СЛУЖБА БЕЗПЕКИ УКРАЇНИ

вул. Володимирська, 33, м. Київ, 01601, тел./факс: (044) 226-34-31, тел. 256-99-05
www.ssu.gov.ua, e-mail: sbu_cu@ssu.gov.ua Код ЄДРПОУ 00034074

05.06.2017 № 30/п-6008/п-400/4101 На № 7/163-7/2017 від 20.04.2017

Народному депутату України
Пастуху Т. Т.

Щодо розгляду депутатського запиту

Шановний Тарасе Тимофійовичу!

Службою безпеки України в межах компетенції уважно розглянуто Ваш депутатський запит, оголошений на засіданні Верховної Ради України 19.05.2017.

Повідомляємо, що 24 червня 2016 року розпорядженням Кабінету Міністрів України № 440-р (далі – Розпорядження), підготовленим на виконання рішення Ради національної безпеки і оборони України від 27.01.2016 "Про Стратегію кібербезпеки України", уведеного в дію Указом Президента України від 15.03.2016 № 96/2016, було схвалено план заходів на 2016 рік з реалізації Стратегії кібербезпеки України.

За результатами виконання передбачених зазначеним планом заходів, відповідно до вимог підпункту 2 пункту 2 Розпорядження Службою безпеки України було надано до Адміністрації Державної служби спеціального зв'язку та захисту інформації України пропозиції (дивись додаток) для їх узагальнення та інформування Апарату Ради національної безпеки і оборони України та Кабінету Міністрів України.

Крім того, інформуємо, що план заходів на 2017 рік з реалізації Стратегії кібербезпеки України, з урахуванням пропозицій Служби безпеки України було затверджено розпорядженням Кабінету Міністрів України від 10.03.2017 № 155-р.

Додаток: інформаційні матеріали щодо виконання Службою безпеки України плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України від 07.06.2017 № 30/4019, прим. № 1, на 10 аркушах.

З повагою

Голова Служби **В. Грицак**

Апарат Верховної Ради України
14.06.2017 10:39
ВХ. № 139461

криптографічного та технічного захисту інформації щодо обмеження використання продукції, технологій та послуг таких суб'єктів".

З огляду на те, що використання послуг представників російських IT-компаній в органах державної влади та на об'єктах критичної інфраструктури надає змогу російським спецслужбам фактично легально отримувати інформацію, що може бути використано на шкоду національним інтересам держави, ініційовано внесення до санкційного списку ряду суб'єктів господарювання IT-сфери, які перебувають під контролем держави-агресора, з метою обмеження використання їх продукції, технологій та послуг.

Також, у рамках визначеної законом компетенції СБ України здійснюються заходи щодо протидії розвідувально-підривній діяльності спецслужб РФ шляхом використання підконтрольних суб'єктів господарювання в IT-сфері для організації кібернетичного впливу на об'єкти критичної інформаційної інфраструктури держави.

У поточному році задокументовано протиправну діяльність групи осіб з числа засновників підприємств – резидентів України, які під виглядом постачальників легальних програмних продуктів, впроваджували на українських підприємствах оборонної сфери російське програмне забезпечення з прихованими функціями несанкціонованого доступу до інформації з обмеженим доступом.

За попередніми даними, вказане програмне забезпечення дозволяло здійснювати несанкціонований збір інформації з комп'ютерних мереж стратегічних підприємств військово-промислового комплексу України, яка у подальшому передавалася на сервери, які територіально розташовані в РФ. Окрім підприємств оборонної сфери, відповідне програмне забезпечення встановлювалось також у банківських установах, аеропортах, об'єктах промисловості, державних та приватних компаніях України.

Здійснюється постійний контроль стану виконання спеціальних обмежувальних заходів, застосованих за ініціативи СБ України до російських антивірусних програмних продуктів "Kaspersky" та "Dr.Web" Указом Президента України від 16.09.2015 № 549/2015 "Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" (далі – Указ).

З початку року, за результатами перевірок виконання Указу Президента у частині заборони використання вказаного російського антивірусного програмного продукту, СБУ попереджено низку фактів впровадження та використання в органах державної влади забороненого програмного забезпечення та антивірусних продуктів.

На виконання п. 24 "Розроблення правового механізму блокування електронних інформаційних ресурсів із забороненим законами контентом та підготовка пропозицій щодо його організаційно-технічного забезпечення"

Протягом 2014-2016 рр. СБ України спільно із зацікавленими державними органами неодноразово порушувалося питання щодо закріплення на законодавчому рівні механізму блокування інформаційних ресурсів із забороненим контентом в інтересах національної безпеки держави та захисту законних прав та свобод громадян.

Зокрема, конкретні пропозиції щодо організаційно-технічного та правового забезпечення такого механізму були передбачені проектом Закону України "Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю" (реєстр. № 2133а), розробленим за ініціативи СБ України та схваленим на засіданні профільного комітету Верховної Ради України.

Водночас, у вересні п.р. за результатами розгляду законопроекту на пленарному засіданні Верховної Ради України вказана ініціатива не була підтримана народними депутатами, хоча її ухвалення є одним з ключових елементів ефективної протидії наростаючій агресії РФ у національному сегменті кіберпростору України. Крім того, зазначена ініціатива критикується представниками приватного сектору, як така, що начебто дублює положення "диктаторського закону" від 16 січня 2014 року.

З огляду на те, що питання блокування протиправного Інтернет-контенту потребує термінового вирішення та пов'язане не лише з кібернетичною, а й з інформаційною безпекою держави, пропонуємо залучити до його упорядкування суб'єктів інформаційної сфери України (Держкомтелерадіо, Національну раду, НКРЗІ та Міністерство інформаційної політики), а також ініціювати відкрите громадське обговорення з метою вироблення оптимального правового механізму блокування електронних інформаційних ресурсів із забороненим законами контентом.

Служба безпеки України

"__" червня 2017 року

Реєстр. № 30 усі 752

Прим. № 1

Інформаційні матеріали

щодо виконання СБ України Плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 24.06.2016 № 440-р

На виконання п. 1 "Удосконалення нормативно-правової бази з питань кібербезпеки. Формування переліку першочергових нормативно-правових актів, які підлягають розробленню та/або внесенню змін".

З метою удосконалення нормативно-правової бази з питань кібербезпеки розроблено та направлено до РНБО України пропозиції до проекту Положення про Національний координаційний центр кібербезпеки у частині визначення завдань, повноважень та складу вказаного координаційного. Зазначені пропозиції враховано у Положенні про Національний координаційний центр кібербезпеки, затвердженому Указом Президента України від 07.06.2016 № 242.

За результатами аналізу існуючої нормативно-правової бази із забезпечення кібербезпеки держави та порядку організації кіберзахисту, підготовлено та направлено до Держспецзв'язку пропозиції щодо необхідності змін та доповнень до чинного законодавства України.

Зокрема, акцентовано увагу на необхідності удосконалення наступних нормативно-правових актів:

– затвердженої відомчим наказом Держспецзв'язку "Моделі технічних розвідок – 2030" (альтернативним варіантом є розробка окремої "Моделі кіберрозвідки – 2030");

– чинних нормативних документів системи технічного захисту інформації, що застосовуються при створенні комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом (НД ТЗІ 2.5-005-99, НД ТЗІ 3.6-001-2000, НД ТЗІ 3.7-001-99, НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-008-2002, НД ТЗІ 2.5-004-99), національними стандартами захисту інформації в ІТС, розробленими на основі міжнародних стандартів інформаційної безпеки серії ISO/IEC 27000;

– "Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" (затверджений наказом Адміністрації Держспецзв'язку від 10.06.2008 р. № 94), у частині необхідності інформування СБУ про загрози ІТС;

– ліцензійних умов провадження господарської діяльності або інших нормативно-правових актів (наприклад, ЗУ "Про захист інформації в інформаційно-телекомунікаційних системах"), спрямованих на забезпечення технічного захисту інформації в ІТС, задіяних у технологічних процесах, суб'єктами господарської діяльності у паливно-енергетичній сфері, сферах транспорту і зв'язку.

Також, надано рекомендації щодо необхідності розробки:

- доручення Президента України органам розвідки і контррозвідки щодо організації здобування оперативної інформації про кіберрозвідки іноземних держав;
- порядку збереження операторами і провайдерами телекомунікацій та Інтернет службових даних та технологічної інформації, що супроводжують здійснення

телекомунікацій, та їх надання правоохоронним органам в обсягах і в терміни, погоджені з СБУ та МВС;

- порядку спільного використання СБУ та МВС цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними;
- нормативно-правових актів щодо підвищення рівня фінансування співробітників підрозділів забезпечення кібербезпеки, які б надавали можливість подальшого маневру грошовими коштами для фінансового заохочення фахівців, задіяних у вирішенні найбільш складних і важливих завдань у сфері кібербезпеки.

З метою посилення можливостей СБ України у сфері кібербезпеки, забезпечення ефективного і дієвого реагування на загрози національній безпеці, розроблено та направлено до Адміністрації Президента України (№ 16/6289 від 27.10.2016 р.) законопроект "Про внесення змін до Закону України "Про Службу безпеки України" (щодо доступу до інформаційних ресурсів)" для подальшого подання на розгляд Верховної Ради України.

Згідно із вказаним документом СБ України надається право при здійсненні оперативно-розшукової та контррозвідувальної діяльності отримувати у визначеному порядку прямий доступ до автоматизованих інформаційних систем, реєстрів та банків даних, держателем (адміністратором) яких є державні органи, а також зобов'язує суб'єктів, яким СБУ адресовано офіційний запит, невідкладно, але не більше ніж протягом трьох робочих днів, надавати інформацію, що запитується.

Здійснено доопрацювання з метою підготовки до другого читання проекту Закону України "Про основні засади забезпечення кібербезпеки України" (реєстр. № 2126а) та підготовки до повторного першого читання проекту Закону України "Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю" (реєстр. № 2133а). Відповідні пропозиції направлені до профільних комітетів Верховної Ради України.

На виконання п. 4 "Розроблення проекту Концепції впровадження Центру реагування на інциденти кібербезпеки в банківській системі та платіжному просторі України"

З метою попередження, виявлення та припинення фактів несанкціонованих дій у відношенні інформаційної інфраструктури установ фінансового сектору України, а також розроблення ефективного механізму оперативного реагування на інциденти кібербезпеки в банківській системі та платіжному просторі України, СБ України ініційовано створення спільної з НБУ робочої групи.

У жовтні поточного року у форматі міжвідомчого круглого столу "Кібербезпека в банківській сфері" обговорено питання щодо необхідності створення Національним банком України Центру реагування на інциденти кібербезпеки у банківській системі та платіжному просторі України (CERT-NBU), порядку його взаємодії з командами реагування на комп'ютерні інциденти, правоохоронними органами і банками України.

За результатами роботи Круглого столу, СБ України підготовлено та направлено на адресу НБУ пропозиції щодо функціонування Центру реагування на інциденти кібербезпеки у банківській системі та платіжному просторі України, а також взаємодії між українськими банками, правоохоронними органами та командами реагування на комп'ютерні інциденти суб'єктів забезпечення кібербезпеки держави.

Крім того, з метою удосконалення системи кіберзахисту банківських інформаційно-телекомунікаційних систем, СБ України направлено до Національного банку інформаційно-аналітичні матеріали щодо стану кіберзахисту електронних платіжних систем вітчизняних банків та пропозиції з підвищення його ефективності.

На виконання п. 5 "Забезпечення участі у заходах щодо зміцнення міжнародного співробітництва у сфері кібербезпеки, зокрема через утворення спільних двосторонніх або багатосторонніх груп для забезпечення здійснення розслідувань кіберзлочинів, а також зміцнення транскордонного співробітництва шляхом проведення спільних операцій, обміну статистичною інформацією і досвідом".

СБ України активізовано двостороннє співробітництво зі спецслужбами та правоохоронними органами США, країн ЄС (Естонії, Литви, Республіки Польща, Чеської Республіки, Румунії, Великобританії, Франції, Республіки Ірландія) та СНД (Республіки Білорусь, Республіки Молдова, Республіки Казахстан, Азербайджан) у сфері обміну досвідом з питань забезпечення кібербезпеки, а також проведення спільних операцій, спрямованих на протидію кіберзагрозам міжнародного характеру.

У рамках функціонуючої у м. Києві спільної робочої групи СБ України - ФБР США з питань протидії міжнародній кіберзлочинності на регулярній основі вирішуються питання оперативного обміну інформацією та спільних розслідувань кіберзлочинів. У липні 2016 р. за сприяння американської сторони представники СБУ взяли участь в організованій ФБР США Міжнародній конференції з питань протидії кіберзагрозам, а також в організованих ЦРУ США навчальних тренінгах щодо проникнення у комп'ютерні мережі.

Налагоджено взаємодію СБ України зі спецслужбами Туреччини, а також країн Азії, насамперед Південної Кореї, Японії у сфері забезпечення кібернетичної безпеки. Протягом поточного року проведено низку зустрічей на рівні експертів із представниками спецслужб та правоохоронних органів вказаних країн, у ході яких визначені конкретні напрямки співробітництва по лініям боротьби з кібертероризмом, протидії кіберзагрозам, захисту критичної інформаційної інфраструктури.

У рамках співробітництва зі спецслужбами Туреччини у серпні 2016 р. представники СБ України взяли участь у тренінгу з питань протидії проникненню ворожих спецслужб до мереж критичної інфраструктури держави, аналізу шкідливого вітчизняного програмного забезпечення та захисту державних мереж від кібератак, що проходив у Близько-Східному університеті, м. Анкара (Туреччина).

На виконання п. 6 "Забезпечення поглиблення співпраці України з ЄС та НАТО для посилення спроможностей держави у сфері кібербезпеки, зокрема в рамках Річної національної програми співробітництва Україна — НАТО на 2016 рік".

СБ України у межах компетенції забезпечено високий рівень взаємодії з міжнародними інституціями для посилення можливостей держави у сфері кібербезпеки. Зокрема, налагоджено співробітництво з Комітетом Конвенції Ради Європи у сфері протидії кіберзлочинності. У травні п.р. представника СБ України було обрано до керівного складу Бюро Комітету Конвенції. У листопаді п.р. взято участь у 16-му пленарному засіданні вказаного Комітету, в ході якого на міжнародному рівні представлено особливості Національної системи кібербезпеки України.

Налагоджено взаємодію з Радою Європи та Європейським Союзом у рамках проекту "Cybercrime@EAP" у напрямку активізації міжнародного співробітництва по лінії протидії кіберзлочинності в країнах-учасниках "Східного партнерства".

У ході регіональної конференції проекту "Cybercrime@EAP II", яка проходила у м. Києві у квітні 2016 р., з метою підвищення взаємодії правоохоронних органів та спецслужб країн-учасників, СБ України запропоновано розроблений для оформлення офіційними рекомендаціями Ради Європи шаблон запитів щодо отримання даних у рамках процедур міжнародного співробітництва із застосуванням мережі національних контактних пунктів 24/7.

Крім того, СБ України було запропоновано започаткування Радою Європи проекту "Cybercrime@EAP III", спрямованого на оптимізацію співробітництва державних, в т.ч. правоохоронних і спеціальних органів країн-членів Східного партнерства з приватним IT-сектором у сфері протидії кіберзагрозам. Ініціатива була підтримана керівництвом Комітету Конвенції Ради Європи.

Крім того, у рамках співробітництва з Радою Європи представники СБ України взяли участь у ряді міжнародних заходів, спрямованих на обмін досвідом та покращення міжнародної взаємодії у сфері кібербезпеки, зокрема, Конференції Європолу з питань боротьби з кіберзлочинністю; II Регіональному засіданні країн-членів Східного партнерства; Міжнародній конференції, присвяченій започаткуванню нового проекту РЄ "Глобальні дії в боротьбі з кіберзлочинністю: від GLACY до GLACY+".

Упродовж звітного періоду СБ України започатковано співробітництво у сфері протидії міжнародній кіберзлочинності з Консультативною Місією ЄС в Україні з питань реформування сектору цивільної безпеки. Зокрема, у червні п.р. відбулась зустріч з радником КМЄС з питань боротьби з кіберзлочинністю, за її результатами досягнуто домовленості щодо надання КМЄС сприяння СБУ в освітній сфері.

У листопаді 2016 р. здійснено інформаційно-аналітичне супроводження 5-го засідання Робочої групи ГУАМ з протидії кіберзагрозам, створеної за ініціативи СБ України. На засіданні погоджено проект Меморандуму про взаєморозуміння держав-членів Організації за демократію та економічний розвиток - ГУАМ у сфері кібербезпеки. За сприяння СБ України вказану Робочу

групу включено до складу учасників проекту Ради Європи "Cybercrime@EAP II".

На виконання "Річної національної програми співробітництва Україна - НАТО на 2016 рік", затвердженої Указом Президента України від 12 лютого 2016 року № 45, СБ України продовжує взаємодію з Північноатлантичним альянсом у сфері забезпечення кібербезпеки у рамках функціонування Трастового фонду Україна-НАТО з питань кібербезпеки.

У взаємодії із зацікавленими державними органами, враховуючи рекомендацій Місії України при НАТО щодо координації діяльності центральних органів виконавчої влади та їх структурних підрозділів, СБ України вжито заходів з реалізації першого етапу проекту трастового фонду Україна-НАТО (далі – ТФ НАТО), яким передбачено створення Ситуаційних центрів з протидії кіберзагрозам на базі Держспецзв'язку та Служби безпеки України з розгалуженою мережею автоматизованих датчиків подій, імплементованих в інформаційно-телекомунікаційних мережах об'єктів критичної інформаційної інфраструктури, що підлягають захисту у реальному часі, а також відповідних лабораторій для розслідування інцидентів у кібернетичній сфері.

Упродовж квітня-травня поточного року, під час робочих зустрічей та консультацій на рівні експертів, з румунською стороною узгоджено тендерну документацію у відповідності до проектного рішення та опрацьовано процедуру закупівлі комп'ютерного й телекомунікаційного обладнання.

Завершено проведення тендерних процедур та визначено головного підрядника постачання та інсталяції відповідного технічного обладнання. Тривають заходи щодо укладання відповідної додаткової угоди між СБУ та Румунською службою інформації щодо визначення порядку та умов постачання й передачі обладнання українській стороні.

У рамках подальшого розвитку та практичного наповнення ТФ НАТО за освітнім напрямом, у взаємодії з Міжнародним Секретаріатом НАТО, СБ України вжито заходів з розробки та реалізації програми поглиблених навчальних та практичних курсів у сфері протидії кіберзагрозам, орієнтованої на представників безпекового сектору України.

З метою оптимізації міжвідомчої взаємодії та координації заходів з реалізації ТФ НАТО, розпорядженням ЦУ СБ України від 09.03.2016 № 96 "Про утворення Координаційної ради з реалізації Трастового фонду Україна – НАТО з питань кібербезпеки", створено Координаційну раду Трастового фонду Україна – НАТО при СБ України.

На виконання п. 7 "Організація у рамках реалізації Трастового фонду Україна — НАТО з кібербезпеки проведення проектно-конструкторських робіт, розрахунків фінансових витрат, та після їх схвалення Кабінетом Міністрів України створення на базі СБУ та Держспецзв'язку ситуаційних центрів з кібербезпеки, об'єднаних в єдину систему виявлення і запобігання кіберзагрозам на об'єктах критичної інфраструктури".

Створено окремий структурний підрозділ у складі функціонального підрозділу Центрального управління СБУ, який організовує, координує в

системі СБУ та безпосередньо здійснює контррозвідувальний захист інтересів держави у сфері інформаційної безпеки, з функціями оперативного пошуку, інформаційного та технологічного забезпечення оперативного процесу, а також функціональністю міжнародного телекомунікаційного контактного пункту та підрозділу швидкого реагування на виявлені кібератаки (Ситуаційний центр з кібербезпеки).

На сьогодні з метою забезпечення умов для належного функціонування Ситуаційного центру з кібербезпеки СБ України, Проектним інститутом Служби безпеки здійснюються заходи з проведення відповідних проектно-конструкторських робіт та розрахунків фінансових витрат.

На виконання п. 10 "Організація та проведення конференцій, семінарів, форумів, засідань за круглим столом, тренінгів, навчань з питань інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі на державному та міжнародному рівні".

18 березня 2016 р. із залученням представників 8 міністерств і відомств, 4 наукових установ та 17 вищих навчальних закладів організовано та проведено на базі Національної академії СБ України VII Науково-практичну конференцію "Актуальні проблеми управління інформаційною безпекою держави" з метою обговорення актуальних проблем у сфері інформаційної та кібербезпеки та вироблення перспективних шляхів їх вирішення.

У рамках співробітництва з Радою Європи, 5 квітня 2016 року у м. Києві проведено міжнародний круглий стіл за участю представників зацікавлених органів державної влади, спеціальних та правоохоронних органів та провідних провайдерів України з питань стану імплементації положень Конвенції Ради Європи "Про кіберзлочинність" в частині співробітництва державного та приватного секторів, зокрема забезпечення отримання та збереження цифрових слідів комп'ютерних злочинів та співпраці з уповноваженими державними органами у сфері боротьби з кіберзлочинністю та кібертероризмом.

У рамках співробітництва з Агентством по боротьбі з організованою злочинністю Великобританії (NCA) проведено із залученням британських експертів тренінг для фахівців Служби безпеки України з питань обробки та аналізу значних масивів інформації, які циркулюють у кіберпросторі.

На виконання п. 14 "Здійснення збирання, узагальнення, аналізу та оцінки інформації про терористичні загрози на об'єктах критичної інфраструктури".

СБ України в рамках визначеної законом компетенції на постійній основі здійснюються заходи із збирання, узагальнення, аналізу та оцінки інформації про терористичні загрози на об'єктах критичної інфраструктури, виявлені вразливості та негативні чинники, що сприяють їх реалізації, з метою інформаційно-аналітичного забезпечення органів державної влади та організації ефективної протидії кібернетичному виливу спецслужб іноземних держав.

терористичних організацій, окремих груп та осіб на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави.

З метою вжиття адекватних заходів протидії кіберзагрозам та забезпечення належного рівня кіберзахисту у поточному році СБ України здійснено аналіз виявлених вразливостей ІТС об'єктів енергетичного та транспортного комплексів, державних реєстрів, інформаційних ресурсів органів державної влади та місцевого самоврядування.

За результатами ряду спеціальних оперативних експериментів, спрямованих на перевірку стану охорони телекомунікаційних об'єктів, які можуть стати об'єктами диверсійно-терористичних посягань, у поточному році вжито заходів щодо підвищення рівня їх антитерористичної захищеності та безпеки функціонування.

Крім того, ***збирання, узагальнення, аналіз та оцінка інформації про терористичні загрози на об'єктах критичної інфраструктури*** проводиться у ході формування пропозицій до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави у рамках виконання постанови Кабінету Міністрів України від 23.08.2016 № 563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави" (далі - Перелік).

Станом на 30 листопада 2016 року опрацьовано інформацію про власні системи для включення до Переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави наступних державних органів: Міністерства внутрішніх справ, Міністерства охорони здоров'я, Державної казначейської служби, Державної міграційної служби, Державної служби статистики, Державної служби з питань геодезії, картографії та кадастру, Державного космічного агентства, Пенсійного фонду України.

Водночас, основні суб'єкти подання відомостей, такі як Міністерство енергетики та вугільної промисловості України, Міністерство юстиції України, Міністерство інфраструктури України, Міністерство фінансів України, Державна фіскальна служба України та інші, які є власниками або розпорядниками інформаційних систем, несанкціоноване втручання в роботу яких може призвести до виникнення надзвичайних ситуацій техногенного характеру з незворотними наслідками для екології та населення, зокрема блокування систем життєзабезпечення, інформацію для формування Переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури по сьогодні не надали. Також не отримано інформації про власні інформаційно-телекомунікаційні системи від підприємств, які мають стратегічне значення для економіки та безпеки держави (визначені Постановою КМУ від 23.12.2004 № 1734). Граничний термін надання відомостей, при цьому, сплив 07 грудня поточного року.

Згадані вище органи, як правило не зацікавлені у віднесенні власних інформаційних систем до вказаного Переліку, оскільки в такому випадку у державних контролюючих органів виникають повноваження щодо проведення заходів з контролю за станом технічного захисту інформації, яка в них обробляється та, за необхідності, втілення заходів протидії технічним розвідкам (зокрема, впровадження комплексної системи захисту інформації), що обумовлює додаткове фінансування.

На виконання п. 16 "Удосконалення взаємодії між основними суб'єктами забезпечення кібербезпеки, зокрема упорядкування порядку спільного використання Національною поліцією та СБУ цілодобової

контактної мережі для надання невідкладної допомоги під час розслідування кіберзлочинів".

З метою удосконалення взаємодії між Національною поліцією та СБ України у сфері забезпечення кібербезпеки розроблено та направлено до Національної поліції пропозиції щодо визначення та упорядкування порядку спільного використання Національною поліцією та СБ України цілодобової контактної мережі для надання невідкладної допомоги під час розслідування кіберзлочинів.

За результатами ряду експертних консультацій та міжвідомчих робочих нарад узгоджено наступні першочергові спільні заходи щодо оптимізації взаємодії (протокол наради № 41/19757 від 16.11.2016):

1. визначення організаційних та технологічних механізмів спільного використання каналів національного контактного пункту "24/7" у відповідності до розподілу компетенцій у сфері забезпечення кібербезпеки держави;
2. встановлення порядку взаємодії Національної поліції та СБУ при використанні процедур міжнародного судового та поліцейського співробітництва з використанням міжнародної мережі контактних пунктів "24/7".

Наразі тривають заходи з розроблення проекту наказу щодо спільного порядку використання Національною поліцією та СБ України цілодобової контактної мережі "24/7" у відповідності до розподілу компетенцій у сфері забезпечення кібербезпеки держави.

На виконання п. 17 "Формування пропозицій щодо організаційно-технічної моделі кіберзахисту, зокрема в частині оперативного реагування на кіберінциденти стосовно об'єктів критичної інфраструктури".

З метою формування та узгодження пропозицій щодо організаційно-технічної моделі кіберзахисту, СБ України взято участь у міжвідомчій нараді, за результатами якої узгоджено Протокол спільних дій суб'єктів забезпечення кібербезпеки (моніторинг та оцінка загроз, реагування, розслідування тощо) під час виявлення кібератак та кіберінцидентів на об'єктах інформаційної інфраструктури (Держспецзв'язку реєстр. № 04/02/01-2088 від 04.11.2016).

Для оптимізації механізму взаємодії СБ України з Держспецзв'язку під час реагування на кіберінциденти у відношенні об'єктів критичної інфраструктури, СБ України розроблено та направлено до Держспецзв'язку пропозиції щодо коригування "Порядку взаємодії Служби безпеки України і Державної служби спеціального зв'язку та захисту інформації України", затвердженого спільним наказом від 23.05.2015 № 343/ДСК/55/ДСК.

На виконання п. 20 "Обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави-агресора, визнаної Верховною Радою України, зокрема посилення державного контролю за станом