НАЦІОНАЛЬНЕ АГЕНТСТВО УКРАЇНИ
З ПИТАНЬ ДЕРЖАВНОЇ СЛУЖБИ

Н А К А З

від _____ 20___ р. Київ №_____

Про затвердження адміністративного регламенту процесу «Кіберзахист інформаційно-комунікаційних систем Національного агентства України з питань державної служби»

Відповідно до абзацу другого частини третьої статті 26 Бюджетного кодексу України, пункту 9 Положення про Національне агентство України з питань державної служби, затвердженого постановою Кабінету Міністрів України від 01 жовтня 2014 року № 500, наказу НАДС від 05 лютого 2024 року № 15-24 «Деякі питання удосконалення внутрішнього контролю в апараті Національного агентства України з питань державної служби, його територіальних органах, на підприємствах, установах та організаціях, що належать до сфери його управління»

НАКАЗУЮ:

1. Затвердити адміністративний регламент процесу «Кіберзахист інформаційно-комунікаційних систем Національного агентства України з питань державної служби», що додається.

2. Контроль за виконанням цього наказу залишаю за собою.

Голова **Наталія АЛЮШИНА**

ЗАТВЕРДЖЕНО

Наказ Національного агентства України

з питань державної служби

_____ 2024 року № _____

Адміністративний регламент процесу «Кіберзахист інформаційно-комунікаційних систем Національного агентства України з питань державної служби»

Забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Формування нової якості національної системи кібербезпеки потребує забезпечення надійного кіберзахисту як необхідної складової для досягнення стратегічної цілі щодо набуття кіберстійкості в умовах воєнної агресії російської федерації проти України.

Для суб'єктів забезпечення кібербезпеки вкрай важливим постає питання посилення спроможностей захисту власної інформаційно-комунікаційної інфраструктури від кіберзагроз та кібератак.

Система заходів кіберзахисту базується на нормативно-правових актах, нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, які розвиваються разом з технологіями забезпечення кібербезпеки.

Цей адміністративний регламент процесу «Кіберзахист інформаційно-комунікаційних систем Національного агентства України з питань державної служби» (далі – процес кіберзахисту ІКС НАДС) розроблено з метою детальної регламентації діяльності СЗІ спільно з ГД, іншими структурними підрозділами апарату НАДС, належного документування процедур, пов'язаних з кіберзахистом та мінімізації кіберзагроз.

Адміністративний регламент процесу кіберзахисту ІКС НАДС складається з наступних розділів:

I. Основні поняття.

II. Блок-схема процесу кіберзахисту ІКС НАДС.

III. Короткий опис операцій, які використовуються в процесі кіберзахисту ІКС НАДС.

IV. Технологічна карта процесу кіберзахисту ІКС НАДС.

V. Перелік прийнятих скорочень.

Розділ І. Основні поняття

1.1. Визначення цілей

Стратегічною метою процесу кіберзахисту ІКС НАДС є забезпечення стійкого, надійного, безперервного функціонування інформаційно-комунікаційних систем шляхом впровадження заходів кіберзахисту, протидії кіберзагрозам та кібератакам.

Кіберзахист визначається як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування ІКС.

Об'єктом кіберзахисту виступає ІКС, в якій обробляються ДІР НАДС.

Заходи з кіберзахисту ІКС та реагування на КІ/КА в НАДС вживаються для забезпечення:

швидкого виявлення КІ/КА;

належного інформування про їх виникнення уповноважених органів;

запобігання, мінімізації та усунення негативних наслідків;

виявлення вразливостей;

відновлення функціонування ІКС;

унеможливлення повторної реалізації виявленого КІ, а щодо КА – збереження можливих електронних доказів.

Кіберзахист ІКС та реагування на КІ/КА в НАДС здійснюється послідовно наступними етапами:

1. Підготовка з кіберзахисту.
2. Виявлення, аналіз та комунікація.
3. Стримування та комунікація.
4. Усунення та комунікація.
5. Відновлення та комунікація.
6. Аналіз ефективності заходів з реагування на КІ/КА.

Показниками досягнення визначеної мети процесу кіберзахисту ІКС НАДС є:

характеристика ІКС;

розроблення переліку заходів кіберзахисту;

ефективне адміністрування кіберзахистом;

опис кожного етапу процесу кіберзахисту;

визначення відповідальних і виконавців кожного етапу кіберзахисту.

1.2. Учасники процесу кіберзахисту ІКС НАДС

1.2.1. Внутрішні учасники:

Голова НАДС або особа, яка виконує його обов’язки; заступник Голови НАДС відповідно до розподілу обов’язків; ГД, УП, СЗІ, інші структурні підрозділи апарату НАДС.

Підприємства, установи і організації, що належать до сфери управління НАДС та його територіальні органи.

1.2.2. Зовнішні учасники:

НКЦК, СБУ, ГШ ЗСУ, ДЦКЗ, CERT-UA, правоохоронні органи, інші ОДВ, визначені законодавством як основні суб'єкти національної системи кібербезпеки (уповноважені органи).

Підприємства, установи, організації, які провадять діяльність з технічного захисту інформації у відповідності до дозволів та ліцензій.

Постачальники електронних комунікаційних мереж та/або послуг, охоронних послуг, розробники інформаційних систем тощо.

1.3. Нормативно-правові акти, які регламентують виконання процесу кіберзахисту ІКС НАДС

№ з/п	Нормативно-правові акти
1.	Закон України «Про основні засади забезпечення кібербезпеки України»
2.	Закон України «Про захист інформації в інформаційно-комунікаційних системах»
3.	Постанова КМУ від 23 грудня 2020 р. № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»
4.	Постанова КМУ від 4 квітня 2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»
5.	Постанова КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»
6.	Постанова КМУ від 01 жовтня 2014 р. № 500 «Про затвердження Положення про Національне агентство України з питань державної служби»
7.	Постанова КМУ від 16 листопада 2002 р. № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах»

№ з/п	Нормативно-правові акти
8.	Постанова КМУ від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»
9.	Постанова КМУ від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»
10.	Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 р. № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури»
11.	Наказ Адміністрації Держспецзв'язку від 03 липня 2023 р. № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»
12.	Наказ Адміністрації Держспецзв'язку від 24 червня 2022 р. № 284, зареєстрованого в Міністерстві юстиції України 11 липня 2022 р. за № 758/38094 «Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об'єктів кіберзахисту»
13.	Наказ НАДС від 28 серпня 2021 р. № 139-21 «Деякі питання реагування на інциденти інформаційної безпеки в інформаційно-телекомунікаційних системах НАДС»
14.	НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53, із змінами, згідно з наказом Адміністрації Держспецзв'язку від 28 грудня 2012 р. № 806

1.4. Документообіг

№ з/п	Документ	Нормативно-правовий акт	Посилання та положення нормативно-правового акта
1.	Окреме доручення Голови НАДС	Положення про Національне агентство України з питань державної служби, затверджене постановою КМУ від 01 жовтня 2014 р. № 500	підпункт 22 пункту 11
2.	Інформування Голови НАДС (доповідна записка)	Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджений постановою КМУ від 04 квітня 2023 р. № 299	пункт 10
3.	Перелік інформаційних активів, систем та мереж (протокол інвентаризаційної комісії тощо)	Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою КМУ від 19 червня 2019 р. № 518	пункт 3 Додатку
		Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03 липня 2023 р. № 570	пункт 3 розділу II
		НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53	пункт 3.1 Додатку
4.	Функціональні повноваження СЗІ та обов'язки персоналу	Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою КМУ від 19 червня 2019 р. № 518	пункти 1, 2 Додатку

№ з/п	Документ	Нормативно-правовий акт	Посилання та положення нормативно-правового акта
	(Положення про СЗІ, посадові інструкції)	Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою КМУ від 29 березня 2006 р. № 373	пункт 18
		НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53	пункти 6.3, 11.6 Додатку
5.	ТД на систему	Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою КМУ від 19 червня 2019 р. № 518	пункт 6 Додатку
6.	Політики безпеки	Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою КМУ від 23 грудня 2020 р. № 1295	пункт 2
		Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою КМУ від 19 червня 2019 р. № 518	пункт 7
		Методичні рекомендації щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації	пункт 4 розділу II, пункт 1 Додатку 5

№ з/п	Документ	Нормативно-правовий акт	Посилання та положення нормативно-правового акта
		Держспецзв'язку від 03 липня 2023 р. № 570	
		НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53	пункти 5.1-5.4 розділу 5
7.	План захисту інформації в системі	Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою КМУ від 29 березня 2006 р. № 373	пункт 19
		НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53	абзац другий пункту 6.5, Додаток
8.	План реагування на КІ/КА	Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03 липня 2023 р. № 570	пункт 4 розділу II
9.	Меморандум про організацію взаємодії між НАДС та ДЦКЗ	Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою КМУ	підпункт 3 пункту 8, пункти 12, 13

№ з/п	Документ	Нормативно-правовий акт	Посилання та положення нормативно-правового акта
	(договір про надання послуг)	від 23 грудня 2020 р. № 1295	
		Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03 липня 2023 р. № 570	пункт 9 розділу I
10.	Листи-повідомлення НАДС	Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах, затверджений постановою КМУ від 16 листопада 2002 р. № 1772	пункт 3
		Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою КМУ від 23 грудня 2020 р. № 1295	абзац третій підпункту 3 пункту 8
11.	Повідомлення про КІ/КА Інформування Голови НАДС (доповідна записка)	Порядок реагування на інциденти інформаційної безпеки в Національному агентстві України з питань державної служби, його територіальних органах, а також підприємствах, установах і організаціях, що належать до сфери його управління, затверджений наказом НАДС від 28 серпня 2021 р. № 139-21	Пункти 8, 9, 14
		Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03 липня 2023 р. № 570	пункт 6 розділу III

№ з/п	Документ	Нормативно-правовий акт	Посилання та положення нормативно-правового акта
12.	Індивідуальна програма професійного розвитку та навчання персоналу, відповідального за забезпечення кіберзахисту ІКС	Порядок проведення оцінювання результатів службової діяльності державних службовців, затверджений постановою КМУ від 23 серпня 2017 р. № 640	пункт 12^1
		НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53	пункт 8.3
13.	Сертифікат (документ, який підтверджує результат навчання персоналу, відповідального за забезпечення кіберзахисту ІКС	Положення про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад, затверджене постановою КМУ від 06 лютого 2019 р. № 106	пункт 16

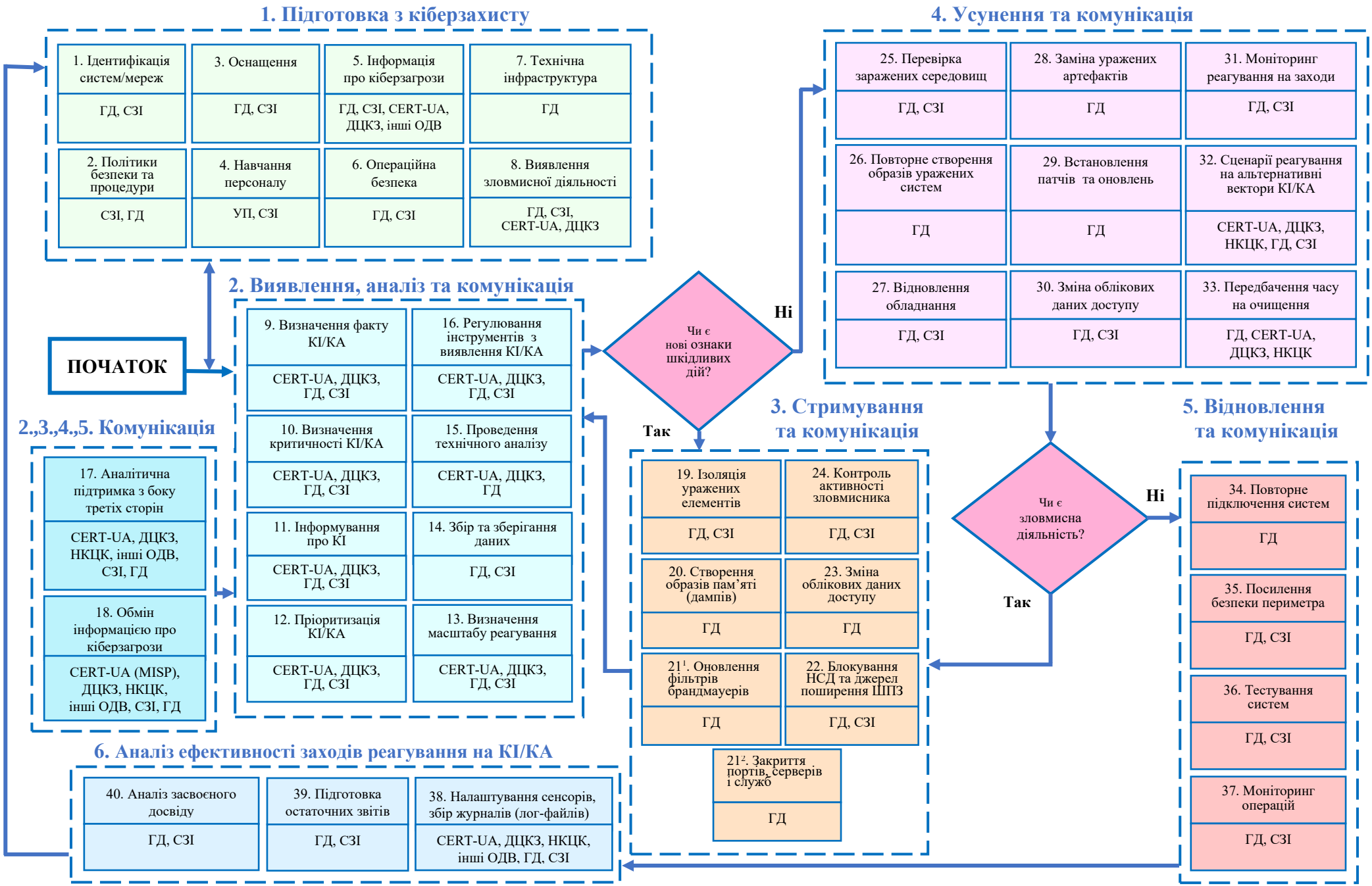
1.5. Прикладне програмне забезпечення

Прикладне програмне забезпечення складається з:

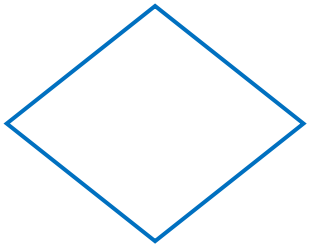
1.5.1. Програмного забезпечення ІКС НАДС: Інформаційна система управління людськими ресурсами та нарахування заробітної плати (HRMIS); Веб-портал Національного агентства України з питань державної служби «Портал управління знаннями»; Веб-портал вакансій CAREER.GOV.UA «Єдиний портал вакансій державної служби»; Система електронного документообігу та автоматизації бізнес-процесів «Мегаполіс.DocNet» тощо;

1.5.2. Програмного забезпечення систем протидії кіберзагрозам: Система виявлення вторгнень (IDS); Система захисту кінцевих точок (хостів) CrowdStrike; антивірусний захист ESET Endpoint Antivirus; мережеві екрани Cisco (фаєрволи) тощо.

Розділ ІІ. Блок-схема процесу кіберзахисту ІКС НАДС



Умовні позначення до блок-схеми

№ з/п	Абревіатура	Розшифровка
1.		Подія, яка є обов’язковою для виконання
2.		Комплекс подій, які обов’язкові для виконання
3.		Послідовність подій, які є обов’язковими для виконання
4.		Умова виконання події для більш повної деталізації етапів процесу

Розділ ІІІ. Короткий опис операцій, які використовуються в процесі кіберзахисту ІКС НАДС

3.1. Процес кіберзахисту та реагування на КІ/КА в системі НАДС здійснюється послідовно наступними етапами:

3.1.1. Підготовка з кіберзахисту

Заходи кіберзахисту з підготовки спрямовані на вивчення, дослідження сучасних видів КІ/КА, розроблення методів і механізмів запобігання та протидії можливим КІ/КА та передбачають:

визначення переліку усіх інформаційних активів, послуг, систем та мереж;

розроблення, затвердження політик безпеки та процедур реагування на КІ/КА (далі – політики безпеки та процедури);

забезпечення штатного функціонування систем та мереж;

запровадження систем виявлення вторгнень IDS (SOC);

визначення порядку інформування про кіберзагрози для проактивного виявлення підозрілої поведінки та/або зловмисної діяльності;

навчання персоналу щодо реагування та протидії кіберзагрозам, порядку сповіщення (інформування) про них;

відстеження сповіщень та аналіз повідомлень про кіберзагрози;

забезпечення операційної безпеки;

підготовки технічної інфраструктури для оброблення КІ/КА;

підготовки інструментальних засобів, середовищ для виявлення підозрілої та/або зловмисної діяльності;

розроблення і тестування алгоритмів/порядку дій для стримування (локалізації) та ліквідації наслідків КІ/КА;

визначення політики та засобів збору електронних доказів про КІ/КА.

3.1.2. Виявлення, аналіз та комунікація

Заходи кіберзахисту щодо виявлення, аналізу КІ/КА та комунікації включають:

визначення факту КІ/КА;

визначення категорії (рівня) критичності КІ/КА;

інформування про КІ/КА;

пріоритизація КІ/КА;

визначення масштабу реагування на КІ/КА;

збір та зберігання даних;

проведення технічного аналізу, зокрема: зіставлення подій між собою та документування їх хронології;

визначення підозрілої поведінки;

визначення першоджерела КІ/КА та умов, які сприяють ескалації КІ/КА;

збір індикаторів кіберзагроз;

аналіз загальних ТПП зловмисника;

аналітичної підтримки з боку третіх сторін (CERT-UA, ДЦКЗ, НКЦК, інші органи державної влади);

обмін інформацією з CERT-UA, ДЦКЗ, уповноваженими ОДВ, внутрішніми учасниками.

3.1.3. Стримування та комунікація

Заходи кіберзахисту зі стримування та комунікації мають на меті зниження негативного впливу КІ/КА, запобігання порушенню безпеки та складаються з:

ізоляції уражених систем, мереж, мережевих сегментів та пристроїв один від одного та/або від систем і мереж, які не були уражені;

створення образів пам'яті (дампів оперативної пам'яті) для збереження електронних доказів, їх використання в рамках розслідування інциденту;

закриття (блокування) мережевих портів та інтерфейсів на уражених системах/мережевих пристроях, через які може здійснюватися взаємодія зловмисника зі службами та сервісами уражених систем;

оновлення фільтрів брандмауерів;

блокування НСД, ведення журналів, ведення логів (створення лог-файлів) щодо НСД;

блокування джерел поширення ШПЗ зловмисника;

скасування привілейованого доступу користувачів, зміна паролів системного адміністратора, паролів облікових записів служб/застосунків, якщо є підозра на проникнення в систему/мережу за допомогою привілейованого доступу;

контроль активності зловмисника;обмін інформацією про кіберзагрози

обмін інформацією внутрішніми та зовнішніми учасниками.

3.1.4. Усунення та комунікація

Заходи кіберзахисту з усунення та комунікації складаються з:

перевірки усіх заражених середовищ (систем, мереж, мережевих пристроїв, хостів, сховищ даних тощо) на предмет вразливостей;

повторного створення образів пам'яті елементів уражених середовищ;

часткового або повного відновлення технологічного, технічного, мережевого, іншого обладнання, яке постраждало від наслідків КІ/КА (за необхідності – заміна такого обладнання);

заміни скомпрометованих артефактів артефактами із систем резервного копіювання та відновлення;

встановлення патчів та оновлень;

зміни усіх паролів у скомпрометованих середовищах (системах/мережах);

моніторингу будь-яких ознак реагування зловмисника на заходи зі стримування;

розроблення сценаріїв реагування на випадки, якщо суб'єкт кіберзагрози (зловмисник) використає альтернативні вектори атак;

передбачення достатньої кількості часу для перевірки того, що всі системи очищено від усіх можливих механізмів збереження кіберзагроз;

обмін інформацією з внутрішніми та зовнішніми учасниками.

3.1.5. Відновлення та комунікація

Заходи кіберзахисту з відновлення та комунікації передбачають:

повторне підключення відновлених/нових систем до мереж;

посилення безпеки периметра (переліків правил брандмауера, списки управління доступом до граничного маршрутизатора, правил доступу з нульовим рівнем довіри);

ретельне тестування систем, у тому числі заходи безпеки;

моніторинг операцій щодо підозрілої поведінки;

обмін інформацією з внутрішніми та зовнішніми учасниками.

3.1.6. Аналіз ефективності заходів з реагування на КІ/КА

Заходи кіберзахисту щодо аналізу ефективності з реагування на КІ/КА включають:

налаштування сенсорів, процедури сповіщення та збору даних журналів (лог-файлів);

підготовки остаточних звітів та внесення змін в документацію та політики безпеки після КІ/КА з урахуванням набутого досвіду;

документування КІ/КА, звітування щодо реагування на КІ/КА;

удосконалення захисних пристроїв систем/мереж;

перегляд політик безпеки та процедур для запобігання подібним інцидентам у майбутньому і застосування набутого досвіду для покращення управління майбутніми КІ/КА;

співпраця з уповноваженими ОДВ;

вжиття додаткових заходів з реагування на КІ/КА з урахуванням наданих рекомендацій та коригування заходів із кіберзахисту, впроваджуючи їх у розроблені процедури реагування.

Розділ IV. Технологічна карта процесу кіберзахисту ІКС НАДС

Функція: «Здійснення заходів щодо кібербезпеки, кіберзахисту та безпеки інформаційних технологій інформаційно-комунікаційної системи Національного агентства України з питань державної служби»

Процес: «Кіберзахист інформаційно-комунікаційних систем Національного агентства України з питань державної служби»

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Підготовка з кіберзахисту														
1.	Ідентифікація інформаційних активів, систем та мереж	Наявність систем та мереж	Протягом року	СЗІ, ГД	Визначення переліку усіх інформаційних активів, послуг, систем та мереж.	ОД Голови НАДС Перелік інформаційних активів, систем та мереж	Голова НАДС, ГД, СЗІ	паперовий	електронний	Перелік інформаційних активів, систем та мереж ТД на систему	ГД, СЗІ зовнішні, внутрішні учасники	паперовий	електронний	ПЗ систем НАДС
2.	Політики безпеки та процедури	Наявність систем та мереж	Протягом року	СЗІ, ГД	Документування: - політик безпеки; - плану реагування на КІ/КА.	ОД Голови НАДС	Голова НАДС СЗІ, ГД	паперовий	електронний	Політики безпеки План реагування на КІ/КА	СЗІ, ГД зовнішні, внутрішні учасники	паперовий	електронний	ПЗ систем НАДС

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3.	Оснащення	Наявність систем та мереж	Протягом року	СЗІ, ГД	Забезпечення штатного функціонування систем та мереж. Запровадження систем виявлення вторгнень IDS (SOC).	ОД Голови НАДС Меморандум про організацію взаємодії між НАДС та ДЦКЗ (договір про надання послуг) Функціональні повноваження СЗІ та обов'язки персоналу	ГД, СЗІ,	паперовий	електронний	ТД на систему	ГД, СЗІ зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
4.	Навчання персоналу	Підвищення рівня компетентності при виконанні завдань з кіберзахисту	За необхідності	СЗІ, ГД, УП	Організація проведення навчань і тренінгів для персоналу в рамках підготовки до реагування на КІ/КА.	ОД Голови НАДС Індивідуальна програма професійного розвитку та навчання персоналу, відповідального за забезпечення кіберзахисту ІКС	УП, ГД, СЗІ, внутрішні учасники	паперовий	електронний	Сертифікат (документ, який підтверджує результат навчання персоналу, відповідального за забезпечення кіберзахисту ІКС)	ГД, УП, СЗІ, внутрішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
5.	Інформація про кіберзагрози	Повідомлення CERT-UA, ДЦКЗ, НКЦК, СБУ ГШ ЗСУ, інших уповноважених ОДВ	Протягом року	СЗІ, ГД	Відстеження сповіщень про кіберзагрози або вразливості, аналіз повідомлень про підозрілу поведінку від користувачів, збір даних про КІ (індикатори, ТТП).	Листи-повідомлення (відкрита інформація, ДСК) CERT-UA, ДЦКЗ, НКЦК, СБУ ГШ ЗСУ, інших уповноважених ОДВ	ГД, СЗІ, CERT-UA, ДЦКЗ, інші уповнова-жені ОДВ	паперовий	електронний	Листи-повідомлення НАДС	ГД, СЗІ, CERT-UA, ДЦКЗ, інші уповнова-жені ОДВ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6.	Операційна безпека	Наявність систем та мереж, повідомлення про КІ	Протягом року	СЗІ, ГД	Здійснення сегментації систем управління від інших систем, управління сенсорами, інформування користувачів про компроментацію системи.	Листи-повідомлення CERT-UA, ДЦКЗ Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Листи-повідомлення НАДС Інформування Голови НАДС	ГД, СЗІ	-	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
7.	Технічна інфраструктура	Наявність систем та мереж, повідомлення про КІ	Протягом року	СЗІ, ГД	Підготовка інформаційно-комунікаційної інфраструктури для оброблення КІ/КА з урахуванням специфіки функціонування системи.	Повідомлення про КІ/КА Політики безпеки План захисту інформації в системі	ГД	-	електронний	Листи-повідомлення НАДС Інформування Голови НАДС	ГД	-	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
8.	Виявлення зловмисної діяльності	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Запровадження правил та сигнатур детекторів для пошуку та виявлення індикаторів кіберзагроз, аналіз журналів (лог-файлів).	Повідомлення про КІ/КА Політики безпеки План захисту інформації в системі	ГД, СЗІ, CERT-UA, ДЦКЗ	-	електронний	Листи-повідомлення НАДС Інформування Голови НАДС	ГД, СЗІ, CERT-UA, ДЦКЗ	-	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2. Виявлення, аналіз та комунікація														
9.	Визначення факту КІ/КА	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Збір інформації щодо підозрілих файлів та/або повідомлень. Оцінка зібраної інформації, формулювання висновку щодо факту КІ/КА за встановленими ознаками.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
10.	Визначення критичності КІ/КА	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Визначення показників відповідно до критеріїв критичності КІ/КА. Визначення категорії (рівня) критичності КІ/КА.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11.	Інформування про КІ	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Призначення групи реагування на КІ/КА. Повідомлення CERT-UA про КІ, інших сил кіберзахисту (за потреби).	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
12.	Пріоритизація КІ/КА	Декілька збоїв у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Визначення функціональних/ інформаційних наслідків КІ/КА. Оцінка впливу КІ/КА, надання пріоритету реагування для кожного КІ/КА.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
13.	Визначення масштабу реагування	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Визначення типу і масштабу КІ/КА. Оцінка впливу на виконання завдань як суб'єкта забезпечення кібербезпеки.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
14.	Збір та зберігання даних	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Збір, зберігання даних для перевірки (верифікації) КІ, категоризація, пріоритизація, пом'якшення наслідків, звітність та ідентифікація (атрибуція), потенційних електронних доказів.	Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
15.	Проведення технічного аналізу	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Формулювання гіпотез про мету та конкретні цілі зловмисника. Оновлення масштабу роботи з інцидентом відповідно до просування розслідування та появи нової інформації. Повідомлення про останні результати. Завершення технічного аналізу.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (за потреби)	Голова НАДС ГД, зовнішні та внутрішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16.	Регулювання інструментів з виявлення КІ/КА	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Зіставлення подій та документування хронології. Визначення відхилень від встановленої базової активності. Визначення першоджерела КІ/КА. Збір індикаторів компрометації. Аналіз загальних ТТП зловмисника. Перевірка і перегляд масштабу проведення процесу реагування на КІ/КА.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
17.	Аналітична підтримка з боку третіх сторін (за потреби)	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Визначення необхідності в аналітичній підтримці з боку CERT-UA, інших сил кіберзахисту, правоохоронних органів для розслідування КІ. Координація і сприяння отримання доступу. Координація заходів з реагування на КІ/КА з постачальниками послуг.	Повідомлення про КІ/КА	CERT-UA, ДЦКЗ, НКЦК, уповнова-жені ОДВ, СЗІ, ГД	паперовий	електронний	Листи-повідомлення НАДС до CERT-UA, ДЦКЗ, НКЦК, інших уповноважених ОДВ Інформування Голови НАДС	Голова НАДС СЗІ, ГД	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
18.	Обмін інформацією про кіберзагрози	Збій у функціонуванні системи/мережі, некоректна робота системи	Протягом року	СЗІ, ГД	Обмін інформацією про КІ відповідно до планів реагування. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки обмін інформацією із основними суб'єктами національної системи кібербезпеки та постачальниками послуг.	Повідомлення про КІ/КА	CERT-UA (MISP), ДЦКЗ, НКЦК, інші ОДВ, СЗІ, ГД	-	електронний	Листи-повідомлення НАДС до CERT-UA (MISP), ДЦКЗ, НКЦК, інших уповноважених ОДВ Інформування Голови НАДС	Голова НАДС СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
3. Стримування та комунікація														
19.	Ізоляція уражених елементів та сегментів	Неповне усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Ізоляція уражених систем та мереж, включаючи периметр, внутрішню мережу, хости/кінцеві точки	Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС СЗІ, ГД, CERT-UA зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
20.	Створення образів пам'яті (дампів)	Неповне усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД	З метою дослідження КІ та виявлення сторонніх процесів створення дампів оперативної пам'яті.	Повідомлення про КІ/КА	ГД	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
21.	Закриття портів, серверів, служб. Оновлення фільтрів брандмауерів.	Неповне усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД	Закриття певних портів, серверів, служб, оновлення фільтрів брандмауерів.	Повідомлення про КІ/КА	ГД	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, CERT-UA	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
22.	Блокування НСД та джерел поширення ШПЗ	Неповне усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Блокування НСД (журналювання, ведення логів щодо спроб НСД), блокування джерел ШПЗ та вихідного трафіка на відомі IP-адреси зловмисника, а також ті, що можуть бути IP-адресами зловмисника.	Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС СЗІ, ГД CERT-UA зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
23.	Зміна облікових даних доступу	Неповне усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Зміна паролів системного адміністратора, зміна закритих ключів і даних облікових записів служб/застосунків (за наявності підозри скасування привілейованого доступу).	Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
24.	Контроль активності зловмисника	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Контроль активності зловмисника, збір додаткових електронних доказів і визначення ТТП зловмисника (перенаправлення зловмисника до sendbox).	Повідомлення про КІ/КА	ГД, СЗІ	-	електронний	Листи-повідомлення НАДС до НКЦК, CERT-UA, ДЦКЗ Інформування Голови НАДС	Голова НАДС СЗІ, ГД CERT-UA зовнішні учасники	паперовий	електронний	ПЗ систем НАДС
4. Усунення та комунікація														
25.	Перевірка заражених середовищ	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Здійснення перевірки будь-яких ознак реагування зловмисника на заходи зі стримування. Розробка плану ліквідації наслідків КІ/КА з урахуванням сценаріїв для випадків, коли зловмисник використовує альтернативні вектори атак та механізми збереження загроз	Листи CERT-UA (відкрита інформація, ДСК) щодо ліквідації наслідків КІ/КА	ГД, СЗІ	паперовий	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до CERT-UA, ДЦКЗ, уповноважених та правоохоронних ОДВ	Голова НАДС ГД, СЗІ, CERT-UA	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
26.	Повторне створення образів уражених систем	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД	Повторне створення образів (дампів) уражених систем із «чистих» резервних копій.	Політики безпеки	ГД	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
27.	Відновлення обладнання	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Відновлення апаратного забезпечення системи.	-	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
28.	Заміна уражених артефактів	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД	Видалення артефактів КІ з уражених систем, мереж тощо.	-	ГД	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
29.	Встановлення патчів та оновлень	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД	Вжиття заходів з встановлення патчів та оновлень.	-	ГД	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
30.	Зміна облікових даних доступу	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Вжиття заходів щодо заміни облікових даних доступу, заміни усіх паролів у скомпрометованих середовищах (системах/мережах).	План захисту інформації в системі	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, СЗІ	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
31.	Моніторинг реагування на заходи	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Проведення ретельного моніторингу будь-яких ознак реагування зловмисника на заходи з ліквідації наслідків КІ/КА.	План реагування на КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС ГД, СЗІ CERT-UA,	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
32.	Сценарії реагування на альтернативні вектори КІ/КА	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Виконання усіх дій, необхідних для ліквідації наслідків КІ/КА, які передбачені планом (політикою) щодо реагування КІ/КА. Продовження дій з виявлення та аналізу для спостереження за будь-якими ознаками повторного проникнення зловмисника.	План реагування на КІ/КА	CERT-UA, ДЦКЗ, НКЦК ГД, СЗІ	паперовий	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (НКЦК, CERT-UA, ДЦКЗ)	Голова НАДС, ГД, СЗІ, CERT-UA, ДЦКЗ, НКЦК, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
33.	Передбачення часу на очищення	Усунення збою у функціонуванні системи, некоректна робота системи	Протягом року	ГД, СЗІ	Передбачення достатньої кількості часу для переконання в тому, що всі системи очищено від усіх можливих механізмів збереження кіберзагроз. Перехід до відновлення (якщо ліквідацію наслідків виконано успішно)	План реагування на КІ/КА	ГД	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (НКЦК, CERT-UA, ДЦКЗ)	Голова НАДС, ГД, СЗІ, CERT-UA, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5. Відновлення та комунікація														
34.	Повторне підключення систем	Усунено збій у функціонуванні системи, некоректну роботу системи	Протягом року	ГД	Відновлення системи НАДС до рівня оперативного використання, відновлення бізнес-процесів. Скасування змін, які внесені ШПЗ зловмисника під час КІ/КА. Зміна усіх паролів у скомпрометованих середовищах, впровадження багатофакторної автентифікації. Вжиття заходів щодо підключення систем.	ТД на систему	ГД	паперовий	електронний	Інформування Голови НАДС	Голова НАДС СЗІ, ГД	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
35.	Посилення безпеки периметра	Усунено збій у функціонуванні системи, некоректну роботу системи	Протягом року	ГД, СЗІ	Посилення безпеки периметра (наборів правил брандмауера, списків управління доступом до граничного маршрутизатора, правил доступу з нульовим рівнем довіри).	Листи-повідомлення (відкрита інформація, ДСК) CERT-UA, ДЦКЗ	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС СЗІ, ГД	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
36.	Тестування систем	Усунено збій у функціонуванні системи, некоректну роботу системи	Протягом року	ГД, СЗІ	Проведення ретельного тестування систем для перевірки нормального функціонування систем. Розгляд імітацій ТТП зловмисника для перевірки ефективності заходів реагування на КІ/КА.	ТД на систему	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС, ГД, СЗІ, зовнішні та внутрішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
37.	Моніторинг операцій	Усунено збій у функціонуванні системи, некоректну роботу системи	Протягом року	ГД, СЗІ	Перегляд усіх відповідних індикаторів кіберзагроз. Врахування усіх подій, виконаних на етапі відновлення для оновлення хронології КІ/КА. Виконання дій для відновлення.	ТД на систему	ГД, СЗІ	-	електронний	Інформування Голови НАДС	Голова НАДС, ГД, СЗІ, зовнішні та внутрішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6. Аналіз ефективності заходів реагування на КІ/КА														
38.	Налаштування сенсорів, збір журналів (лог-файлів)	Усунено КІ, система працює у штатному режимі	Протягом року	СЗІ, ГД	Додавання патчів/оновлень програмного забезпечення у масштабах установи для знешкодження (усунення) зловмисних ТТП. Продовження відслідковування середовища на предмет наявності доказів постійної присутності зловмисника (якщо такі можуть мати місце).	План реагування на КІ/КА	ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення НАДС до уповноважених ОДВ (НКЦК, CERT-UA, ДЦКЗ)	ГД, СЗІ, CERT-UA, ДЦКЗ, НКЦК, інші уповнова-жені ОДВ, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам
39.	Підготовка остаточних звітів	Усунено КІ, система працює у штатному режимі	Протягом року	СЗІ, ГД	Формування звіту за результатами реагування на КІ/КА, оновлення документації та політик після КІ/КА, співпраця з CERT-UA, іншими уповноваженими та правоохоронними органами з метою надання необхідних артефактів та/або вжиття додаткових дій з реагування.	План реагування на КІ/КА Політики безпеки ТД на систему	ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення до уповноважених ОДВ (НКЦК, CERT-UA, ДЦКЗ) Внесення змін до політик безпеки (за необхідності)	ГД, СЗІ, CERT-UA, ДЦКЗ, НКЦК, інші уповнова-жені ОДВ, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

№ з/п	Операція			Відповідальні виконавці		Вхідний документ				Вихідний документ				Прикладне програмне забезпечення
	Найменування	Умова виконання	Строк виконання	Назва суб'єкта внутрішнього контролю	Стислий опис виконуваної роботи	Найменування документу	Назва учасника процесу	Формат документу		Найменування документу	Назва учасника процесу	Формат документу		
								паперовий	електронний			паперовий	електронний	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
40.	Аналіз засвоєного досвіду	Усунено КІ/КА, система працює у штатному режимі	Протягом року	СЗІ, ГД	Проведено аналіз набутого досвіду з усіма залученими сторонами для оцінки наявних заходів безпеки та процесу управління КІ/КА, на які здійснювалось реагування, визначення політик та процедур, які потребують змін, покращення обміну інформацією з CERT-UA, іншими уповноваженими, правоохоронними органами, визначення додаткових інструментів (ресурсів), необхідних для покращення виявлення та аналізу, а також пом'якшення наслідків майбутніх КІ/КА	План реагування на КІ/КА Політики безпеки ТД на систему	ГД, СЗІ	-	електронний	Інформування Голови НАДС Листи-повідомлення до НКЦК, CERT-UA, ДЦКЗ, уповноважених та правоохоронних ОДВ (за необхідності) Внесення змін до політик безпеки (за необхідності) Внесення змін до Плану реагування на КІ/КА (за необхідності)	ГД, СЗІ, CERT-UA, ДЦКЗ, НКЦК, інші уповноважені ОДВ, зовнішні учасники	паперовий	електронний	ПЗ систем НАДС ПЗ систем протидії кіберзагрозам

Розділ V. Перелік прийнятих скорочень

№ з/п	Абревіатура	Розшифровка
1.	НКЦК	Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України
2.	ГШ ЗСУ	Генеральний штаб Збройних Сил України
3.	СБУ	Служба безпеки України
4.	Держспецзв’язку	Державна служба спеціального зв’язку та захисту інформації України
5.	ДЦКЗ	Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України
6.	CERT-UA	Урядова команда реагування на комп'ютерні надзвичайні події України Держспецзв’язку
7.	НАДС	Національне агентство України з питань державної служби
8.	ГД	Генеральний департамент з питань цифровізації у сфері державної служби НАДС
9.	УП	Управління з питань персоналу НАДС
10.	СЗІ	Сектор з питань захисту інформації НАДС
11.	ДІР	Державні інформаційні ресурси
12.	ІКС	Інформаційно-комунікаційна система
13.	ДСК	Документ для службового користування
14.	КА	Кібератака
15.	КІ	Кіберінцидент
16.	КМУ	Кабінет Міністрів України
17.	ОД	Окреме доручення Голови НАДС
18.	ОДВ	Органи державної влади
19.	НД	Нормативний документ
20.	НСД	Несанкціонований доступ
21.	ПЗ	Програмне забезпечення
22.	ТД	Технічна документація
23.	ТТП	Тактики, технікі та процедури

№ з/п	Абревіатура	Розшифровка
24.	ШПЗ	Шкідливе програмне забезпечення
25.	HRMIS	Implementation of Human Resources and Payroll Management Information System Інформаційна система управління людськими ресурсами та нарахування заробітної плати
26.	IDS	Intrusion Detection System Система виявлення вторгнень
27.	MISP	Malware Information Sharing Platform Платформа обміну інформацією щодо шкідливого програмного забезпечення CERT-UA
28.	SOC	Security Operations Center Оперативний центр реагування на кіберінциденти ДЦКЗ Держспецзв'язку

Завідувач Сектору з питань
захисту інформації НАДС **Олег ЛУЦЕНКО**