ISSN 2073-7394

Національний університет
“Полтавська політехніка імені Юрія Кондратюка”

National University
“Yuri Kondratyuk Poltava Polytechnic”

Системи управління, навігації та зв'язку

Control, navigation and communication systems

Випуск 1 (75) **Issue 1 (75)**

Щоквартальне видання

Засноване у 2007 році

У журналі відображені результати наукових досліджень з розробки та удосконалення систем управління, навігації та зв’язку у різних проблемних галузях.

Засновник і видавець:
Національний університет
“Полтавська політехніка імені Юрія Кондратюка”

Телефон:
+38 (050) 302-20-71

E-mail редколегії:
kuchuk_nina@ukr.net

Інформаційний сайт:
http://journals.nupp.edu.ua/sunz

Quarterly

Founded in 2007

Journal represent the research results on the development and improvement of control, navigation and communication systems in various areas

Founder and publisher:
National University
"Yuri Kondratyuk Poltava Polytechnic"

Phone:
+38 (050) 302-20-71

E-mail of the editorial board:
kuchuk_nina@ukr.net

Information site:
http://journals.nupp.edu.ua/sunz

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор

*Журнал індексується міжнародними наукометричними базами: Index Copernicus (ICV = **82.05**), General Impact Factor, Google Scholar, Academic Resource Index, Scientific Indexed Service*

*Затверджений до друку Вченою Радою Національного університету “*Полтавська політехніка імені Юрія Кондратюка*” (протокол від 09 лютого 2024 року № 2).*

Свідоцтво про державну реєстрацію КВ № 24464-14404 ПР від 27.03.2020 р.

Включений до “Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії ” до категорії Б – наказами МОН України від 17.03.2020 № 409 та від 09.02.2021 № 157

Полтава • 2024

УДК 351.865 **doi: 10.26906/SUNZ.2024.1.066**

Є. О. Живило, І. В. Ромашко

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

ПРОТОКОЛ СПІЛЬНИХ ДІЙ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІД ЧАС РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, А ТАКОЖ ПРИ УСУНЕННІ ЇХ НАСЛІДКІВ

Анотація. Кіберпростір разом з іншими фізичними просторами визнано одним з театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ (Дорожня карта створення Кібервійськ Збройних Сил України – наказ Генерального штабу Збройних Сил України, від 22.04.2022 №48) до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури держави від кібератак, а й проведення превентивних наступальних кібердій (проведення кібероперацій) у кіберпросторі, що включає порушення сталого функціонування критично важливих об'єктів інфраструктури противника шляхом руйнування електронно-комунікаційних систем, які управляють такими об'єктами. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. Зважаючи на досвід ведення бойових дій під час введення правового режиму воєнного стану та враховуючи невизначеність суб'єктів та об'єктів, їх функцій та завдань для дій в певних сферах, в тому числі і у сфері кібербезпеки, в мирний час, призвів до незлагодженості та неузгодженості цих дій суб'єктами забезпечення кібербезпеки держави. А враховуючи, що з введенням правового режиму воєнного стану певні суб'єкти міняють своє місцезнаходження, переміщують інформаційні активи та обладнання на нові місця дислокації з використанням хмарних сервісів, зазначене доволі сильно ускладнює процес узгодження та координації дій щодо реагування на кіберінциденти, а також усунення їх наслідків. Це призводить до вимушеного перерозподілу завдань та функцій по виконанню заходів кіберзахисту на різних об'єктах. За цих умов, на постійній чи тимчасовій основі створюються нові суб'єкти кіберзахисту, що потребує часу на набуття ними спроможностей для виконання завдань за призначенням. У такій ситуації Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, сталого реагування на загрози в кібернетичному просторі, досягнення кіберстійкості на всіх рівнях та взаємодії складових сектору безпеки і оборони щодо забезпечення кібербезпеки в рамках кібероборони держави. Отже, виходячи з необхідності наукового обґрунтування інституційних засад постає необхідним чітко визначити: "перелік суб'єктів забезпечення кібербезпеки щодо виконання дій, встановлених цим Протоколом", як в мирний час так і в умовах правового режиму воєнного стану; зазначеним вище суб'єктам їх роль та місце, перелік та порядок дій під час реагування на кіберінциденти та усунення їхніх наслідків, як в мирний час так і в умовах правового режиму воєнного стану. При цьому, наукова новизна очікуваних результатів полягає в теоретичному обґрунтуванні та наданні практичних рекомендацій щодо вдосконалення механізмів управління та взаємодії складовими (х) сектору безпеки і оборони під час планування підготовки держави до кібероборони, проведення заходів з нейтралізації та активної протидії кіберзагрозам в національному сегменті кіберпростору держави.

Ключові слова: суб'єкти забезпечення кібербезпеки, кіберпростір, кіберзахист, активні кібердії, деструктивні кібератаки, критична інформаційна інфраструктура.

Постановка проблеми у загальному вигляді

Сьогодні, створення умов безпечних спільних дій суб'єктів забезпечення кібербезпеки (далі – СЗК) в національному сегменті кіберпростору України, реалізація державно-приватної взаємодії у сфері кібербезпеки (далі – КБ), а також їх об'єднане застосування в інтересах особи, суспільства і держави є доволі суттєвим та змістовним завданням.

За цих умов посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України набуває першочергового значення і стає запорукою подальшого успіху на шляху створення безпеки життєво важливих національних інтересів України у кіберпросторі.

Відповідно до статті 5 закону України "Про основні засади забезпечення кібербезпеки України" координацію діяльності у сфері КБ як складової національної безпеки України здійснює Президент України через очолювану ним Раду національної безпеки і оборони України (Далі – РНБО України). В свою чергу Національний координаційний центр кібербезпеки (Далі – НКЦК), як робочий орган РНБО України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони які забезпечують КБ.

Внаслідок повномасштабної збройної агресії росії проти України функціонування національної системи кібербезпеки (Далі – НсКБ) під час дії правового режиму воєнного стану в Україні було частково нівельовано.

Тому з метою визначення правових та організаційних основ забезпечення національних інтересів України у кіберпросторі було запропоновано внести

зміни до законів України:

- "Про Національний банк України" де визначався порядок функціонування, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України;

- "Про оборону України" щодо здійснення заходів з кібероборони (активного кіберзахисту) (Далі – КО) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії.

- "Про Державну службу спеціального зв'язку та захисту інформації України" щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, координації діяльності СЗК щодо кіберзахисту [8], впровадження організаційно-технічної моделі кіберзахисту, координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури (Далі – ОКІ) на вразливість.

Паралельно з цим, також слід відмітити січневі події 2022 року, які відбулись на тлі загострення ситуації в Україні. Так, у ніч з 13 на 14 січня низка українських урядових ресурсів зазнала атак хакерів, які здійснили Deface (англ. deface – заміна сторінок сайтів) і, як повідомили експерти Microsoft, запустили шкідливе програмне забезпечення, замасковане під програми-вимагачі.

При цьому необхідно зауважити, що співробітники НКЦК діяли відповідно до своїх повноважень, визначених Положенням, затвердженим Указом Президента України від 7 червня 2016 року № 242, а саме здійснювали координацію та контроль за діяльністю суб'єктів сектору безпеки та оборони, які забезпечували кібербезпеку, а також аналізували дані про кіберінциденти щодо державних електронних інформаційних ресурсів та критично важливих об'єктів інфраструктури держави [1].

Зважаючи на ситуацію яка склалась, Апаратом РНБО України було прийнято рішення, щодо виконання ряду заходів які дозволять запобігти (унеможливлять) в майбутньому ймовірним кіберінцидентам [5], а саме:

1. Забезпечення розробки та впровадження узгодженого Протоколу спільних дій СЗК, власників (розпорядників) об'єктів критичної інформаційної інфраструктури (Далі – ОКІІ) при виявленні, попередженні, припиненні кібератак та кіберінцидентів, а також під час усунення їхніх наслідків;

2. Запровадження механізмів додаткового стимулювання мотивації до праці фахівців сектору безпеки та оборони, які беруть безпосередню участь в організації та реалізації заходів щодо протидії кіберзагрозам;

3. Активізація співпраці із закордонними партнерами щодо протидії кібератакам на критичну інформаційну інфраструктуру, проведення розслідувань таких кібератак, встановлення причин та умов, що призвели до їх скоєння.

Отже враховуючи зазначене вище, завдання щодо розробки Протоколу спільних дій СЗК під час реагування на кіберінциденти, а також при усуненні їх наслідків постає сама собою.

Аналіз останніх досліджень і публікацій

Активність у кіберпросторі України має систематичний характер. Протягом першого півріччя 2022 року Україна знову опинилася в центрі кібератак, спрямованих на її критичну інфраструктуру (Далі – КІ). Сьогодні протистояння в кіберпросторі національного сегменту відбувається на тлі військової агресії з боку росії.

Для реалізації її планів, до оперативного складу угрупування діяльність якого спрямована на реалізацію активних дій у національному кіберпросторі України залучені такі російськомовні хакерські угруповання, як ФАПСІ, КиберБеркут, Iridium, Sofacy Group (ГРУ ГШ РФ), APT29 (ФСБ РФ), Turla (ФСБ РФ), UAC-0010 (ФСБ РФ), Sandworm, Тролі з Ольгіна та інші.

При цьому, на противагу кібер угрупованням росії розгорнута ціла українська ІТ-армія яка нараховує понад 300 тисяч кіберфахівців. До її складу входять: Служба безпеки України (Далі – СБ України), CERT-UA Державної служби спеціального зв'язку та захисту інформації України (Далі – ДССЗЗІ України), InformNapalm, IT Army of Ukraine, Український Кібер Альянс (FalconsFlame, Trinity, Ruh8), Українські Кібер Війська, Центр "Миротворець" та інші. Вона об'єднує українських та міжнародних ІТ-фахівців, засновників, творців, комунікаторів для боротьби з російською агресією на кіберфронті. В цих умовах ІТ-армія проводить кібератаки і DDoS-атаки на ресурси бізнес-корпорацій ("Газпром", "Лукойл"), банків ("Сбербанк", ВТБ, "Газпромбанк"), а також на сайти держ-служб росії, кремля й держдуми.

Попри зазначені перемоги все ж таки їхні атаки на наші критичні системи, об'єкти та інфраструктуру все ж таки мали (ють) успіх.

За оприлюдненими даними Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA до групи загроз [10], яка створила реальну небезпеку вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури за цей період слід віднести: WhisperGate /WhisperKill, FoxBlade, він же Hermetic Wiper, SonicVote, HermeticRansom, CaddyWiper, DesertBlade, Industroyer2, Lasainraw, IssacWiper, FiberLake, DoubleZero, Cobalt Strike Beacon та інші [12].

Виходячи з використаних тактик противника, слід зазначити, що в основному вони були спрямовані на:

блокування роботи ОКІІ, телекомунікаційного обладнання та приладдя органів державної влади, доведення його до непридатності для використання з наступним виведенням його з ладу взагалі;

застосування фішингових атак на держслужбовців, військових, працівників КІ з метою отримання конфіденційної або секретної інформації, а також фінансових даних;

отримання кіберзловмисниками інформації щодо облікових даних, які дозволяють дістати доступ до систем, сервісів або служб, якими користу-

ються відповідні співробітники, персонал, особи та працівники на своїх персональних ЕВМ на об'єктах інформаційної діяльності установ (організацій) державної, приватної та колективної форми власності;

розповсюдження в популярних мессенджерах шахрайських публікацій щодо отримання соціальних виплат, фінансової допомоги та інше, метою яких є компрометація та отримання персональної інформації власників платіжних карток.

Але попри зазначені негаразди в цих умовах відбулась згуртованість дій фахівців КБ Європейського Союзу, європейських країн, уряду США, НАТО і ООН дії яких спрямовані на противагу деструктивним атакам, шпигунським операціям, руйнування чи деградацію української мови, обмеження урядових та військових функцій і підривання довіри громадськості до цих же інституцій.

В цих умовах урядом України проводиться ряд заходів пов'язаних з розбудовою державної системи захисту КІ, визначаються правові та організаційні засади забезпечення її діяльності, реалізується державна політика у сфері захисту КІ, безпечним користуванням українцями телефонами, інтернетом та інше.

Аналізуючи досвід реагування на кіберзагрози та кіберінциденти спеціалістами провідних країн світу в галузі КБ, українські фахівці з КБ дійшли висновку, що велика кількість таксономій і схем класифікації інцидентів забезпечують чудові вказівки в рамках роботи центру безпеки (SOC) одного підприємства, установи або організації.

Однак такі системи не розглядають визначення пріоритетів інцидентів або оцінку ризиків із загальнонаціональної точки зору, що може залучати велику кількість різноманітних підприємств. Великі національні операційні центри з КБ, як-от Агентство кібербезпеки та безпеки інфраструктури (CISA), повинні оцінювати ризики, вміщуючи різноманітну групу власників та операторів приватних критично важливих інфраструктурних об'єктів, а також відомств і агенцій уряду США.

Національна система оцінки кіберінцидентів (NCISS) розроблена, щоб забезпечити повторюваний і послідовний механізм для оцінки ризику інциденту в цьому контексті.

При цьому необхідно наголосити, що NCISS базується на Спеціальній публікації Національного інституту стандартів і технологій (NIST) 800-61 Rev. 2, Посібнику з обробки інцидентів з комп'ютерною безпекою, і розроблено для включення категорій потенційного впливу на конкретні суб'єкти, які дозволяють персоналу CISA оцінювати серйозність ризику та пріоритет інцидентів з загальнонаціональної точки зору. NCISS дозволяє подібному інциденту, який зазнали дві різні зацікавлені сторони, мати суттєво різну оцінку на основі потенційного впливу кожного постраждалого суб'єкта на національному рівні. Система не призначена для абсолютного оцінювання ризику, пов'язаного з інцидентом.

Так NCISS використовує середнє арифметичне зважене, щоб отримати оцінку від нуля до 100. Ця оцінка керує процесами сортування та ескалації інцидентів CISA і допомагає визначити пріоритетність обмежених ресурсів реагування на інциденти та необхідний рівень підтримки для кожного інциденту.

Наразі система не розроблена для підтримки випадків, коли кілька взаємопов'язаних інцидентів можуть збільшити загальний ризик, наприклад, кілька одночасних компромісів організацій у певному секторі чи регіоні.

Однак подібні події все ще можуть бути легко посилені за допомогою експертного втручання людини.

Вхідні дані для системи оцінювання є сумішшю дискретних та аналітичних оцінок. Хоча всі спроби звести до мінімуму індивідуальні упередження за допомогою тренувань і вправ, різні індивідуальні рахунки неминуче матимуть дещо різні погляди на свої відповіді на деякі запитання щодо оцінки.

Використання кількох дискретних вхідних даних, які можна перевірити, зменшує вплив будь-якого окремого аналітичного фактора, підвищуючи загальну надійність системи.

NCISS узгоджується зі схемою серйозності кіберінцидентів (CISS), щоб рівні серйозності в NCISS відображалися безпосередньо на рівнях CISS.

Виділення невирішених раніше частин загальної проблеми

За результатами опрацювання існуючої нормативно-правової бази держави, проєктів нормативних документів та технічних рішень щодо роботи центрів безпеки СЗК, які визначають пріоритети інцидентів або здійснюють оцінку ризиків із загальнонаціональної точки зору слід відмітити наступне.

Вперше Протокол спільних дій реагування на загрози кібербезпеці держави було підготовлено Адміністрацією ДССЗЗІ України на виконання вимог підпункту "г" підпункту 3 пункту 2 Рішення РНБО 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. Проектну назву Постанови Кабінету Міністрів України було запропоновано наступну – "Про затвердження Протоколу спільних дій основних СЗК, суб'єктів кіберзахисту та власників (розпорядників) ОКІІ під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків" [2].

Зазначеним Протоколом передбачалось міністерствам, іншим центральним органам виконавчої влади визначити (створити) підрозділи (команди, центри, групи), які забезпечуватимуть кіберзахист та реагування на кіберзагрози щодо ОКІІ у відповідній галузі або сфері діяльності та/або покласти функції з кіберзахисту на підрозділи із захисту інформації (Далі – ЗІ). Також, державним органам, органам місцевого самоврядування, органам управління

Збройними Силами, іншими військовими формуваннями утвореними відповідно до законів, правоохоронним органам, підприємствам, установам та організаціям, у власності чи розпорядженні яких є ОКІІ та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) таких об'єктів [7], пропонувалось організувати створення або створити на таких об'єктах підрозділи кіберзахисту та/або покласти функції з кіберзахисту на підрозділи із ЗІ.

Тож, на той час проєкт Протоколу носив лише загальний характер та встановлював лише перелік взаємно пов'язаних у часі та за цілями обов'язкові дії СЗК під час реагування на кіберінциденти та усунення їхніх наслідків.

При цьому, сам порядок (механізм) здійснення цих спільних дій, роль та місце кожного СЗК визначено не було, що надалі залишало на низькому рівні організацію взаємодії. Крім того, перелік обов'язкових дій СЗК, зазначених в проєкті Протоколу, був загальним та не відображав специфічних завдань та функцій цих СЗК.

Також, в проєкті Протоколу було визначено шість рівнів кіберзагроз, при цьому зазначалось, що заходи реагування на кіберінциденти на всіх етапах виконувались для кожного рівня кіберзагрози. Проте, ймовірніше всього, для кожного рівня кіберзагроз було необхідно здійснювати різні за складністю дії з реагування на кіберзагрози та кіберінциденти, а також ймовірніше всього вони повинні були носити різний ступінь залученості СЗК.

В зазначеному проєкті спільно розглядались функції та завдання Міністерства оборони України та Генерального штабу Збройних Сил України, хоча в положенні і інструкціях зазначених органів управління (органах військового управління) різне призначення, тому з метою уникнення дублювання зазначених функцій під час виконання дій в ході реагування на кіберінциденти та усунення їхніх наслідків, а також враховуючи, що ці функції і завдання є різними, пропонувалось завдання на кожному етапі реагування на кіберінциденти визначати окремо для Міністерства оборони України і окремо для Генерального штабу Збройних Сил України та Збройних Сил України.

Слід відмітити, що зміст проєкту Протоколу не відповідав його назві.

В проєкті Протоколу не було визначено перелік узгоджених за часом та завданнями спільних та взаємопов'язаних обов'язкових дій СЗК під час реагування на кіберінциденти. Були перелічені лише загальні завдання СЗК, визначені іншими нормативно-правовими документами.

Ще доволі суттєвою проблематикою було те, що внаслідок невдалого перекладу англійських назв етапів реагування на кіберінциденти частково втрачалась відповідність назв цих етапів їх змісту.

Тому, назву етапу реагування Containment, що перекладено як "стримування", в подальшому пропонується змінити на "локалізація" (змістом цього етапу є ізоляція уражених елементів об'єктів кіберзахисту з метою нерозповсюдження загрози); назву Eradication, що перекладено як "усунення наслідків", пропонується замінити на "усунення загрози" (так усунення наслідків кіберінцидента здійснюється у ході наступного етапу – "відновлення"). Також, з метою забезпечення взаємосумісності та взаємодії з підрозділами КБ Європейського союзу та НАТО пропонується вказати англійські варіанти назв етапів реагування на кіберінциденти відповідно до NIST Special Publication 800-61.

Для вирішення завдань, щодо врегулювання та імплементації норм та правил міжнародних організацій сфери КБ та КО пропонується дати визначення термінам "критичні інформаційні активи" та "критичні інциденти безпеки", які наведені у пункті проєкту Протоколу, вираз "є інформацією з обмеженим доступом" замінити виразом "розповсюджується відповідно до Загальних правил обміну інформацією про кіберінциденти (Протокол TLP), схвалених рішенням НКЦК при РНБО України (пункт 3.1 Протоколу № 18 від 25.10.2021)", додати: "забезпечення обізнаності користувачів з базових питань кібербезпеки" та "проведення кібернавчань".

Проаналізувавши чинні положення (аксіоматики) існуючої законодавчої, державної та відомчої нормативно-правової бази, а також нормативно-правового поля міжнародних організацій пропонується об'єднати та викласти в редакції нового Проєкту заходи по розробленню детального плану та стандартних операційних процедур реагування на кіберінциденти.

Апробацію зазначеного плану провести під час проведення заходів колективної підготовки СЗК держави та, за необхідності, внести відповідні коригування до них.

Враховуючи неоднозначне тлумачення визначення рівнів кіберзагрози пропонується розглянути можливість визначення рівнів кіберзагрози за моделлю NCISS – National Cyber Incident Scoring System (США), опис якої доступний за посиланням: https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System.

Розглядаючи порядок інформування СЗК, який виявив факт проведення протиправних дій в кіберпросторі, інших СЗК, пропонується таке інформування здійснювати через одного із "ключових" суб'єктів НсКБ, наприклад через НКЦК при РНБО України або ДССЗЗІ України. Крім того, вважається недоцільним інформувати всіх без виключення СЗК, вказаних в проєкті Протоколу.

Також пропонується визначити ступені критичності тих кіберінцидентів, про які СЗК інформуються негайно.

В додатках зазначеного проєкту Протоколу пропонується навести завдання НКЦК при РНБО України. Також для кожного з етапів реагування на кіберінциденти з урахуванням рівнів кіберзагроз пропонується розробити алгоритми виконання конкретних практичних спільних дій СЗК під час реагування на кіберінцинденти, а також при усуненні їхніх наслідків. Інформацію, яка наведена у додатку до проєкту Протоколу "Додаткові завдання окремих

суб'єктів взаємодії на кожному етапі реагування на кіберінциденти" пропонується використати для розробки зазначених алгоритмів.

В цілому, вивчаючи проєкт документа слід зауважити, що Протокол встановлює лише "перелік взаємно пов'язаних у часі та за цілями обов'язкових дій СЗК під час реагування на кіберінциденти та усунення їхніх наслідків".

Проте сам порядок (механізм) здійснення цих спільних дій, роль та місце кожного СЗК не визначено, що надалі залишає на низькому рівні організацію взаємодії.

Крім того, перелік обов'язкових дій СЗК, зазначених в проєкті Протоколу, є загальним та не відображає специфічних завдань та функцій цих СЗК.

Виходячи із викладеного, пропонується доопрацювати проєкт Протоколу в частині визначення не тільки переліку, але й порядку (механізму) спільних дій СЗК під час реагування на кіберінциденти та усунення їхніх наслідків, із врахуванням специфічних завдань та функцій цих СЗК.

Формулювання цілей статті (постановка завдання)

В даній статті проаналізовано особливості взаємодії основних суб'єктів НсКБ в умовах:

особливого періоду,

правового режиму воєнного та надзвичайного стану,

здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії,

проведення операції об'єднаних сил (антитерористичної операції).

За результатами опрацьованого аналізу, запропоновано перелік взаємно пов'язаних у часі та узгоджених за алгоритмами обов'язкових дій СЗК під час реагування на кіберінциденти та усунення їх наслідків, проведення превентивних наступальних дій (операцій) у кіберпросторі з врахуванням дефініцій та визначень які встановлені спільними міжвідомчими наказами основних суб'єктів НсКБ.

Виклад основного матеріалу дослідження

В рамках виконання вимог плану оборони України, введеного в дію Указом Президента України від 24 лютого 2022 року № 70/2022 "Про рішення Ради національної безпеки і оборони України від 24 лютого 2022 року "Про введення в дію плану оборони України та Зведеного плану територіальної оборони України", та вимог Закону України "Про основні засади забезпечення кібербезпеки України" в частині відбиття воєнної агресії у кіберпросторі (КО) та впровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури СЗК під час реагування на кіберінциденти [3], а також при усуненні їхніх наслідків вважається за потрібне:

1. Уточнити склад СЗК щодо виконання дій, встановлених зазначеним вище документом та визначити основних суб'єктів НсКБ і сил кіберзахисту з метою виконання їх спільних дій під час реагування на кіберінциденти, а також при усуненні їхніх наслідків.

В подальшому пропонується віднести до основних суб'єктів НсКБ наступні елементи:

сили безпеки і оборони, сили кіберзахисту, НКЦК, як робочий орган РНБО України;

центральні органи виконавчої влади, інші державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, або безпосередньо проводять відповідно до компетенції заходи із забезпечення КБ;

місцеві органи виконавчої влади, органи місцевого самоврядування, що провадять діяльність у сфері ЗІ та кіберзахисту;

ОКІ незалежно від форми власності; підприємства, установи та організації незалежно від форми власності, що провадять діяльність у сфері ЗІ та кіберзахисту, взаємодіють із силами кіберзахисту або виконують роботи та надають послуги за державні кошти [4].

В умовах правового режиму воєнного стану цей перелік може бути змінений Генеральним штабом Збройних Сил України.

2. Використовувати наступні терміни та визначення у новій редакції Протоколу, а саме:

сили кіберзахисту – урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, інші команди реагування на комп'ютерні надзвичайні події, підрозділи (групи, команда, служби) ЗІ, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов'язані з кіберзахистом [6];

рівень кіберзагрози – показник небезпеки від потенційного або незворотнього настання кіберінциденту, що може спричинити значні руйнівні для критичної інформаційної інфраструктури країни наслідки;

Інші терміни вживати у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про національну безпеку України", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні комунікації".

3. Встановити такі етапи реагування на кіберінциденти: підготовка; виявлення та аналіз; стримування; усунення; відновлення; заходи після інциденту.

При цьому етап підготовки спрямований на забезпечення готовності реагування на кіберінциденти, а також запобігання їм, і передбачає виконання таких заходів:

розробка та оновлення політик безпеки;

затвердження детального плану реагування на кіберінциденти, перевірка використання його та, за необхідністю внесення коригувань до нього, оцінка ризиків;

визначення критичних інформаційних активів, визначення критичних інцидентів безпеки; створення, перевірка, проведення навчань;

створення/або визначення команди реагування на інциденти CSIRT/CIRT/CERT, порядку комунікації з правоохоронними органами, CERT-UA.

Етап виявлення та аналізу передбачає виявлення подій, які можуть спричинити виникненню інциденту, узагальнення інформації щодо них та наявності вразливостей, і передбачає такі заходи:

забезпечується постійний контроль та моніторинг ІТ-систем;

здійснюється виявлення аномалій, виявлення та аналіз, а також підтвердження інцидентів безпеки;

при виявленні інциденту, виконується початковий аналіз його з метою визначення масштабності, причини виникнення і яким чином відбувається інцидент (інструменти або методи, які використовувалися для атаки, якими вразливими місцями скористалися);

відбувається збір додаткових даних з різних джерел, їх дослідження, встановлення типу інциденту, згідно Переліку категорій кіберінцидентів і рівня його критичності;

при аналізі виникнення інциденту команда суб'єкта взаємодії отримує достатньо інформації для визначення наступних заходів, як стримування, усунення та відновлення;

всі зібрані дані документуються, а команда суб'єкта взаємодії інформує про кіберінцидент відповідно до класифікації (таксономії) кіберінцидентів та протоколу обміну інформацією про кіберінциденти.

Етап стримування спрямований на забезпечення розроблення суб'єктами взаємодії цілеспрямованої стратегії її відновлення, а також призначення та реалізацію першочергових заходів стримування для запобігання поширенню загрози.

При здійсненні довгострокового стримування відбувається внесення тимчасових виправлень до систем задля можливості їх застосування до завершення налаштування систем (їх елементів), які відтворені з їх неуражених копій.

Етап усунення наслідку кіберінциденту спрямований на реалізацію заходів з видалення шкідливого програмного забезпечення з усих уражених систем, усунення наслідків впливу інциденту, визначення першопричин іициденту та вжиття заходів для запобігання атакам подібного типу у майбутньому.

Етап відновлення передбачає реалізацію суб'єктом взаємодії заходів з відновлення системи до штатного режиму функціонування та переконання в її стабільному функціонуванні, що передбачає:

підключення раніше ізольованих уражених сегментів після відновлення до основної системи;

вжиття заходів із запобігання додатковим атакам;

тестування, перевірка та контроль відновлених після ураження систем для їх повернення до штатного функціонування з урахуванням встановленого часу для відновлення.

Етап заходів: після інциденту передбачає:

аналіз отриманого досвіду інциденту після його закінчення, проведення навчань та зустрічей з метою обміну досвідом;

перегляд та внесення змін до політик безпеки та документації за результатами дослідження інциденту;

оцінку дій щодо реагування на інцидент з метою покращення процесів реагування на кіберінциденти у майбутньому.

4. В залежності від рівня критичності кіберінцидентів для прийняття рішення щодо впровадження додаткових заходів кіберзахисту встановлюються такі рівні кіберзагроз:

базовий ("білий"),

низький ("зелений"),

середній ("жовтий"),

високий ("помаранчевий"),

серйозний ("червоний"),

надзвичайний ("чорний").

Базовий ("білий") рівень вказує на:

нульовий рівень загроз від настання кіберінцидентів,

наявність несуттєвих подій,

стале функціонування ОКІІ держави.

Низький ("зелений") рівень вказує на низький стан загроз, динаміка критичності якого залежить від настання критичності кіберінцидентів. Не існує жодної незвичайної активності, окрім звичайного занепокоєння про відомі хакерські дії, віруси та іншу зловмисну діяльність.

Середній ("жовтий") рівень вказує на середній рівень загроз від настання кіберінцидентів, при якому спостерігається збільшення хакерських дій, вірусів або іншої зловмисної діяльності.

Існує потенціал для кіберзловмисної діяльності, але виявлена невідома раніше або відома така діяльністъ, але значного впливу на системи не відбулося.

Високий "помаранчевий" рівень вказує на високий рівень загроз від настання кіберінцидентів через зростаючі хакерські дії, віруси або іншу зловмисну діяльністъ, яка компрометує системи або звужує надання послуг.

На цьому рівні існують відомі вразливості, які використовуються з помірним ступенем пошкодження чи порушення або потенціал для значного порушення системи є високим.

Серйозний "червоний" рівень вказує на серйозний рівень загроз від настання кіберінцидентів через зростання хакерських дій, вірусів або іншої зловмисної діяльності, які націлені або компрометують основну інфраструктуру, спричиняють різноманітні перебої надання послуг, різноманітні компрометації систем або ОКІ.

На цьому рівні використовуються вразливості із небезпечним ступенем і поширеним рівнем пошкодження, або порушення чи потенціал для серйозного порушення є високим.

Надзвичайний "чорний" рівень вказує на найвищий рівень загроз від настання кіберінцидентів через зростання хакерських дій, вірусів або іншої зловмисної діяльності, внаслідок яких дуже поширюються перебої і/або значна деструктивна компрометація систем невідомими засобами або послаблюється один чи більше секторів КІ.

На цьому рівні використовуються вразливості із небезпечним ступенем або поширеним рівнем пошкодження чи порушення ОКІ.

5. Заходи етапів реагування на кіберінциденти виконуються для кожного рівня кіберзагрози.

У випадку отримання випереджувальної інформації про підготовку та безпосередню загрозу проведення кібератак проти ОКІІ держави з метою випереджувального реагування, нарощування готовності відповідних сил та засобів рішення про введення необхідних етапів реагування на кіберінциденти приймається НКЦК.

У випадку раптового початку проведення кібератак проти ОКІІ держави рішення про введення відповідних етапів реагування на кіберінциденти приймаються керівництвом суб'єкта забезпечення КБ, силами та засобами якого виявлено факти проведення зазначених протиправних дій в кіберпросторі (кібератак, кіберінцидентів тощо), про що невідкладно інформуються інші СЗК.

Інформація про конкретний ОКІ, щодо якого стався кіберінцидент, є інформацією з обмеженим доступом.

Враховуючи зазначене, є необхідним визначити додаткові завдання окремих суб'єктів взаємодії на кожному етапі реагування на кіберінциденти, а саме.

Під час Етапу 1 (підготовка):

1). ДССЗЗІ України:

координує діяльність інших суб'єктів взаємодії щодо кіберзахисту;

здійснює оцінку стану захищеності державних інформаційних ресурсів в інформаційно-комунікаційних 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 держав) цих 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 практично 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 СЗК 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 (КО) [11], координують діяльність державних органів та органів місцевого самоврядування щодо підготовки та ведення КО;

отримують від основних СЗК та узагальнюють інформацію щодо ОКІІ воєнної сфери та сфери оборони держави;

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

підтримують сили та засоби для дій в кі0ерпросторі 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 КО;

здійснюють підготовку та застосування Збройних Сил України 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 КО, створення та розвиток відповідних організаційних структур, їх комплектування, підготовку та всебічні: 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 КБ;

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

подають ДССЗЗІ України встановленим порядком розвідувальну інформацію про технічні розвідки іноземних держав, які діють у кіберпросторі.

4). СБ України:

здійснює відповідно до законодавства контрозвідувальну діяльність із запобігання розвідувально-підривним терористичним та іншим посяганням на КБ України;

інформує основних СЗК 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 КБ держави;

негласно перевіряє готовність ОКІ до масованих кібератак та кіберінцидентів та інформує ДССЗЗІ України про виявлені у процесі контррозвідувальної діяльності вразливості, що становлять загрозу безпеці ОКІІ;

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

5). Національна поліція України:

інформує основних СЗК про організацію, сили, засоби, методи, тактику дій злочинних угруповань, 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 КБ ОКІ, а також роз'яснювальну роботу серед всіх верств населення;

повідомляє основних СЗК про виявлені у процесі оперативно-розшукової діяльності вразливості, що становлять загрозу безпеці ОКІІ;

інформує суб'єктів/операторів критичної інформаційної інфраструктури про виявлені у процесі оперативно-розшукової діяльності посягання на безпеку їхніх інформаційних, комунікаційних та інформаційно- комунікаційних систем, умови, що сприяють реалізації кіберзагроз, можливі причини виникнення таких умов та шляхи їхнього усунення.

6). Сили кіберзахисту:

з урахуванням інформації, отриманої від основних СЗК 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 виявления кіберінцидентів.

7). Власники та/або керівники ОКІ:

проводять оцінку поточного стану ЗІ та кіберзахисту ОКІІ (прогнозування виникнення нових кіберзагроз, їх врахування в моделі загроз, визначення необхідності її коригування тощо), розраховують ризики КБ;

на підставі аналізу розрахованих ризиків КБ здійснюють практичні заходи щодо забезпечення ЗІ та кіберзахисту ОКІІ з урахуванням інформації, отриманої від основних СЗК та/або суб'єктів кіберзахисту [9];

здійснюють моніторинг, реєстрацію та аудит подій на ОКІІ;

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 ЗІ відповідно до визначеної політики безпеки;

розробляють плани відновлення сталого функціонування своїх ОКІІ з розрахованим цільовим часом відновлення, у разі порушення його функціонування внаслідок реалізації кібератаки;

надають на запит ДССЗЗІ України необхідну інформацію про реалізовані заходи щодо кіберзахисту ОКІІ.

Під час Етапу 2 (виявлення та аналіз):

1). ДССЗЗІ України:

координує діяльність інших суб'єктів взаємодії щодо вжиття необхідних заходів з кіберзахисту з урахування виявлених кіберзагроз щодо ОКІІ;

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

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

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

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

здійснюють з основними суб'єктами забезпечення КБ підготовку та проведення заходів щодо КО;

вживають заходів щодо КО (активного кіберзахисту);

інформують ДССЗЗІ України, CERT-UA, СБ України, Національну поліцію України, розвідувальні органи України та інших СЗК про ймовірні об'єкти та джерело кібератаки.

3). СБ України:

виявляє спеціальними методами та засобами кібератаки на ОКІІ, 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 ДССЗЗІ України 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 України:

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 ОКІІ.

5). Сили кіберзахисту:

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

здійснюють блокування джерел кібератак та кіберінцидентів;

інформують ДССЗЗІ України, СБ України та Національну поліцію України 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 їх наслідки.

6). Власники та/або керівники ОКІ:

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 інформаційно-комунікаційних систем з метою мінімізації наслідків;

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

Під час Етапу 3 (стримування):

1). ДССЗЗІ України:

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). Власники та або керівники ОКІ:

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

забезпечують своєчасне та безперешкодне ознайомлення представників Національної поліції та СБ України з виявленими слідами протиправної діяльності в кіберпросторі для їх оперативного аналізу.

Під час Етапу 4 (усунення):

1). ДССЗЗІ України:

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 ОКІІ та усунення наслідків кібератак і кіберінцидентів;

вивчає спільно з Національною поліцією та СБ України 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). СБ України:

вивчає спільно з ДССЗЗІ України та Національною поліцією України 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.

4). Сили кіберзахисту:

здійснюють, з урахуванням інформації отриманої від ДССЗЗІ України та СБ України, практичні заходи з кіберзахисту ОКІІ 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 ДССЗЗІ України, а також міжнародну взаємодію з командами реагування інших країн (CERT, CSIRT, MCSIRT) щодо припинення (блокування) кібератак (кіберінцидентів) та усунення їхніх наслідків.

5). Власники та/або керівники ОКІ:

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

Під час Етапу 5 (відновлення):

1). ДССЗЗІ України:

координує діяльність інших суб'єктів взаємодії щодо кіберзахисту під час відновлення сталого функціонування ОКІІ.

2). СБ України:

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 підготовки або скоєння;

негласно оцінює стан готовності ОКІ до реагування на кібератаки та кіберінциденти.

3). Національна поліція України:

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

вивчає спільно з ДССЗЗІ України та СБ України 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.

4). Власники та/або керівники ОКІ:

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

забезпечують, у разі необхідності, фізичний доступ представників ДССЗЗІ України, суб'єктів кіберзахисту (відповідно до підпорядкованості) до інформаційно-комунікаційних систем для виконання заходів щодо блокування та локалізації негативних наслідків кібератак (кіберінцидентів) та відновлення сталого функціонування цих систем.

Під час Етапу 6 (заходи після інциденту):

1). ДССЗЗІ України:

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 субє'ктами 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 КО;

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 СЗК з питань ЗІ, кіберзахисту, КБ та КО.

3). СБ України:

надає ДССЗЗІ України підготовлену на основі оперативних матеріалів узагальнену інформацію щодо фактичної готовності ОКІІ до можливих кібератак (кіберінцидентів), а також обґрунтовані пропозиції щодо її поліпшення;

надає ДССЗЗІ України прогностичну інформацію щодо можливих в подальшому кібератак та кіберінцидентів, а також рекомендації щодо заходів кіберзахисту.

4). Національна поліція України:

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 ДССЗЗІ України 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). Власники та/або керівники ОКІ: здійснюють збір, узагальнення та аналіз інформації про кібератаки (кіберінциденти) та подають її до ДССЗЗІ України та суб'єктам кіберзахисту (відповідно до підпорядкованості);

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

6. Методичні рекомендації щодо змісту заходів за етапами реагування на кіберінциденти, типи (таксономію) кіберінцидентів, загальні правила обміну інформацією про кіберінциденти затверджує Адміністрація ДССЗЗІ України.

Висновки з даного дослідження і перспективи подальших досліджень у даному напрямку

Отже за результатами проведеної роботи в даній публікації були досліджені передумови і особливості формування законодавства України у сфері КБ, визначені проблеми та перспективи його подальшого розвитку з точки зору оцінки наявних небезпек та загроз. Визначені напрями адаптації чинного законодавства про КБ до стандартів ЄС у межах реалізації положень Угоди про асоціацію між Україною та ЄС та представлено рекомендації, щодо попередження, виявлення та порядку реагування на існуючі загрози національному сегменту кіберпростору держави.

Також були визначені найбільш перспективні напрями розвитку національної системи кіберзахисту, а саме вдосконалення правової основи кіберзахисту ОКІ; впровадження системи незалежного аудиту інформаційної безпеки на ОКІ; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення КБ в яких держава повинна відігравати сервісну роль.

Список літератури

1. Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242: Указ Президента України №27/2020 від 28 січ. 2020 р. URL: https://www.president.gov.ua/documents/272020-32041.

2. Президент увів у дію рішення РНБО про захист від кібератак, 2017 р. URL: https://www.ukrinform.ua/rubric-polytics/2296115-prezident-uviv-u-diu-risenna-rnbo-pro-zahist-vid-kiberatak.html.
3. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК, 28 вер. 2022 р. URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html.
4. Про критичну інфраструктуру: закон України док. 1882-IX, від 16 листоп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
5. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету міністрів України від 10 березня 2017 р. № 155-р. URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80#Text.
6. Грабовий А. М. Закон про кібербезпеку та стратегія кібербезпеки України. Онлайн-видання Юрист&Закон. 2022. №28. URL: https://uz.ligazakon.ua/ua/magazine_article/EA010553.
7. Онищук І.І. Особливості бюджетного процесу в умовах воєнного стану. Пресцентр ініціативи "Децентралізація". 2022. URL: https://decentralization.gov.ua/news/14654.
8. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету міністрів України від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text.
9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України №96/2016р. ред. від 28 серпня 2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html.
10. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України: Постанова правління Національного банку України від 12 серпня 2022 р. № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text.
11. Тютюнік В., Горовенко В. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. Оборонно-промисловий кур'єр. 01 листопада 2021 р. URL: https://opk.com.ua/%D0%B2%D1%81%D0%B5%D0%BE%D1%85%D0%BE%D0%BF%D0%BB%D1%8E%D1%8E%D1%87%D0%B0-%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D1%80/.
12. Онлайн-шахрайство з використанням тематики "допомоги від Червоного Хреста" (CERT-UA#5063): CERT-UA Державної служби спеціального зв'язку та захисту інформації України. 27 липня 2022 р. URL: https://cert.gov.ua/article/987552.

Received (Надійшла) 20.11.2023
Accepted for publication (Прийнята до друку) 31.01.2024

Protocol of general actions of cyber security subjects during response to cyber incidents, as well as in the elimination of their consequences

Y. Zhyvylo, I. Romashko

Abstract. Cyberspace, along with other physical spaces, is recognized as one of the theaters of war. The tendency to create cyber troops is gaining momentum (Roadmap for the creation of Cyber Troops of the Armed Forces of Ukraine - Order of the General Staff of the Armed Forces of Ukraine, dated April 22, 2022 No. 48), whose tasks include not only ensuring the protection of the state's critical information infrastructure from cyber attacks, but also conducting preventive offensive (carrying out cyber operations) in cyberspace, including the disabling of critical infrastructure facilities of the enemy by destroying the information systems that manage such facilities. An increase in the intensity of interstate confrontation and reconnaissance and subversive activities in cyberspace is predicted. The circle of states that are trying to form their own cyber intelligence, to master modern technologies of reconnaissance and explosive activities in cyberspace is expanding, and they are strengthening state control over national segments of the Internet. Taking into account the experience of conducting hostilities during the introduction of the legal regime of martial law and given the uncertainty of subjects and objects, their functions and tasks for actions in certain areas, including in the field of cybersecurity, in peacetime led to adversity and inconsistency of these actions by the subjects of support state cybersecurity. And given that with the introduction of the legal regime of martial law, certain entities change their location, move information assets and equipment to new locations using cloud services, which greatly complicates the process of harmonization and coordination of actions to respond to cyber incidents, as well as elimination of consequences. This leads to a forced redistribution of tasks and functions for the implementation of cyber defense measures at various facilities. Under these conditions, new subjects of cyber defense are created on a permanent or temporary basis, which requires time for them to acquire the abilities to perform their intended tasks. In such a situation, Ukraine should be able to ensure its socio-economic development in the digital world, which requires the acquisition of the ability to effectively deter destructive actions in cyberspace, a sustainable response to threats in cyberspace, the achievement of cyber resilience at all levels, and the interaction of the components of the security and defense sectors to ensure cybersecurity within the cyber defense of the state. So, based on the need for a scientific justification of the institutional framework, it is necessary to clearly define: "a list of subjects for ensuring cybersecurity for the implementation of the actions established by this Protocol", both in peacetime and under the legal regime of martial law; the above subjects, their role and place, the list and procedure for responding to cyber incidents and eliminating their consequences, both in peacetime and under the legal regime of martial law. At the same time, the scientific novelty of the expected results lies in the theoretical substantiation and provision of practical recommendations for improving the mechanisms for managing and interacting with the components of the security and defense sector when planning the state's preparation for cyber defense, taking measures to neutralize and actively counter cyber threats in the national segment of the state's cyberspace.

Keywords: cybersecurity subjects, cyberspace, cyber defense, active cyber actions, destructive cyber attacks, critical information infrastructure.