ЗАТВЕРДЖЕНО

Наказ Державної служби статистики

12 липня 2024 року № 181

Політика управління інцидентами кібербезпеки в інформаційній системі органів державної статистики

І. Загальні положення

1. Політика управління інцидентами кібербезпеки в інформаційній системі органів державної статистики (далі – Політика) визначає механізм ужиття заходів працівниками Держстату під час виявлення, аналізу й опрацювання інцидентів кібербезпеки (далі – КБ) відповідно до етапів реагування на різні види подій у кіберпросторі (далі – кіберінциденти/кібератаки) та визначення категорій (рівнів) їх критичності.

2. У цій Політиці терміни вживаються у значеннях, наведених у Цивільному процесуальному кодексі України, законах України "Про основні засади забезпечення кібербезпеки України", "Про Державну службу спеціального зв’язку та захисту інформації України", "Про критичну інфраструктуру", "Про захист інформації в інформаційно-комунікаційних системах", Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Порядку реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженому постановою Кабінету Міністрів України від 04 квітня 2023 року № 299, і Методичних рекомендаціях щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 03 липня 2023 року № 570 (далі – Методичні рекомендації).

3. Ця Політика визначає засади управління інцидентами КБ та її метою є забезпечення кібербезпеки під час ужиття послідовних заходів із реагування на кіберінцидент/кібератаку відповідно до визначених категорій (рівнів) їх критичності.

4. Категорія (рівень) критичності кіберінциденту/кібератаки визначається на етапі виявлення й аналізу кіберінциденту/кібератаки відповідно до Методичних рекомендацій та класифікується за категоріями (рівнями), визначеними пунктом 6 Порядку реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженому постановою Кабінету Міністрів України від 04 квітня 2023 року № 299.

5. Ця Політика визначає такі види інцидентів КБ:
порушення цілісності інформації;
порушення конфіденційності;
порушення доступності;
порушення спостережності.

6. З метою вжиття заходів з реагування на кіберінцидент/кібератаку в апараті Держстату утворюється постійна група реагування на інциденти КБ (далі – ГРІ), склад якої затверджується наказом Держстату.

До складу ГРІ включаються працівники самостійних структурних підрозділів апарату Держстату, до функціональних обов'язків яких належать питання забезпечення кібербезпеки, кіберзахисту та безпеки інформаційних технологій Держстату, захисту інформаційних ресурсів в ІС ОДС, забезпечення безперебійного функціонування інформаційних, комунікаційних систем і ресурсів, сталої роботи корпоративної мережі Держстату, а також координація та забезпечення статистичної конфіденційності, організації пропускного режиму та здійснення режимно-секретної роботи.

7. Організацію роботи ГРІ забезпечує департамент інформаційних технологій (далі – відповідальний підрозділ).

8. Відповідальний підрозділ забезпечує інформаційний обмін і координацію дій ГРІ під час реагування на кіберінциденти/кібератаки відповідно до Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затвердженого 22 вересня 2022 року протоколом № 20 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони.

Під час обміну інформацією про кіберінциденти/кібератаки відповідальний підрозділ керується загальними правилами обміну інформацією про кіберінциденти (протокол TLP), наведеними в додатку 1 до Методичних рекомендацій, і переліком категорій і типів кіберінцидентів, наведеним у додатку 2 до Методичних рекомендацій.

9. ГРІ вживає заходів з реагування на кіберінцидент/кібератаку послідовно за такими етапами, як підготовка, виявлення й аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти / кібератаки, які забезпечують:

оперативне виявлення, оцінку та реагування на інциденти КБ;

належне інформування про виникнення інцидентів КБ уповноважених органів та залучених сторін;

відповідність рівня КБ вимогам нормативно-правових актів і законодавству у сфері кібербезпеки, а також міжнародним стандартам у цій сфері;

мінімізацію й усунення негативних наслідків;

сталість і надійність роботи ІС ОДС;

унеможливлення повторної реалізації виявленого кіберінциденту;

запобігання інцидентам КБ у майбутньому, поліпшення впровадження та використання захисних заходів КБ;

захист ІС ОДС від порушень конфіденційності, цілісності, доступності та спостережності.

10. Координацію, перегляд Політики здійснює департамент інформаційних технологій. Зміни до Політики разом із проєктом наказу Держстату про їх унесення/затвердження подаються в установленому порядку на розгляд Голові Держстату.

ІІ. Етап підготовки

1. Реагування на кіберінциденти/кібератаки розпочинається з етапу підготовки, під час якого вживаються заходи з вивчення та дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам.

2. Заходи з підготовки складаються з:

визначення переліку всіх інформаційних активів, систем і мереж, а також установлення показників їх штатного функціонування;

розробки планів реагування на інциденти КБ за формою відповідно до Додатку 1 до цієї Політики;

розробки сценаріїв реагування на окремі види інцидентів КБ відповідно до сценарію з переліку сценаріїв, наведеного в Додатку 2 до цієї Політики, що є найбільш імовірними для Держстату;

розроблення та затвердження політик і процедур реагування на кіберінциденти/кібератаки, проведення навчань щодо їх засвоєння та використання працівниками органів державної статистики;

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

методичне консультування користувачів щодо реагування та протидії кіберзагрозам і процедур сповіщення про них;

визначення порядку інформування, використання інформації про кіберзагрози для виявлення підозрілої поведінки та потенційної діяльності зловмисника;

підготовки інфраструктури для оброблення кіберінцидентів/кібератак, розроблення й тестування алгоритмів / порядку дій для стримування (локалізації) та ліквідації наслідків кіберінцидентів/кібератак;

формування політики та засобів збору електронних доказів та іншої інформації про кіберінцидент/кібератаку.

3. ГРІ розробляє плани реагування на інциденти КБ (за різними категоріями й типами) для впорядкування та координації дій працівників органів державної статистики під час реагування на інциденти КБ з урахуванням Типового переліку

заходів із реагування на кіберінциденти/кібератаки для одночасного відстеження заходів до їх завершення, наведеного в Додатку 4 до Методичних рекомендацій.

4. ГРІ встановлює постійний зв’язок і обмін інформацією із суб’єктами, які безпосередньо в межах своєї компетенції вживають заходів із забезпечення кібербезпеки, а також постійний зв'язок із фахівцями урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (далі – CERT-UA).

5. ГРІ здійснює моніторинг наявної інформації про інциденти КБ, які відбувалися в органах державної статистики в минулому, та формує базу знань, що складається з інформації про інциденти КБ, які коли-небудь відбувалися в органах державної статистики та реагування на які здійснювалося відповідно до планів і сценаріїв реагування на інциденти КБ.

6. ГРІ аналізує та моделює поведінку зловмисника відповідно до життєвого циклу відомих (типових) вивчених кіберінцидентів/кібератак, використовуючи інформацію із власної бази знань і з бази знань ТТП MITRE ATT&CK, інструментів моделювання активності зловмисника Kill Chain та Diamond Model of Intrusion 17 Analysis, баз даних вразливостей CVE, NVD тощо, а також досвіду суб’єктів, з якими встановлено зв’язок і обмін інформацією про кіберзагрози, рекомендацій CERT-UA, Державного центру кіберзахисту Держспецзв’язку, Департаменту кіберполіції Національної поліції України, Служби безпеки України тощо.

7. ГРІ використовує для реалізації наявний план реагування на інцидент КБ, що зберігається в базі знань для поточного інциденту КБ відповідної категорії та типу. Якщо подібних інцидентів КБ у базі знань немає, то ГРІ розробляє новий комплекс заходів, який оформлюється у вигляді плану реагування на інцидент КБ за формою відповідно до Додатка 1 цієї Політики, та в подальшому зберігається в базі знань.

8. Користувачі ІС ОДС мають бути ознайомлені з цією Політикою, володіти якомога більшою кількістю інформації про виявлення кіберінцидентів/кібератак, знати порядок повідомлення визначених осіб відповідального структурного підрозділу про інцидент КБ, проходити періодичні навчання навичкам кібергігієни та реагування на підозрілу поведінку шляхом участі в онлайн- і офлайн-заходах (навчальні курси, воркшопи, вебінари, семінари, лекції тощо).

ІІІ. Етап виявлення і аналізу

1. З метою виявлення й аналізу події ГРІ запроваджує план реагування на інциденти КБ, відповідні технології та засоби збору достатньої кількості інформації для проведення моніторингу, виявлення та сповіщення про підозрілу поведінку, що може бути пов’язана з кіберінцидентом/кібератакою.

2. На етапах виявлення й аналізу інциденту КБ ГРІ вживає таких заходів:
визначення факту інциденту КБ;
визначення категорії (рівня) критичності інциденту КБ;
інформування про інцидент КБ;
пріоритетизація інциденту КБ;
визначення масштабу проведення реагування на інцидент КБ;
збір і зберігання даних;
проведення технічного аналізу, зокрема: зіставлення подій між собою та документування їх хронології; визначення підозрілої поведінки; визначення першопричини (першоджерела) інциденту КБ і умов, що сприяють його ескалації; перевірка й перегляд проведення процесу реагування на інцидент КБ;
аналітичну підтримку з боку третіх сторін (відповідно до пункту 4 розділу ІІ цієї Політики);
налаштування інструментів з виявлення інцидентів КБ.

3. До основних ознак інциденту КБ належать такі (невичерпний перелік):
суттєве зниження продуктивності ІС ОДС або її недоступність;
повідомлення від антивірусного програмного забезпечення;
несанкціонована діяльність у ІС ОДС;
стрімке збільшення мережевого трафіку;
численні повідомлення про помилки та збої;
зафіксовані спроби підбору паролів;
заздалегідь відома негативна подія безпеки;
подія безпеки, що зафіксована у неробочий час;
невідомі облікові записи;
відсутні та/або відключені засоби забезпечення безпеки;
спроби застосування методів соціальної інженерії;
тощо.

4. Аналіз інциденту КБ розпочинається за фактом отримання ГРІ від користувачів ІС ОДС або залучених третіх сторін (якщо це зазначено в договірних умовах) повідомлення про виникнення інциденту КБ. Після отримання повідомлення про інцидент КБ ГРІ проводить класифікацію інциденту КБ, аналіз зібраної інформації та приймає рішення щодо підтвердження його статусу. За необхідності ГРІ може залучати працівників інших самостійних структурних підрозділів апарату Держстату та третіх сторін (якщо це зазначено в договірних умовах).

5. У повідомленні від користувачів ІС ОДС або залучених третіх сторін (якщо це зазначено в договірних умовах) ГРІ аналізує інформацію, що містить:
опис проблеми, що спостерігається;
час виникнення інциденту КБ;
інші дані щодо інциденту КБ.

6. ГРІ вживає заходів з інформування про інцидент КБ шляхом повідомлення відповідальних суб'єктів за реагування на конкретний інцидент КБ (CERT-UA; за необхідності можуть бути проінформовані інші суб'єкти) відповідно до пункту 8 розділу І цієї Політики. При цьому інформується керівництво Держстату відповідно до розподілу функціональних повноважень та відповідальний адміністратор системи (мережевий адміністратор, адміністратор безпеки тощо) про необхідність проведення розслідування та реагування.

IV. Етап стримування

1. На етапі стримування ГРІ вживає заходів щодо попередження подальшої ескалації інциденту КБ і зменшення його негативного впливу шляхом усунення / зменшення можливостей зловмисника, у відмові йому в доступі. Тип стратегії стримування, що використовується, визначає конкретний сценарій інциденту КБ, а саме:

уживає основних заходів стримування;

відповідно до плану реагування на інцидент КБ ГРІ збирає інформацію про інцидент КБ для проведення подальшого розслідування;

погоджує з керівництвом Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання;

вибір методів збору інформації;

за необхідності переривання роботи ІС ОДС погоджує таке переривання з керівництвом Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання.

2. До основних заходів зі стримування належать:

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

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

оновлення фільтрів брандмауерів;

блокування несанкціонованого доступу, журналювання, ведення логів (створення лог-файлів) щодо несанкціонованого доступу; блокування джерел поширення шкідливого програмного забезпечення;

установлення правил блокування сервером доменних імен (DNS) відомих доменних імен зловмисника, а також тих, що можуть бути IP адресами зловмисника (на основі аналізу);

закриття (блокування) мережевих портів та інтерфейсів на вражених системах/мережевих пристроях, через які може здійснюватися взаємодія зловмисника зі службами та сервісами вражених систем (наприклад, SSH, HTTP (HTTPS), SMTP, IMAP, FTP тощо), а також на невражених системах/мережевих пристроях (лише за необхідності та при загрозі використання цих портів (інтерфейсів) зловмисником для досягнення власних цілей);

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.

3. ГРІ обирає методи та заходи, спрямовані на зменшення впливу інциденту КБ на процеси діяльності Держстату, окремо для кожного конкретного інциденту КБ, залежно від його категорій і типів, та у відповідності з розробленим планом реагування.

Будь-які методи, дії та порядок використання або виконання обраних методів й заходів погоджуються та координуються керівництвом Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання.

4. ГРІ оцінює можливий вплив запланованих заходів на безперервність діяльності враженої ІС ОДС. За необхідності допускається ізолювання або роз'єднання складових ІС ОДС на період проведення повного розслідування інциденту КБ.

V. Етап усунення інциденту КБ та відновлення функціонування ІС ОДС

1. ГРІ вживає заходів щодо усунення наслідків та відновлення штатного режиму функціонування ІС ОДС шляхом усунення артефактів інциденту (наприклад, видалення зловмисного коду, створення повторного образу пам'яті елементів "заражених" систем) і пом'якшення наслідків від реалізації кіберзагроз або інших умов, якими скористався зловмисник (зловмисні групи).

2. Заходи з усунення наслідків передбачають:

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

повторне створення образів пам'яті елементів уражених середовищ, відновлення систем від заводських налаштувань;

часткове або повне відновлення технологічного, технічного, мережевого, іншого обладнання, що постраждало від наслідків інциденту КБ (за необхідності – заміна такого обладнання);

заміну скомпрометованих артефактів артефактами із систем резервного копіювання та відновлення (відповідно до передбачених процедур перевірки артефактів на предмет компрометації, порушення властивостей інформації та будь-яких дій з ними);

установлення патчів і оновлень;

зміну всіх паролів у скомпрометованих середовищах (системах / мережах);

моніторинг 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, оскільки зловмисники часто використовують більше ніж один механізм.

3. Процедура усунення інциденту КБ та відновлення функціонування ІС ОДС залежить від виду інциденту КБ і повинна визначатись для кожного інциденту КБ окремо.

4. Після відновлення функціонування ІС ГРІ повинна перевірити відсутність ознак повторення інциденту КБ і повідомити про завершення робіт керівництво Держстату відповідно до розподілу функціональних повноважень.

VI. Етап аналізу ефективності заходів з реагування на інциденти КБ

1. На етапі аналізу ефективності заходів реагування на інциденти КБ ГРІ документує інцидент (формує звіт щодо реагування на інцидент КБ), здійснює відповідне інформування Голови Держстату щодо необхідності вдосконалення захисних пристроїв систем/мереж, переглядає документацію та політики для запобігання подібним інцидентам у майбутньому й застосування набутого досвіду для поліпшення управління майбутніми інцидентами.

2. Основні цілі етапу аналізу ефективності заходів реагування на інцидент КБ передбачають:

упевненість в усуненні та подоланні першопричин інциденту;

визначення проблем (відхилень від норм експлуатації) з програмним і апаратним забезпеченням, які необхідно розв’язати;

визначення відхилень від вимог політик КБ із визначенням ступеня впливу цих відхилень на розвиток інциденту КБ;

визначення проблем з організаційною політикою та процедурами, які необхідно розв’язати;

запровадження постійного перегляду й оновлення ролей користувачів ІС ОДС, зон відповідальності та повноважень кожного працівника органів державної статистики; визначення потреб у спеціальних членів ГРІ, визначених відповідальними працівників за реагування на інциденти КБ;

удосконалення інструментів, необхідних для виконання заходів із захисту, виявлення, аналізу та/або реагування на інциденти КБ.

3. Під час виконання заходів із розслідування інцидентів КБ ГРІ має використовувати методи та засоби, що запобігають випадковому або навмисному внесенню змін в дані, що вивчаються й аналізуються.

4. ГРІ повинна з’ясувати в межах повноважень причини інциденту КБ і провести аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень. ГРІ повинна визначити: які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, положення, розділи, пункти нормативних актів), причетність до інциденту КБ, якщо це

трапилось, третіх сторін із визначенням, наскільки це можливо, ступеня їх впливу на виникнення і перебіг інциденту КБ.

5. Після завершення розслідування ГРІ має підготувати та надати керівництву Держстату відповідно до розподілу функціональних повноважень звіт про інцидент КБ за формою, наведеною в Додатку 3.

Сформований звіт про інцидент КБ після узгодження з керівництвом Держстату відповідно до розподілу функціональних повноважень може бути наданий усім зацікавленим третім сторонам, якщо це визначено договірними умовами та/або чинним законодавством.

6. ГРІ вживає заходів щодо внесення інформації про закриття інциденту КБ у журналі реєстрації інцидентів КБ.

Заступник директора департаменту
інформаційних технологій Олександра ДОРОХОВА

Додаток 1
до Політики
(пункт 2 розділу ІІ)

Форма
плану реагування на інциденти КБ

Етапи реагування на інциденти КБ	Опис дій	Відповідальні
1	2	3
Крок 0 – Управління технічними засобами для реагування на інциденти КБ	Мінімальний набір засобів та інструментів для швидкого реагування на інциденти КБ уключає: - журнал для реєстрації дій з реагування на інциденти КБ; - актуальний план комунікацій, який містить перелік прикладних систем, адміністраторів прикладних систем, власників прикладних систем та експертів, що володіють спеціальними знаннями в різних технічних галузях; - портативний комп'ютер з установленим ПЗ для збору та розслідування інформації про інцидент КБ; - змінні носії інформації; - оптичні диски або твердотілі накопичувачі (flash) для забезпечення запуску ОС на комп'ютері без попередньої установки на жорсткий диск; - мережеві кабелі; - портативні пристрої для неруйнуючого копіювання інформації з жорстких дисків та інших носіїв; - облікові записи для доступу до прикладних систем та/або мережевого обладнання.	ГРІ
Крок 1 – Визначення та реєстрація інциденту КБ	Структурний підрозділ / працівник Держстату, який виявив можливі ознаки інциденту КБ, зазначає в повідомленні таку інформацію: - опис проблеми, що спостерігається; - час виникнення ознак інциденту; - інші суттєві дані щодо можливого інциденту – у відповідь на запитання осіб, відповідальних за реєстрацію та / або	ГРІ

1	2	3
	реагування на інцидент. Відповідальний за реєстрацію інциденту КБ учасник ГРІ фіксує інформацію про подію в описі інциденту, здійснює її класифікацію. До складу ГРІ можуть входити всі відповідальні працівники та відділи організації, які необхідні для залучення під час реагування на інцидент КБ. У випадку, якщо відповідальний за реєстрацію інциденту КБ учасник ГРІ дійде висновку, що надіслані дані не є ознакою інциденту КБ, подія визначається як "не інцидент" і на цьому процес обробки завершується.	
Крок 2 – Реагування на інцидент	ГРІ аналізує всю доступну інформацію про інцидент КБ, проводить пошук інформації в "базі знань" і визначає, чи відбувався подібний інцидент КБ у минулому. Якщо подібних інцидентів КБ у базі знань немає, ГРІ розробляє комплекс заходів, який оформляється у вигляді нового плану реагування на інцидент КБ. ГРІ визначає спосіб реагування на виявлений інцидент КБ відповідно до прийнятих планів реагування на інциденти КБ, залежно від його критичності та вектору загрози (наприклад, DDOS, атака зловмисного програмного забезпечення, злом системи, викрадення сесії або пошкодження інформації), інформує керівництво Держстату відповідно до розподілу функціональних повноважень та відповідні зацікавлені сторони (та за потреби) про прийнятий порядок з реагування. У випадку серйозності інциденту КБ та його впливу на неперервність надання послуг організацією ГРІ звертається до департаменту поширення інформації та	ГРІ, керівництво Держстату відповідно до розподілу функціональних повноважень

1	2	3
	комунікацій з проханням підготувати текст повідомлення для всіх зацікавлених сторін і передати його для офіційного оприлюднення. У процесі реагування ГРІ збирає інформацію про інцидент КБ для проведення подальшого розслідування. Вибір методів збору інформації залежить від виду інциденту КБ і погоджується з керівництвом Держстату відповідно до розподілу функціональних повноважень. ГРІ відповідає за забезпечення схоронності, цілісності та конфіденційності зібраної інформації про інцидент КБ.	
Крок 3 – Зменшення впливу інциденту	ГРІ обирає методи та заходи, спрямовані на зменшення впливу інциденту КБ на процеси діяльності організації, окремо для кожного конкретного інциденту КБ, залежно від його виду та у відповідності з цим планом. Будь-які методи, дії та порядок їхнього використання або виконання погоджуються та координуються керівництвом Держстату відповідно до розподілу функціональних повноважень або залученою зацікавленою третьою стороною. Будь-які заходи зменшення впливу інциденту КБ на інформаційні ресурси / системи, що перебувають в експлуатації, виконуються відповідно до прийнятих в організації політик та процедур. Переривання роботи активів для будь-яких виправлень і налаштувань погоджується з їх власниками та керівництвом організації. У разі неможливості обмежити подальший вплив інциденту КБ на роботу активів і процесу діяльності організації ГРІ повідомляє керівництво організації для вжиття необхідних заходів.	ГРІ, керівництво Держстату відповідно до розподілу функціональних повноважень

1	2	3
Крок 4 – Усунення інциденту та відновлення функціонування	З метою відновлення нормального функціонування активів ГРІ вживає заходів з усунення причин і наслідків інциденту КБ. Процедура усунення інциденту КБ і відновлення функціонування залежить від виду інциденту КБ та визначається для кожного інциденту КБ окремо. ГРІ та інші особи залучені до виконання запланованих дій роблять усе можливе для недопущення негативного впливу на функціонування активів. Усі дії з усунення інциденту КБ ГРІ фіксує у відповідних журналах і реєстрах. Після відновлення функціонування активів ГРІ перевіряє відсутність ознак повторення інциденту КБ і повідомляє про завершення робіт керівництву Держстату відповідно до розподілу функціональних повноважень.	ГРІ, керівництво Держстату відповідно до розподілу функціональних повноважень
Крок 5 – Аналіз інциденту	ГРІ проводить розслідування, вивчає й аналізує зібрану інформацію про інцидент КБ. ГРІ з’ясовує причини інциденту КБ і проводить аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень: у діях працівників організації, у роботі активів організації, відхилень від норм проєктування, розробки, експлуатації програмного забезпечення й обладнання, відхилень від вимог політик КБ із визначенням ступеня впливу цих відхилень на розвиток інциденту КБ. ГРІ визначає: які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів), причетність до інциденту КБ, якщо це трапилось, інших підприємств, організацій і установ із	ГРІ

1	2	3
	визначенням, наскільки це можливо, ступеня їх впливу на виникнення і перебіг інциденту КБ. ГРІ зазначає пропозиції щодо уникнення подібної ситуації в майбутньому. Під час виконання робіт із розслідування інцидентів КБ використовуються методи та засоби, що запобігають випадковому або навмисному внесенню змін у дані, що вивчаються й аналізуються. Усі дії щодо аналізу інциденту КБ ГРІ фіксує у відповідному реєстрі.	
Крок 6 – Закриття інциденту та звітування	ГРІ здійснює остаточне детальне звітування про інцидент КБ перед керівництвом Держстату відповідно до розподілу функціональних повноважень та відповідними контролюючими органами (якщо необхідно) у формі подання звіту про інцидент КБ. Якщо інцидент вплинув на інформацію будь-якої третьої сторони, відповідальний співробітник організації повідомляє третю сторону та надає всі подробиці про інцидент і всі дії, ужиті для запобігання або зменшення ймовірності його виникнення в майбутньому. Якщо інцидент вплинув на інформацію третьої сторони, організація інформує контролюючі органи про інцидент КБ лише після узгодження із третьою стороною.	ГРІ, керівництво Держстату відповідно до розподілу функціональних повноважень

Додаток 2
до Політики
(пункт 2 розділу II)

Перелік сценаріїв реагування
на інциденти КБ

1. **Brute Forcing / Брут-Форс**

Деталі: Зловмисник пробує вгадати пароль, намагаючись підібрати кілька варіантів паролів

Індикатор загрози: численні невдалі спроби входу за короткий проміжок часу

Що потрібно дослідити:

журнали активних каталогів
журнали додатків
журнали операційної системи

Рекомендовані дії: якщо дії не є законними, вимкніть обліковий запис і проведіть розслідування / заблокуйте зловмисника

2. **Botnets / Ботнет**

Деталі: зловмисники використовують сервер-жертву для проведення DDoS-атак або інших зловмисних активностей

Індикатори загрози:

підключення до підозрілих IP-адрес
аномально високий обсяг мережевого трафіку

Що потрібно дослідити:

мережевий трафік
журнали ОС (нові процеси)
зверніться до власника сервера
зверніться до служби підтримки

Рекомендовані дії:

Якщо підтверджено:

ізолювати сервер
видалити шкідливі процеси
виправити вразливість, яка використовується для зараження

3. **Ransomware / Програма-вимагач**

Деталі: тип шкідливого програмного забезпечення, яке шифрує файли й вимагає від користувача викуп (грошовий платіж), для того щоб розшифрувати файли

Індикатори загрози:

антивірусні оповіщення
підключення до підозрілих Ips

Що потрібно дослідити:

журнали антивірусів
журнали ОС
журнали облікових записів
мережевий трафік

Рекомендовані дії:

здійснити антивірусну перевірку
ізолювати комп'ютер

4. **Data Exfiltration / Витік даних**

Деталі: зловмисник (або недобросовісний працівник) передає дані зовнішнім сторонам

Індикатори загрози:

аномально високий мережевий трафік
підключення до хмарних сховищ (Dropbox, Google Cloud)
незвичайні USB-накопичувачі

Що потрібно дослідити:

мережевий трафік
журнали проксі-сервера
журнали операційної системи

Рекомендовані дії:

якщо співробітник: зверніться до керівника, проведіть повну перевірку
якщо зовнішня загроза: ізолюйте комп'ютер, відключіть його від мережі

5. **Compromised Account / Скомпрометований обліковий запис**

Деталі: зловмисники отримують доступ до одного облікового запису (шляхом соціальної інженерії або будь-яким іншим способом)

Індикатори загрози:

входи в акаунт у неробочий час
зміна групи облікових записів

аномально високий мережевий трафік

Що потрібно дослідити:

журнали активних каталогів
журнали ОС
мережевий трафік
зверніться до користувача за роз'ясненнями

Рекомендовані дії:

Якщо підтверджено:

вимкнути обліковий запис
змінити пароль
провести аналіз причин компрометації доступ до облікового запису

6. Denial Of Service (Dos/DDoS) / Відмова в обслуговуванні

Деталі: зловмисник може спричинити втручання в роботу системи, використовуючи DoS-уразливості або генеруючи великий обсяг трафіку

Індикатор загрози: аномально високий мережевий трафік на загальнодоступних серверах

Що потрібно дослідити:

мережевий трафік
журнали брандмауера
журнали операційної системи

Рекомендовані дії:

якщо DoS через вразливості: зверніться до команди з реагування для усунення проблеми
якщо DDoS через мережевий трафік: зверніться до служби підтримки мережі або провайдера

7. Advanced Persistent Treats (APTs) / Розширені постійні загрози

Деталі: зловмисники отримують доступ до системи і створюють бекдори для подальшої їх експлуатації, зазвичай їх важко виявити.

Індикатори загрози:

підключення до підозрілих IP-адрес
аномально високий обсяг мережевого трафіку
журнали доступу в неробочий час
створення нових облікових записів адміністратора

Що потрібно дослідити:

мережевий трафік

журнали доступу
журнали ОС (нові процеси, нові з'єднання, аномальні користувачі)
зверніться до власника сервера/команди підтримки

Рекомендовані дії:

Якщо підтверджено:

ізолювати робоче місце
почати формальний процес розслідування
розпочати реалізацію ескалації / комунікації із зацікавленими сторонами

Додаток 3
до Політики
(пункт 5 розділу VI)

Форма звіту про інцидент КБ

_____

(назва інциденту КБ)

Відповідальна особа за виявлення та реагування на інцидент КБ
(ПІБ, посада, контактний номер телефону)

Перелік відомостей про інцидент КБ	Опис інциденту КБ
1	2
Дата і час виявлення інциденту	
Поточний статус (новий, у процесі, вирішено)	
Тип інциденту	
Класифікація інциденту	
Область ураження (перелік уражених мережі, систем та / або програм; зміни з моменту попереднього запису)	
Вплив інциденту (перелік зацікавлених сторін, які зазнали впливу; зміни у впливі з моменту попереднього запису)	
Серйозність інциденту (опишіть вплив інциденту на організацію; зміни в серйозності інциденту з моменту попереднього запису)	
Необхідність залучення зацікавлених сторін (наприклад правоохоронних органів)	
Дії, вжиті для вирішення інциденту	
Додаткова інформація	
Контактні дані відповідальних осіб за реагування на інциденти та інших осіб за потреби	

1	2
Час, що знадобився для відновлення	
Висновки та / або пропозиції щодо поліпшення реагування на інциденти КБ	