Міністерства оборони України, Збройних Сил України для дій в кіберпросторі, підготовки та ведення кібероборони, створення та розвиток відповідних організаційних структур, їх комплектування, підготовку та всебічне забезпечення;

здійснюють військову співпрацю з НАТО, пов'язану з безпекою кіберпростору та спільним захистом від кіберзагроз, в тому числі й з військовими CERT країн-членів НАТО.

3) Розвідувальні органи України:

здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

надають в установленому законодавством порядку основним суб'єктам забезпечення кібербезпеки інформацію щодо виявлених в ході здійснення розвідувальної діяльності зовнішніх загроз національній безпеці у кіберпросторі;

подають Держспецзв'язку встановленим порядком розвідувальну інформацію про технічні розвідки іноземних держав, які діють у кіберпросторі.

4) СБУ:

здійснює відповідно до законодавства контррозвідувальну діяльність із запобігання розвідувально-підривним, терористичним та іншим посяганням на кібербезпеку України;

інформує основних суб'єктів забезпечення кібербезпеки про організацію, сили, засоби, методи, тактику розвідувально-підривної діяльності технічних розвідок іноземних держав, міжнародних та іноземних терористичних угруповань, які діють у кіберпросторі, що стали відомими в ході контррозвідувального забезпечення кібербезпеки держави;

негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів та інформує Держспецзв'язку про виявлені у процесі контррозвідувальної діяльності вразливості, що становлять загрозу безпеці об'єктів критичної інформаційної інфраструктури;

інформує суб'єктів/операторів критичної інформаційної інфраструктури про розкриті злочини, спрямовані проти безпеки їхніх інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, умови, що сприяють реалізації кіберзагроз, можливі причини виникнення таких умов та шляхи їхнього усунення.

5) Національна поліція:

інформує основних суб'єктів забезпечення кібербезпеки про організацію, сили, засоби, методи, тактику дій злочинних угрупувань, що стали відомими в ході оперативно-розшукової діяльності та при обміні інформацією з правоохоронними органами іноземних держав та міжнародних правоохоронних органів (Європол, Інтерпол тощо);

проводить профілактичні (попереджувальні) заходи із забезпечення кібербезпеки об'єктів критичної інфраструктури, а також роз'яснювальну роботу серед всіх верств населення;

повідомляє основних суб'єктів забезпечення кібербезпеки про виявлені у процесі оперативно-розшукової діяльності вразливості, що становлять загрозу безпеці об'єктів критичної інформаційної інфраструктури;

інформує суб'єктів/операторів критичної інформаційної інфраструктури про виявлені у процесі оперативно-розшукової діяльності посягання на безпеку їхніх інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, умови, що сприяють реалізації

кіберзагроз, можливі причини виникнення таких умов та шляхи їхнього усунення.

6) Суб'єкти кіберзахисту:

з урахуванням інформації, отриманої від основних суб'єктів забезпечення кібербезпеки аналізують ризики, впроваджують та вдосконалюють заходи з кіберзахисту;

здійснюють моніторинг кіберзагроз та виявлення кіберінцидентів;

проводять навчання та тренінги фахівців з кіберзахисту, зокрема з питань моніторингу кіберзагроз та виявлення кіберінцидентів.

7) Суб'єкти/оператори критичної інформаційної інфраструктури:

проводять оцінку поточного стану захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури (прогнозування виникнення нових кіберзагроз, їх врахування в моделі загроз, визначення необхідності її коригування тощо), розраховують ризики кібербезпеки;

на підставі аналізу розрахованих ризиків кібербезпеки здійснюють практичні заходи щодо забезпечення захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури з урахуванням інформації, отриманої від основних суб'єктів забезпечення кібербезпеки та/або суб'єктів кіберзахисту;

здійснюють моніторинг, реєстрацію та аудит подій на об'єктах критичної інформаційної інфраструктури;

супроводжують та актуалізують еталонні, архівні і резервні копії програмних компонентів, забезпечують зберігання резервних копій даних;

забезпечують виконання персоналом і користувачами вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки;

розробляють плани відновлення сталого функціонування своїх об'єктів критичної інформаційної інфраструктури з розрахованим цільовим часом відновлення, у разі порушення його функціонування внаслідок реалізації кібератаки;

надають на запит Держспецзв'язку необхідну інформацію про реалізовані заходи щодо кіберзахисту об'єктів критичної інформаційної інфраструктури.

7. Під час Фази 1 (виявлення спроб та/або фактів вчинення кібератак та кіберінцидентів, стримування кібератак, обмін інформацією між суб'єктами взаємодії щодо таких фактів):

1) Держспецзв'язку:

координує діяльність інших суб'єктів взаємодії щодо вжиття необхідних заходів з кіберзахисту з урахування виявлених кіберзагроз щодо об'єктів критичної інформаційної інфраструктури;

забезпечує реагування на кібератаки (кіберінциденти), залучаючи, за необхідності, можливості суб'єктів кіберзахисту;

інформує Національну поліцію та СБУ про об'єкт та джерело кібератаки, а суб'єктів/операторів критичної інформаційної інфраструктури щодо таких фактів;

обробляє та накопичує дані про вчинення та/або спроби вчинення кібератак (кіберінцидентів);

надає консультативно-методичну допомогу суб'єктам кіберзахисту і суб'єктам/операторам критичної інформаційної інфраструктури з питань реагування на кіберінциденти та заходів, які необхідно вжити для стримування кібератак.

2) Міністерство оборони України та Генеральний штаб Збройних Сил України з отриманням інформації про об'єкт та джерело кібератаки на об'єкти воєнної сфери або сфери оборони держави:

здійснюють з основними суб'єктами забезпечення кібербезпеки підготовку та проведення заходів щодо кібероборони;

вживають заходів щодо кібероборони (активного кіберзахисту);

інформують Держспецзв'язку, CERT-UA, СБУ, Національну поліцію, розвідувальні органи України та інших суб'єктів забезпечення кібербезпеки про ймовірні об'єкт та джерело кібератаки.

3) СБУ:

виявляє спеціальними методами та засобами кібератаки на об'єкти критичної інформаційної інфраструктури, надає їм оперативну та правову оцінку, перевіряє отриману інформацію стосовно їх спрямованості, мотивів, суб'єктів, засобів, методів, тактики, можливих наслідків, умов та чинників, що сприяли їх здійсненню;

повідомляє Держспецзв'язку первинну інформацію про виявлені кібератаки та кіберінциденти, інформує про результати її оперативної та правової оцінки, пропозиції щодо вжиття невідкладних заходів кіберзахисту, а також інші відомості, необхідні для вжиття зазначених заходів.

4) Національна поліція:

відповідно до законодавства здійснює заходи щодо розшуку та виявлення осіб, підозрюваних у скоєнні злочину, на підставі інформації про об'єкт та джерело кібератаки, отриманої від інших суб'єктів взаємодії;

інформує суб'єктів взаємодії про виявлені у процесі оперативно-розшукової діяльності про об'єкт та джерело кібератаки на об'єкти критичної інформаційної інфраструктури.

5) Суб'єкти кіберзахисту:

у разі виявлення кіберінцидентів або фактів здійснення кібератак, негайно інформують щодо таких подій всіх суб'єктів взаємодії;

здійснюють блокування джерел кібератак та кіберінцидентів;

інформують Держспецзв'язку, СБУ та Національну поліцію про об'єкт та джерело кібератаки для вжиття заходів із запобігання та припинення кіберзлочинів;

здійснюють обробку, накопичення та аналіз даних про спроби та/або факти вчинення кібератак (кіберінцидентів), а також про їхні наслідки.

6) Суб'єкти/оператори критичної інформаційної інфраструктури:

здійснюють невідкладне (протягом однієї години) інформування суб'єктів взаємодії про виявлені кіберінциденти чи спроби та/або факти вчинення кібератак;

негайно втручаються у разі виявлення кібератаки у процес функціонування об'єктів критичної інформаційної інфраструктури з метою мінімізації наслідків;

зберігають (фіксують) ознаки кібератаки (кіберінцидента), у тому числі на матеріальних носіях інформації;

підсилюють захист найбільш важливих сервісів, проводять екстрені заходи із забезпечення безпеки внутрішньої мережі, захисту периметра;

забезпечують своєчасне та безперешкодне ознайомлення представників Національної поліції та СБУ з виявленими слідами противоправної діяльності в кіберпросторі для їх оперативного аналізу.

8. Під час Фази 2 (припинення та усунення наслідків кібератак та кіберінцидентів, відновлення сталого функціонування об'єктів критичної інформаційної інфраструктури):

1) Держспецзв'язку:

надає консультативно-методичну і практичну допомогу суб'єктам/операторам критичної інформаційної інфраструктури та суб'єктам кіберзахисту, координує їх дії щодо припинення кібератаки або кіберінцидента (за необхідності з виїздом на місце події);

здійснює у разі необхідності практичні заходи, спрямовані на кіберзахист об'єктів критичної інформаційної інфраструктури та усунення наслідків кібератак і кіберінцидентів;

координує діяльність інших суб'єктів взаємодії щодо кіберзахисту під час відновлення сталого функціонування об'єктів критичної інформаційної інфраструктури;

вивчає спільно з Національною поліцією та СБУ механізми виявлених кіберінцидентів і кібератак, оцінює негативні наслідки та розробляє шляхи їхньої локалізації;

здійснює взаємодію з суб'єктами кіберзахисту, а також міжнародну взаємодію з командами реагування (CERT, CSIRT) інших країн щодо припинення (блокування) кібератак (кіберінцидентів) та усунення їхніх наслідків.

2) Міністерство оборони України та Генеральний штаб Збройних Сил України:

організовують та здійснюють заходи з кіберзахисту об'єктів воєнної сфери або сфери оборони держави, а також практичні заходи щодо усунення наслідків реалізації кібератак і кіберінцидентів;

надають консультативно-методичну та практичну допомогу підрозділам воєнної сфери та сфери оборони щодо припинення та усунення наслідків кібератаки або кіберінцидента (за необхідності з виїздом на місце події);

забезпечують безпосередню взаємодію з військовими CERT країн-членів НАТО щодо припинення кібератак (кіберінцидентів).

3) СБУ:

вивчає спільно з Держспецзв'язку та Національною поліцією механізми виявлених кіберінцидентів і кібератак, долучається до оцінки негативних наслідків та розробки шляхів їх локалізації;

інформує інших суб'єктів взаємодії про виявлені причини виникнення (здійснення) кіберінцидентів і кібератак, умови, що цьому сприяли, та шляхи їхнього усунення;

проводить заходи з документування фактичних даних про кібератаки, які могли призвести або призвели до вчинення кримінальних правопорушень, криміналістичне дослідження матеріалів, пов'язаних з кібератаками чи кіберінцидентами, здійснює оперативний розшук осіб, причетних до їх готування або скоєння;

негласно оцінює стан готовності об'єктів критичної інфраструктури до реагування на кібератаки та кіберінциденти.

4) Національна поліція:

відповідно до законодавства здійснює заходи щодо встановлення осіб, підозрюваних у скоєнні злочину, та притягнення їх до відповідальності;

вивчає спільно з Держспецзв'язку та СБУ механізми виявлених кіберінцидентів і кібератак, долучається до оцінки негативних наслідків та розробки шляхів їхньої локалізації;

проводить аналіз подій, спрямований на встановлення причин та передумов виявлених кіберінцидентів і кібератак.

5) Суб'єкти кіберзахисту:

здійснюють, з урахуванням інформації отриманої від Держспецзв'язку та СБУ, практичні заходи з кіберзахисту об'єктів критичної інформаційної інфраструктури та усувають наслідки кібератаки або кіберінцидента;

надають консультативно-методичну та практичну допомогу суб'єктам/операторам критичної інформаційної інфраструктури щодо припинення та усунення наслідків кібератаки або кіберінцидента (за необхідності з виїздом на місце події);

здійснюють взаємодію з Держспецзв'язку, а також міжнародну взаємодію з командами реагування інших країн (CERT, CSIRT, MCSIRT) щодо припинення (блокування) кібератак (кіберінцидентів) та усунення їхніх наслідків.

6) Суб'єкти/оператори критичної інформаційної інфраструктури

усувають наслідки кібератак (кіберінцидентів) з урахуванням інформації, отриманої від інших суб'єктів взаємодії;

здійснюють власними силами відновлення сталого функціонування комунікаційних та/або технологічних систем, виведених з ладу внаслідок кібератак (кіберінцидентів) після нейтралізації загроз, узгоджуючи такі дії з Держспецзв'язку та/або суб'єктами кіберзахисту (відповідно до підпорядкованості);

забезпечують, у разі необхідності, фізичний доступу представників Держспецзв'язку, суб'єктів кіберзахисту (відповідно до підпорядкованості) до об'єктів критичної інформаційної інфраструктури для виконання заходів щодо блокування та локалізації негативних наслідків кібератак (кіберінцидентів) та відновлення сталого функціонування цих об'єктів.

9. Під час Фази 3 (аналіз виявлених кібератак та кіберінцидентів, проведених заходів, надання рекомендацій щодо попередження реалізації кіберзагроз):

1) Держспецзв'язку:

здійснює аналіз даних про спроби та/або факти вчинення кібератак (кіберінцидентів), а також про їхні наслідки;

проводить актуалізацію державного реєстру кіберінцидентів з урахуванням нових даних про спроби та/або факти вчинення кібератак (кіберінцидентів), а також про їхні наслідки;

здійснює обмін інформацією з суб'єктами кіберзахисту, а також з командами реагування (CERT, CSIRT) інших країн щодо виявлених кібератак та кіберінцидентів та проведених заходів попередження реалізації кіберзагроз;

готує та надає суб'єктам кіберзахисту та суб'єктам/операторам критичної інформаційної інфраструктури практичних рекомендацій за результатами аналізу даних про спроби та/або факти вчинення кібератак (кіберінцидентів), а також про їхні наслідки.

2) Міністерство оборони України та Генеральний штаб Збройних Сил України:

встановленим порядком отримують та узагальнюють інформацію щодо результатів підготовки та ведення кібероборони;

здійснюють підготовку та надання рекомендацій щодо попередження реалізації кіберзагроз у воєнній сфері та сфері оборони;

забезпечують взаємодію з військовими CERT країн-членів НАТО та з виконавчими підрозділами суб'єктів забезпечення кібербезпеки з питань захисту інформації, кіберзахисту, кібербезпеки та кібероборони.

3) СБУ:

надає Держспецзв'язку підготовлену на основі оперативних матеріалів узагальнену інформацію щодо фактичної готовності об'єктів критичної інформаційної інфраструктури до можливих кібератак (кіберінцидентів), а також обґрунтовані пропозиції щодо її поліпшення;

надає Держспецзв'язку прогностичну інформацію щодо можливих в подальшому кібератак та кіберінцидентів, а також рекомендації щодо заходів кіберзахисту.

4) Національна поліція:

інформує громадян про заходи щодо забезпечення безпеки в кіберпросторі;

надає рекомендації суб'єктам кіберзахисту та суб'єктам/операторам критичної інформаційної інфраструктури, громадянам стосовно запобігання кіберзлочинам.

5) Суб'єкти кіберзахисту:

аналізують та проводять експертну оцінку даних про спроби та/або факти вчинення кібератак (кіберінцидентів), способи реалізації кібератак і кіберінцидентів, розробляють заходи з протидії кібератакам і кіберінцидентам;

ведуть власні бази даних кіберінцидентів, забезпечують передачу відповідної інформації до загальної інтерактивної бази даних про кіберінциденти (державного реєстру кіберінцидентів);

здійснюють взаємодію з Держспец'зв'язку та командами реагування (CERT, CSIRT) інших країн з питань попередження кіберзагроз (кіберінцидентів);

здійснюють підготовку та надання суб'єктам/операторам критичної інформаційної інфраструктури практичних рекомендацій щодо попередження кібератак (кіберінцидентів).

6) Суб'єкти/оператори критичної інформаційної інфраструктури:

здійснюють збір, узагальнення та аналіз інформації про кібератаки (кіберінциденти) та подають її до Держспецзв'язку та суб'єктам кіберзахисту (відповідно до підпорядкованості);

розраховують ризики кібербезпеки, на підставі розрахунків вдосконалюють політику безпеки та розробляють нові заходи з протидії кібератакам і кіберінцидентам.

*Л.О. Євдоченко*

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## до проекту постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків»

Мета: проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» створить механізм взаємодії суб'єктів забезпечення кібербезпеки під час попередження, виявлення, припинення та усуненні наслідків кібератак та кіберінцидентів.

**1. Підстава розроблення проекту постанови**

Проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» розроблено Адміністрацією Держспецзв'язку на виконання підпункту "г" підпункту 3 пункту 2 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32, та пункту 2 Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р.

**2. Обґрунтування необхідності прийняття акта**

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96, визначено основні загрози кібербезпеці для об'єктів критичної інфраструктури та шляхи протидії ним, у тому числі шляхом розроблення та впровадження протоколів спільних дій суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів (абзац четвертий підпункту 4.4 пункту 4 Стратегією кібербезпеки України).

14 грудня 2016 року під головуванням Секретаря РНБО України О. Турчинова відбулося засідання Національного координаційного центру кібербезпеки, на якому було розглянуто проект протоколу спільних дій для суб'єктів забезпечення кібербезпеки (моніторингу та оцінки загроз, реагування, розслідування тощо) під час виявлення кібератак та кіберінцидентів на об'єктах інформаційної інфраструктури та прийнято рішення про взяття його за основу (протокол № 3 від 14.12.2016).

Згідно з рішенням Національного координаційного центру кібербезпеки при РНБО України (підпункт 2.2 пункту 2 протоколу № 2 від 06.10.2016)

Держспецзв'язку необхідно створити з використанням команди реагування на комп'ютерні надзвичайні події України CERT-UA у складі Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку в інтересах суб'єктів забезпечення кібербезпеки загальні бази даних кіберінцидентів.

Проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» (далі – проект Постанови) підготовлено Адміністрацією Держспецзв'язку на виконання підпункту 3г) пункту 2 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32, та пункту 2 Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р.

**3. Суть проекту постанови**

Проект постанови встановлює перелік взаємно пов'язаних у часі та за цілями обов'язкових дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак і кіберінцидентів та усунення їх наслідків. Проектом постанови встановлюються чотири фази взаємодії суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури (суб'єктів взаємодії), а також їх функцій та обов'язків під час реалізації заходів з попередження, виявлення, припинення кібератак і кіберінцидентів та усунення їх наслідків.

**4. Правові аспекти**

Основними нормативно-правовими актами у сфері регулювання проекту Постанови є: Конституція України; Закон України "Про національну безпеку України"; Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"; Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96; Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32; Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373; Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23 серпня 2016 року № 563; План заходів на 2017 рік з реалізації Стратегії кібербезпеки України,

затверджений розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р.

**4-1. Відповідність засадам реалізації органами виконавчої влади принципів державної політики цифрового розвитку**

В проекті Постанови відсутні положення, які не узгоджуються із засадами реалізації органами виконавчої влади принципів державної політики цифрового розвитку.

Проект Постанови не стосується питань інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, електронної демократії, надання адміністративних послуг або цифрового розвитку.,

**5. Фінансово-економічне обґрунтування**

Реалізація проекту Постанови не потребує додаткових витрат з державного чи місцевих бюджетів.

**6. Прогноз впливу**

Проект Постанови є регуляторним актом.

Проект Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

Проект Постанови не спрямований безпосередньо на регулювання трудових відносин, а тому реалізація його положень не вплине на ринок праці.

Проект Постанови не стосується питань громадського здоров'я, екології та навколишнього середовища, інших сфер суспільних відносин.

**6-1. Стратегічна екологічна оцінка**

Проект Постанови не передбачає заходів для проведення моніторингу наслідків виконання документа державного планування для довкілля, у тому числі для здоров'я населення, та не стосується вимог Закону України «Про стратегічну екологічну оцінку».

**7. Позиція заінтересованих сторін**

Проект Постанови не матиме впливу на ключові інтереси заінтересованих сторін та не потребує проведення консультацій із заінтересованими сторонами.

Проект Постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

Проект Постанови не стосується питань соціально-трудової сфери та сфери наукової та науково-технічної діяльності.

**8. Громадське обговорення**

Проект Постанови розміщено на офіційному веб-сайті Держспецзв'язку за адресою: www.dsszzi.gov.ua.