Прим. № ___

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

03 липня 2023 року № 570

Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі

Відповідно до пункту 3 постанови Кабінету Міністрів України від 04 квітня 2023 року № 299 «Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411,

НАКАЗУЮ:

1. Затвердити Методичні рекомендації щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, що додаються.

2. Відділу інформаційних комунікацій Адміністрації Державної служби спеціального зв’язку та захисту інформації України забезпечити оприлюднення цього наказу на офіційному вебсайті Державної служби спеціального зв’язку та захисту інформації України.

3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України відповідно до розподілу обов’язків.

Голова Служби
бригадний генерал Юрій ЩИГОЛЬ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
03 липня 2023 року № 570

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі

І. Загальні положення

1. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (далі – Рекомендації) розроблені на виконання вимог пункту 3 постанови Кабінету Міністрів України від 04 квітня 2023 року № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» та призначені для суб'єктів забезпечення кібербезпеки під час вжиття заходів із кіберзахисту відповідно до етапів реагування на різні види подій у кіберпросторі (далі – кіберінциденти/кібератаки) та визначення категорій (рівнів) їх критичності.

2. Рекомендації розроблено відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про критичну інфраструктуру», Стратегії кібербезпеки України, затвердженої Указом Президента України від 01 лютого 2022 року № 37, Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, постанови Кабінету Міністрів України від 04 квітня 2023 року № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», а також Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затвердженого 22 вересня 2022 року пунктом 2.1 протоколу № 20 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України.

3. Рекомендації розроблені з урахуванням положень:

Посібника (сценаріїв) з реагування на інциденти та вразливості у сфері кібербезпеки: Оперативні процедури планування та проведення заходів із реагування на інциденти і вразливості у сфері кібербезпеки в інформаційних системах федеральних органів виконавчої влади (Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems), виданого Агентством з кібербезпеки та захисту інфраструктури (CISA);

Посібника з усунення інцидентів комп'ютерної безпеки (NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide), виданого Національним інститутом стандартів та технологій (NIST);

Посібника із заходів безпеки та приватності для інформаційних систем і організацій (NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);

Рекомендацій для класифікації та опису кібератак і вторгнень Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK);

Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури», затверджених наказом Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 (зі змінами);

ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT);

НД ТЗІ 3.6-006-21 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

4. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

Рекомендації можуть бути використані усіма суб'єктами забезпечення кібербезпеки.

5. У цих Рекомендаціях терміни вживаються в такому значенні:

автентифікація – перевірка достовірності користувача інформаційної, електронної комунікаційної, інформаційно-комунікаційної та/або системи управління технологічними процесами (далі – системи) суб'єкта забезпечення кібербезпеки через порівняння відтворених ним автентифікаційних даних з даними, делегованими для перевірки та доступу до зазначених систем;

авторизація – надання прав користувачу або групі користувачів на виконання певних дій у системах суб'єкта забезпечення кібербезпеки;

артефакт – будь-які інформаційні елементи систем суб'єкта забезпечення кібербезпеки, що використовуються при роботі (свідчать про роботу або є наслідками роботи) цих систем;

бекдор – технологія, метод та/або засіб обходу засобів захисту систем суб'єкта забезпечення кібербезпеки з метою несанкціонованого доступу до таких систем з використанням засобів приховування такого обходу та доступу;

брандмауер – програмний, апаратний або програмно-апаратний засіб, що обмежує мережевий трафік відповідно до набору правил, встановлених мережевим адміністратором;

дамп оперативної пам’яті – записаний у встановленому вигляді стан оперативної пам’яті системи суб’єкта забезпечення кібербезпеки в певний момент часу з даними цього стану;

журнал (лог-файл) – спеціальний файл, у якому накопичується автоматично зібрана інформація про події в системах та мережах суб’єкта забезпечення кібербезпеки;

зловмисник – неавторизований користувач, який намагається отримати доступ до систем (системи) суб’єкта забезпечення кібербезпеки або вже отримав доступ до зазначених систем (системи) та вживає заходів (дій), що можуть бути віднесені до підозрілої поведінки;

компрометація системи – порушення сталого, надійного та штатного режиму функціонування систем суб’єкта забезпечення кібербезпеки та/або порушення конфіденційності, цілісності, доступності інформації (інших властивостей інформації), що обробляється в цих системах;

патч – компонент програмного забезпечення, призначений для автоматизованого внесення певних змін до файлів систем (системи) суб’єкта забезпечення кібербезпеки з метою унеможливлення реалізації кіберзагрози чи експлуатації вразливостей;

підозріла поведінка – дії (бездіяльність) користувача, програмного чи апаратного забезпечення, що можуть бути ідентифіковані як спроби втручання в роботу систем суб’єкта забезпечення кібербезпеки, інших об’єктів кіберзахисту з метою експлуатації вразливостей та реалізації кіберзагроз, та можуть бути ознаками виникнення події кібербезпеки та/або кіберінциденту/кібератаки;

пісочниця (Sandbox) – узагальнена назва програмного, апаратного або програмно-апаратного засобу, що містить технології, механізми та/або засоби для безпечного виконання програм та програмного коду в ізольованому контрольованому середовищі та призначений для аналізу програмних елементів (коду) на предмет підозрілої поведінки;

руткіт – програмний засіб, призначений для приховування слідів присутності зловмисника або шкідливого програмного забезпечення (далі – ШПЗ) в системах;

система виявлення вторгнень (IDS – Intrusion Detection System) – програмний, апаратний або програмно-апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до систем та мереж або несанкціонованого управління ними через мережу Інтернет;

система запобігання вторгненням (IPS – Intrusion Prevention System) – програмний, апаратний або програмно-апаратний засіб, який проводить моніторинг систем та мереж в реальному часі з метою виявлення, запобігання або блокування підозрілої поведінки;

система управління подіями інформаційної безпеки (SIEM – Security Information and Event Management) – програмний або програмно-апаратний засіб, який збирає інформацію щодо подій інформаційної безпеки для подальшого аналізу і класифікації системним адміністратором або фахівцем з інформаційної безпеки;

системи управління провадженнями (тікетами) (TMS – Ticket Management System) – програмний засіб, призначений для фіксації, обробки, зберігання інформації щодо провадження (тікету) (інформації щодо обробки даних, процедур обробки даних, розширеної аналітики, бізнес-інформації, інформації щодо співпраці із суб'єктами забезпечення кібербезпеки, математичних та інших обчислень тощо) та її подальшого аналізу в рамках вирішення завдань суб'єкта забезпечення кібербезпеки;

тактики, техніки та процедури (ТТП) – ієрархічна модель опису поведінки та дій актора (користувача, адміністратора, зловмисника) щодо будь-якої діяльності в системах/мережах, а також спроб діяльності з метою впливу на ці системи;

ШПЗ – програмне забезпечення, функціональні можливості якого передбачають реалізацію несанкціонованих або неавторизованих процесів, які мають прямий або опосередкований вплив на сталий, надійний та штатний режим функціонування систем суб'єкта забезпечення кібербезпеки, за якого порушуються властивості інформації, що обробляється в цих системах.

Інші терміни вживаються у значеннях, наведених в 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.

6. Рекомендації не поширюються на події щодо проведення пошуку та виявлення потенційних вразливостей систем, що організовуються та проводяться відповідно до Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 року № 497.

7. Інформаційний обмін, координація та спільні дії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки здійснюються 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 України (далі – Порядок). Під час обміну інформацією про кіберінциденти/кібератаки суб'єкти забезпечення кібербезпеки керуються загальними правилами обміну інформацією про кіберінциденти (Протокол TLP) (додаток 1) та переліком категорій і типів кіберінцидентів (додаток 2).

8. Рекомендації містять заходи із кіберзахисту, що можуть проводитися суб'єктами забезпечення кібербезпеки послідовно за такими етапами, як

підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки.

Послідовність заходів до кіберзахисту етапів реагування на кіберінциденти/кібератаки графічно наведено у додатку 3.

9. Заходи з реагування на кіберінцидент/кібератаку проводяться суб'єктами забезпечення кібербезпеки таким чином, щоб забезпечити:

швидке виявлення кіберінциденту/кібератаки;

належне інформування про їх виникнення уповноважених органів та залучених сторін;

запобігання, мінімізацію та усунення негативних наслідків;

виявлення вразливостей;

відновлення надання суб'єктами забезпечення кібербезпеки послуг;

сталість і надійність систем та інших об'єктів кіберзахисту, що належать суб'єктам забезпечення кібербезпеки;

унеможливлення повторної реалізації виявленого кіберінциденту, а щодо кібератак – збереження можливих електронних доказів.

Окремі заходи є повторюваними і можуть виконуватися та змінюватися безперервно, доки підозріла поведінка не буде усунена, наслідки кіберінциденту/кібератаки не будуть ліквідовані, електронні докази, необхідні для проведення розслідування та аналізу процесу реагування на кіберінциденти/кібератаки, не будуть зібрані. Типовий перелік заходів із реагування на кіберінциденти/кібератаки для одночасного відстеження заходів до їх завершення наведено у додатку 4.

Необхідно зауважити, що заходи можуть бути як реалізовані безпосередньо суб'єктом забезпечення кібербезпеки, так і отримані як послуги від сил кіберзахисту із зазначенням у договорі вимог з кібербезпеки.

ІІ. Етап підготовки

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

Підготовка до реагування на кіберінциденти/кібератаки починається заздалегідь до того, як вони відбудуться, заради пом'якшення будь-якого впливу на суб'єкт забезпечення кібербезпеки. Типовий перелік заходів підготовки до реагування на кіберінциденти/кібератаки для одночасного відстеження наведено у додатку 5.

2. Заходи з підготовки складаються з:

визначення переліку усіх інформаційних активів, послуг, систем та мереж, встановлення показників штатного функціонування систем та мереж суб'єктів забезпечення кібербезпеки;

розроблення та затвердження політик та процедур реагування на кіберінциденти/кібератаки, проведення навчань щодо їх засвоєння та використання персоналом суб’єкта забезпечення кібербезпеки;

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

складання планів управління персоналом суб’єкта забезпечення кібербезпеки;

навчання користувачів щодо реагування та протидії кіберзагрозам та процедур сповіщення про них;

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

підготовки інфраструктури для оброблення кіберінцидентів/кібератак, зокрема з урахуванням специфіки функціонування систем суб’єкта забезпечення кібербезпеки;

розроблення і 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. Створюється перелік усіх інформаційних активів та послуг, що надаються (за наявності), усіх систем та мереж суб’єкта забезпечення кібербезпеки, а також встановлюються показники штатного функціонування систем та мереж (особливо щодо тих систем та мереж, що безпосередньо впливають на діяльність суб’єкта забезпечення кібербезпеки).

4. Заходи з розроблення та затвердження політик та процедур реагування на кіберінциденти/кібератаки, проведення навчань щодо їх засвоєння та використання персоналом суб’єкта забезпечення кібербезпеки передбачають такі постійні та циклічні дії:

розробка та затвердження планів реагування на кіберінциденти/кібератаки, включаючи процеси та процедури реагування (за різними категоріями кіберінцидентів), призначення команди реагування на кіберінциденти/кібератаки та її керівника;

запровадження політик та процедур для переведення кіберінцидентів/кібератак на вищу/нижчу категорію (рівень) критичності, а також звітування про кіберінциденти/кібератаки та вжиті заходи щодо реагування на них відповідно до Порядку;

запровадження політики збору інформації, пов’язаної з кіберінцидентом/кібератакою, її зберігання, передачі, обліку;

розробка та впровадження у повсякденну діяльність планів реагування (політик, інструкцій) на випадок виникнення надзвичайних ситуацій (для унеможливлення виникнення кіберінциденту/кібератаки на інформаційно-комунікаційних технологіях, програмних, програмно-апаратних засобах, інших технічних та технологічних засобах і обладнанні, що піддалося впливу даних ситуацій);

інформування, взаємодія та обмін електронними доказами з уповноваженими/правоохоронними органами.

5. Заходи щодо підготовки інструментальних засобів, середовищ для виявлення підозрілої поведінки (підозрілої поведінки зловмисника) передбачають наявність чіткого уявлення про інфраструктуру (системи, мережі, мережеві пристрої, хости (кінцеві точки), які потребують захисту) та запровадження:

систем виявлення вразливостей і реагування на кіберінциденти та кібератаки для проведення цілодобового моніторингу, аналізу та передачі інформації про кіберінциденти/кібератаки;

рішень для виявлення кіберзагроз та відповідного реагування на кіберінциденти/кібератаки на рівні робочих та серверних станцій (“кінцевих точок”);

можливостей із запобігання втрати даних, зокрема шляхом створення резервних копій електронних інформаційних ресурсів (у разі, якщо у володінні чи розпорядженні суб’єкта забезпечення кібербезпеки перебувають національні електронні інформаційні ресурси, що є критичними для його сталого функціонування, суб’єкти забезпечення кібербезпеки з метою усунення можливих наслідків кіберінцидентів/кібератак створюють резервні копії національних електронних інформаційних ресурсів, які передають на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством);

систем виявлення вторгнень та систем запобігання вторгненням;

брандмауерів;

систем авторизації;

перехоплення і подальшого аналізу мережевого трафіка;

систем управління подіями інформаційної безпеки.

Проводиться моніторинг сповіщень, створених системою виявлення вразливостей (інцидентів), а також запроваджуються додаткові вимоги щодо журналювання (логування), зберігання та управління журналами (лог-файлами).

6. У реагуванні на кіберінциденти/кібератаки бере участь персонал суб’єкта забезпечення кібербезпеки з підтвердженою кваліфікацією та відповідними навичками. Запроваджується періодична перевірка компетенцій фахівців шляхом виконання практичних вправ у режимі реального часу з метою підвищення готовності до реагування на кіберінциденти/кібератаки.

Важливим є залучення до навчань з реагування саме того персоналу суб’єкта забезпечення кібербезпеки, який буде здійснювати реагування на підозрілу поведінку (або кіберінциденти/кібератаки) на практиці, що дозволить зменшити витрати, підвищити компетенції та покращити навички спеціалістів (фахівців), які дійсно цього потребують. За можливості, навчання необхідно організовувати в органах, установах, організаціях та на підприємствах з урахуванням підпорядкованості в секторі, міжсекторальних зв’язків, належності до державного/приватного сектору, конкретної галузі,

кількості персоналу суб’єкта забезпечення кібербезпеки, специфіки діяльності, бізнес-процесів.

Окремо можуть проводитися регулярні навчання та вправи з відновлення системи для ефективного тестування політик забезпечення безперебійної роботи систем, резервного копіювання та відновлення.

7. Користувачі мають володіти якомога більшою кількістю інформації про виявлення підозрілої поведінки, знати порядок повідомлення про неї відповідним уповноваженим підрозділам (посадовим особам) суб’єкта забезпечення кібербезпеки та порядку реагування (подальші дії) на них. Для цього мають бути передбачені такі процедури:

ознайомлення з політикою використання систем, мереж і застосунків (із засвідченням (фіксацією) такого ознайомлення);

поширення рекомендацій, інструкцій та інших наочних матеріалів щодо виявлення підозрілої поведінки, дій та елементів, що можуть бути ознаками події безпеки, в паперовому (пам’ятки, брошури, бюлетені, плакати тощо) чи електронному вигляді (сповіщення на комп’ютер, кінцеве (термінальне) обладнання, розсилка на електронні пошти користувачів);

поширення зазначених вище матеріалів на офіційних платформах суб’єкта забезпечення кібербезпеки (вебсайти, соціальні мережі, інші платформи);

навчання користувачів навичкам кібергігієни та реагуванню на підозрілу поведінку шляхом проведення онлайн- та офлайн-заходів (навчальні курси, воркшопи, вебінари, семінари, лекції тощо);

підвищення обізнаності користувачів щодо порядку та способів звітування та звернення до посадових осіб (спеціалістів), що відповідають за підтримку інформаційних ресурсів та платформ суб’єкта забезпечення кібербезпеки та реагування на події інформаційної та кібербезпеки суб’єкта забезпечення кібербезпеки (проведення регулярних опитувань);

забезпечення зворотного зв’язку щодо виявлення підозрілої поведінки, дій та елементів користувачем (створюються канали інформування, в тому числі анонімні та альтернативні).

8. Заходи інформування про кіберзагрози можуть містити звітність про аналіз кіберзагроз, дані про профілі та наміри суб'єктів кіберзагроз (зловмисників), організаційні цілі та кампанії, а також більш конкретні індикатори кіберзагроз і напрями дій.

Важливим аспектом підготовки до реагування на можливі кіберінциденти/кібератаки є встановлення постійного зв’язку та обмін інформацією із суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, інших сил кіберзахисту, партнерів, відкритих джерел і підприємств та організацій усіх форм власності, в обов’язковому порядку – з фахівцями урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (далі – CERT-UA). Також позитивною практикою є наявність політик із взаємодії з представниками правоохоронних органів.

Доцільним є запровадження активного відстеження сповіщень про кіберзагрози чи вразливості від суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, інших сил кіберзахисту, партнерів, відкритих джерел, підприємств та організацій усіх форм власності. Крім цього, застосовуються індикатори кіберзагроз та усі (за можливості) наявні джерела інформації про кіберзагрози (загрози інформаційній безпеці), а також використані інші можливості захисту для виявлення та блокування підозрілої поведінки.

Заходи виявлення зловмисної діяльності передбачають:

використання інформації про кіберзагрози для створення правил і сигнатур з метою виявлення діяльності, пов'язаної з кіберінцидентом/кібератакою, та визначення масштабу кіберінциденту/кібератаки;

налаштування інструментів і аналіз лог-файлів та сповіщень;

пошук ознак діяльності, пов'язаної з кіберінцидентом/кібератакою та потенційно пов'язаної з ним/нею інформацію, щоб визначити тип кіберінциденту/кібератаки (додаток 2), наприклад, атака за допомогою зловмисного програмного забезпечення (далі – ПЗ), компрометація системи, перехоплення сеансу, пошкодження даних, передача/перенесення чи викрадення даних тощо.

9. Заходи з підготовки інфраструктури для оброблення (опрацювання) кіберінцидентів/кібератак, зокрема з урахуванням специфіки функціонування систем суб'єкта забезпечення кібербезпеки, передбачають:

застосування своїх можливостей для утримання, відтворення, аналізу, відновлення, а також документування скомпрометованих ресурсів;

застосування можливостей збору даних, що можуть бути електронними доказами;

створення безпечного сховища (тобто доступного лише для команди реагування на кіберінцидент/кібератаку та спеціалістів (фахівців), що надають допомогу в реагуванні) для зберігання даних про кіберінциденти/кібератаки у паперовій та/або електронній формі (журнали, реєстри, бази даних, пристрої пам'яті);

надання засобів для збору електронних доказів, зокрема створення образів дисків і активної пам'яті, а також засоби для безпечного оброблення ШПЗ;

наявність інструментів аналізу (програмних, апаратних та/або програмно-апаратних засобів) ШПЗ (того, що викликає підозру як ШПЗ) для ізолювання в пісочниці з метою вивчення технологій, засобів та інструментів впливу на системи/мережі, аналізу відповідно до типових (вже відомих) вивчених зразків ШПЗ (пошуку невідомих технологій, засобів та інструментів), отримання висновків щодо шкідливості вивченого програмного забезпечення;

упровадження системи управління провадженнями (тікетами), в якій буде зафіксовано відповідну детальну інформацію щодо підозрілої поведінки, пов'язаної з кіберінцидентом/кібератакою, наприклад, щодо уражених систем (програмного та апаратного забезпечення цих систем), мереж, мережевих

пристроїв та хостів, користувачів, виду діяльності, конкретного зловмисника, тактик, технік та процедур, що були застосовані до цих систем/мереж.

10. Заходи з розроблення і тестування алгоритмів/порядку дій для стримування (локалізації) та ліквідації наслідків кіберінцидентів/кібератак передбачають дії, які дають змогу переконатися в тому, що застосовані процеси та ресурси реагування на кіберінциденти/кібератаки працюватимуть та будуть якомога ефективнішими під час їх виявлення. Ці дії передбачають:

сегментацію систем та ресурсів команди реагування на кіберінциденти/кібератаки і управління ними окремо від інших систем суб'єкта забезпечення кібербезпеки;

управління датчиками (сенсорами, пристроями) безпеки за допомогою програмних, апаратних або програмно-апаратних засобів із віддаленим (дистанційним) підключенням;

повідомлення користувачів та залучених осіб про системи та послуги, що зазнали впливу кіберінциденту/кібератаки, шляхом надсилання відповідних повідомлень на електронну пошту, особисті мобільні пристрої тощо;

використання захищених робочих станцій (робочих станцій, що відокремлені від інших систем та/або мереж та захищені від впливу ШПЗ (програмного забезпечення зловмисника)) для проведення моніторингу та заходів із реагування; забезпечення того, що захисні системи мають надійні процеси резервного копіювання та відновлення;

створення політики щодо приховування реагування на кіберінцидент/кібератаку командою реагування, витоку інформації, що пов'язана з кіберінцидентом/кібератакою та відповідними заходами реагування, для зменшення ймовірності інформування зловмисника про вжиті заходи кіберзахисту.

11. Важливо підготувати засоби та задокументувати порядок (політику) збору електронних доказів безпосередньо до кіберінциденту/кібератаки.

Електронні докази збираються відповідно до порядку (політики), що відповідає чинним нормативно-правовим актам та законодавству України. Цей порядок (політика) доцільно розробляти разом з відповідними правоохоронними органами, щоб будь-які електронні докази могли бути визнані прийнятними для кримінального провадження та суду.

Запроваджуються процедури обліку електронних доказів (щоразу, коли електронні докази передаються від особи до особи, у бланках для відстеження руху електронних доказів (носіїв електронних доказів) має бути детально описано факт приймання-передачі з підписами кожної сторони). Для всіх електронних доказів, а також іншої інформації, що пов'язана та є важливою для електронних доказів, необхідно вести детальний журнал (в паперовій та/або електронній формі), де мають бути внесені такі дані:

ідентифікаційна інформація (наприклад, порядковий номер, дата фіксації електронного доказу, місцезнаходження в системі обліку електронних доказів, серійний номер, номер моделі, ім'я хоста, IP-адреса);

ім’я, посада та номер телефону кожної особи, яка була залучена до збору чи управління електронними доказами під час розслідування кіберінциденту/кібератаки;

час і дата (включаючи часовий пояс) кожного випадку управління електронними доказами;

місця, де зберігалися електронні докази.

інша пов’язана з електронними доказами інформація (скріншоти, облікові номери пристроїв, супроводжуючі чи уточнювальні файли, образи пам’яті тощо).

Електронні докази отримуються від системи/мережі, яка становить інтерес, як тільки є підозра, що міг (могла) статися кіберінцидент/кібератака. Користувачів та адміністраторів систем слід ознайомити із кроками, яких їм необхідно вжити для збереження електронних доказів.

Збір електронних доказів має відбуватися у безпечний спосіб, який гарантує безпеку ураженої системи/мережі, безпеку сховища (ресурсу), де зберігаються електронні докази, безпеку засобів обліку та засобів збору таких доказів.

III. Етап виявлення та аналізу

1. Найскладнішою частиною процесу реагування на кіберінцидент/кібератаку є точне виявлення та оцінювання можливих кіберінцидентів/кібератак, визначення того, чи стався кіберінцидент/кібератака, і якщо це трапилося, визначення типу та масштабу компрометації систем/мереж, що були уражені.

2. Задля виявлення та аналізу події запроваджуються політика (план) реагування, 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. Необхідно впевнитися, що у суб’єкта забезпечення кібербезпеки наявні затверджені політики (процедури) для розрізнення потенційних кіберінцидентів/кібератак від санкціонованої діяльності (наприклад, підтвердження, що ймовірний інцидент – не ситуація, коли адміністратор мережі використовує інструменти віддаленого адміністрування для оновлення ПЗ).

3. Заходи з виявлення та аналізу містять:

визначення факту кіберінциденту/кібератаки;

визначення категорії (рівня) критичності кіберінциденту/кібератаки;

інформування про кіберінцидент/кібератаку;

пріоритетизацію кіберінциденту/кібератаки;

визначення масштабу проведення реагування на кіберінциденти/кібератаки;

збір та зберігання даних;

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

першопричини (першоджерела) кіберінциденту/кібератаки та умов, що сприяють ескалації кіберінциденту/кібератаки; збір індикаторів кіберзагроз; аналіз загальних тактик, технік та процедур (далі – ТТП) зловмисника; перевірку і перегляд масштабу проведення процесу реагування на кіберінциденти/кібератаки;

аналітичну підтримку з боку третіх сторін (відповідно до пункту 8 розділу ІІ Рекомендацій);

налаштування інструментів з виявлення кіберінцидентів/кібератак.

4. Визначення факту кіберінциденту/кібератаки складається з таких етапів:

виявлення користувачем (при використанні систем, мереж, інформаційних ресурсів та платформ суб'єкта забезпечення кібербезпеки), адміністратором систем (мережевим адміністратором, адміністратором безпеки в результаті моніторингу систем/мереж або спрацювання засобів, перелічених у пункті 5 розділу ІІ Рекомендацій, підозрілої поведінки;

звітування щодо виявленої підозрілої поведінки користувачем (шляхом звернення до посадових осіб (спеціалістів), що відповідають за підтримку інформаційних ресурсів та платформ суб'єкта забезпечення кібербезпеки та реагування на події інформаційної та кібербезпеки суб'єкта забезпечення кібербезпеки. Такі процедури вже мають бути передбачені на етапі підготовки. Адміністратор систем (мережевий адміністратор, адміністратор безпеки) може повідомити керівництво суб'єкта забезпечення кібербезпеки про виявлені факти підозрілої поведінки та/або розпочати негайне реагування на підозрілу поведінку в рамках своїх повноважень (якщо наслідки підозрілої поведінки можна усунути швидко без інформування керівництва);

збір інформації щодо підозрілої поведінки (хто повідомив, його контактні дані, аспекти підозрілої поведінки, дії в системах/мережах, що можуть бути наслідками підозрілої поведінки, уражені системи/мережі/платформи, висновки щодо подальшого розгортання подій внаслідок підозрілої поведінки, пошук ознак кіберінциденту/кібератаки);

оцінка зібраної інформації та формулювання висновку щодо факту кіберінциденту/кібератаки (або ж події інформаційної та кібербезпеки, помилкового спрацювання (False Positive)).

5. Категорія (рівень) критичності кіберінциденту/кібератаки визначається відповідно до трьох критеріїв критичності кіберінциденту/кібератаки:

А. Загроза порушення сталого, надійного та штатного режиму функціонування систем (системи):

А1. Загрози немає.

А2. Безпосередня загроза для сталого, надійного та штатного режиму функціонування систем (конкретної системи суб'єкта забезпечення кібербезпеки).

А3. Безпосередня загроза для сталого, надійного та штатного режиму функціонування декількох систем окремого суб'єкта забезпечення кібербезпеки.

А4. Безпосередня загроза для сталого, надійного та штатного режиму функціонування значної кількості систем декількох суб'єктів забезпечення кібербезпеки.

А5. Транскордонний вплив загрози порушення сталого, надійного та штатного режиму функціонування систем.

Б. Загроза порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі):

Б1. Загрози немає.

Б2. Створені передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).

Б3. Порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).

В. Загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури:

В1. Загрози немає;

В2. Передумови для припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В3. Потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В4. Реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В5. Невідворотна загроза для повноцінного функціонування держави або загроза життю громадян України.

Суб'єкт забезпечення кібербезпеки, вибравши необхідні варіанти в трьох критеріях критичності кіберінциденту/кібератаки, визначає категорію (рівень) критичності кіберінциденту/кібератаки відповідно до таблиці. Зіставлення критеріїв критичності кіберінциденту/кібератаки необхідно здійснювати послідовно від А до В.

Варіанти категорій (рівнів) критичності кіберінциденту/кібератаки враховуються відповідно до однакової важливості усіх критеріїв визначення категорії (рівня) критичності кіберінциденту/кібератаки та узгоджені між собою. Якщо для кіберінциденту/кібератаки можливі два варіанти категорії (рівня) критичності кіберінциденту/кібератаки (наприклад, середній (жовтий) та високий (помаранчевий)), рекомендовано обирати вищу категорію (рівень) критичності кіберінциденту/кібератаки (в зазначеному прикладі – високий (помаранчевий)).

Якщо не вдається визначити категорію (рівень) критичності кіберінциденту/кібератаки, необхідно перевизначити показники відповідно до критеріїв визначення категорії (рівня) критичності кіберінциденту/кібератаки

або повідомити ці показники суб'єкту, відповідальному за реагування на кіберінцидент/кібератаку, з урахуванням необхідності отримання додаткової інформації про кіберінцидент/кібератаку відповідно до пункту 7 розділу I Рекомендацій.

Таблиця

Визначення категорії (рівня) критичності кіберінциденту/кібератаки

Критерії визначення категорії (рівня) критичності													Категорія (рівень) критичності, що визначається
А					Б			В					
А1	А2	А3	А4	А5	Б1	Б2	Б3	В1	В2	В3	В4	В5	
●					●			●					0, некритичний (білий)
	●				●			●					1, низький (зелений)
	●				●				●				1, низький (зелений)
		●			●			●					1, низький (зелений)
		●				●		●					1, низький (зелений)
	●					●		●					2, середній (жовтий)
	●					●			●				2, середній (жовтий)
		●				●		●					2, середній (жовтий)
	●						●	●					3, високий(помаранчевий)
	●						●		●				3, високий(помаранчевий)
	●						●			●			3, високий(помаранчевий)
	●						●				●		4, критичний (червоний)
		●					●				●		4, критичний (червоний)
		●					●					●	5, надзвичайний (чорний)
			●				●					●	5, надзвичайний (чорний)
				●			●				●		5, надзвичайний (чорний)
				●			●					●	5, надзвичайний (чорний)

6. Про кіберінцидент/кібератаку інформують відповідальних суб'єктів за реагування на конкретний кіберінцидент/кібератаку (CERT-UA; за необхідності можуть бути проінформовані інші суб'єкти). Для інформування використовують картку інформування про кіберінцидент/кібератаку (додаток 6). Також інформується керівництво суб'єкта забезпечення кібербезпеки та керівник відповідного підрозділу у сфері ІТ, інформаційної безпеки чи кібербезпеки/кіберзахисту, а також відповідальний адміністратор системи (мережевий адміністратор, адміністратор безпеки тощо) про необхідність проведення розслідування та реагування.

7. У випадках, коли мають місце декілька кіберінцидентів/кібератак, необхідно визначити черговість реагування на кожен кіберінцидент/кібератаку з метою ефективного розподілу ресурсів на реагування (часових, людських, матеріальних тощо) та зменшення негативного впливу (подальшої ескалації) кіберінциденту/кібератаки на системи/мережі суб'єкта забезпечення кібербезпеки. Для цього необхідно визначити пріоритети реагування відповідно до:

категорії кіберінциденту/кібератаки;

особливостей впливу кіберінциденту/кібератаки системи/мережі суб'єкта забезпечення кібербезпеки (особливості підозрілої поведінки, виявленої в рамках реагування на кіберінцидент/кібератаку, шляхи проникнення в системи/мережі, способи поширення у внутрішньому

периметрі системи/мережі, негативний вплив на інфраструктуру системи/мережі (мережеві пристрої, хости, сховища даних, а також на програмне забезпечення зазначеної інфраструктури);

функціональних наслідків кіберінциденту/кібератаки (впливу на поточну функціональність уражених систем/мереж, впливу на бізнес-процеси та надання послуг користувачам цих систем/мереж, майбутніх функціональних наслідків кіберінциденту/кібератаки, якщо його не буде негайно стримано (локалізовано));

інформаційних наслідків кіберінциденту/кібератаки (впливу на конфіденційність, цілісність і доступність (інші властивості) інформації, що обробляється в уражених системах/мережах суб'єкта забезпечення кібербезпеки), інформаційного впливу на інші суб'єкти забезпечення кібербезпеки (партнерів, наприклад, у випадках доступу та модифікації конфіденційної інформації);

можливості відновлення після кіберінциденту/кібератаки (кількість ресурсів (часових, людських, матеріальних тощо), які необхідно витратити на відновлення після цього кіберінциденту/кібератаки, зусилля, необхідні для фактичного відновлення після кіберінциденту/кібератаки, визначення, наскільки ці зусилля будуть варті мети, задля якої вони застосовуються, та як зусилля з відновлення співвідносяться з будь-якими іншими вимогами з реагування на кіберінциденти/кібератаки).

Враховуючи зазначені аспекти, команда реагування на кіберінциденти/кібератаки суб'єкта забезпечення кібербезпеки дає оцінку (кількісну та/або якісну) впливу кожного кіберінцидента/кібератаки та надає пріоритет реагування, відповідно до якого здійснює розподіл ресурсів та проводить подальші заходи з реагування на кіберінцидент/кібератаку.

Варто враховувати, що кожен суб'єкт забезпечення кібербезпеки визначає наслідки впливу кіберінцидентів/кібератаки відповідно до власних бізнес-процесів, особливостей функціонування, надання послуг, ресурсів, організаційно-штатної структури та інших чинників. У разі потреби суб'єкт забезпечення кібербезпеки може звернутися за допомогою у пріоритетизації кіберінцидентів/кібератак до CERT-UA, команд реагування на комп'ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов'язані з кіберзахистом.

8. Для визначення масштабу проведення реагування на кіберінциденти/кібератаки необхідно використовувати наявні дані, щоб визначити тип доступу, ступінь впливу на активи, рівень привілеїв, яких досягнув зловмисник, а також функціональний або інформаційний вплив. Важливо виявити пов'язану із ситуацією зловмисну діяльність, слідкуючи за мережевими даними, а також пов'язаними із процесом реагування артефактами на боці хоста (лог-файли хоста, брандмауера) та проксі-сервера разом з іншими мережевими даними.

Початкове визначення масштабу інциденту для визначення заходів щодо реагування може містити аналіз результатів, отриманих з:

автоматичної системи або детекторів (датчиків) виявлення та сповіщення;

повідомлення/звіту від користувача, підрядника (виконавця) або стороннього постачальника послуг;

повідомлення/звіту про інцидент або оновлення даних у рамках поінформованості щодо ситуації від інших внутрішніх або зовнішніх компонентів суб'єкта забезпечення кібербезпеки.

9. Збір та зберігання даних, пов'язаних з кіберінцидентом/ кібератакою, має відбуватися відповідно до правил збору такої інформації, затверджуватися в рамках виконання заходів етапу підготовки. Ця інформація може бути використана для категоризації кіберінцидентів/кібератак, їх пріоритезації (визначення першочерговості заходів реагування для ефективного розподілу ресурсів, зменшення негативних наслідків кіберінциденту/кібератаки), та інформування/звітності. За необхідності (та коли це можливо) така інформація зберігається й захищається як електронні докази. Збору та збереженню підлягають:

дані з фізичного периметра систем, внутрішньої мережі (мережевих пристроїв), серверів та кінцевих точок (хостів);

журнали (лог-файли) аудиту, операцій, будь-яких змін на носіях, виявлення атак/вторгнень, підключень, функціонування системи та дій користувачів (журнал реєстрації операцій);

дампи оперативної пам'яті та дисків (для збереження доказів та криміналістичного аналізу).

Облік електронних доказів та інших даних (ідентифікаційної інформації, інформації щодо посадових осіб, що проводять збір електронних доказів, інформації щодо кожного випадку управління доказами) ведеться в окремому детальному журналі (в паперовій та/або електронній формі).

10. Проведення технічного аналізу, при якому має бути сформоване та розвинене технічне та контекстне розуміння кіберінциденту/кібератаки, передбачає:

зіставлення між собою подій та документування їх хронології (збір, збереження і аналіз журналів (лог-файлів) та/або сповіщень засобів, передбачених пунктом 5 розділу II Рекомендацій);

вивчення підозрілої поведінки (оцінка уражених систем/мереж на предмет наявності впливу зловмисника);

визначення першопричини кіберінциденту (збір інформації про вразливості системи/кіберзагрози, які можна буде використати під час пошуків та інформування про подальші заходи з реагування);

збір індикаторів кіберзагроз кіберінциденту/кібератаки (визначення і документування показників (даних), які можна буде використовувати для кореляційного аналізу в системах/мережах);

аналіз та моделювання поведінки зловмисника відповідно до життєвого циклу відомих (типових) вивчених кіберінцидентів/кібератак (з використанням інформації з бази знань TTП MITRE ATT&CK, інструментів моделювання активності зловмисника Kill Chain та Diamond Model of Intrusion

Analysis, баз даних вразливостей CVE, NVD тощо), досвіду суб'єктів, з якими встановлено зв'язок та обмін інформацією про кіберзагрози, та власного досвіду в реагуванні на кіберінциденти/кібератаки, рекомендацій CERT-UA, Державного центру кіберзахисту Держспецзв'язку, Департаменту кіберполіції Національної поліції України, Служби безпеки України, Національного банку України тощо);

перевірка і перегляд масштабів проведення розслідування (використання наявних даних та результатів заходів із реагування, що тривають, які дозволяють визначити будь-які додаткові потенційно уражені системи, пристрої та пов'язані з ними облікові записи).

11. На етапі виявлення та аналізу команда реагування на кіберінциденти/кібератаки може використати інформацію щодо ТТП зловмисника для того, щоб змінити налаштування інструментів та засобів, що використані під час реагування (згідно із пунктом 5 розділу II Рекомендацій). Ці дії мають дати змогу уповільнити темпи просування ШПЗ (ШПЗ зловмисника) вглиб периметра систем (внутрішнього та зовнішнього (фізичного)), внутрішньої мережі, мережевих пристроїв, хостів та сховищ даних, збільшити витрати зловмисника (часові, матеріальні, людські), зменшити поточний вплив зловмисника та збільшити ймовірність виявлення наслідків подальших заходів (дій) зловмисника. Необхідно враховувати можливе введення до мережі/системи нових інструментів та/або модифікацію наявних, щоб обійти механізми реагування, орієнтовані на наявні індикатори.

IV. Етап стримування

1. Мета етапу стримування полягає в тому, щоб попередити подальшу ескалацію та зменшити негативний вплив кіберінциденту/кібератаки шляхом усунення/зменшення можливостей зловмисника, у відмові йому в доступі. Тип стратегії стримування, що використовується, визначає конкретний сценарій кіберінциденту/кібератаки.

2. Оцінюючи напрям дій зі стримування, необхідно враховувати:

будь-які додаткові несприятливі впливи у певній сфері, вплив на доступність (можливість надання послуг клієнтам тощо);

тривалість процесу стримування, необхідні ресурси та ефективність стримування (наприклад, повне чи часткове стримування; повне стримування чи рівень стримування невідомий);

будь-який вплив на спроможність збору, збереження, захисту і документування доказів.

3. Важливо врахувати, що зловмисники можуть активно відслідковувати заходи з реагування та змінювати свої ТТП, щоб уникнути впливу заходів із кіберзахисту, які були проведені на етапах виявлення та стримування. Тому складається більш повна картина можливостей і потенційних реакцій зловмисника, які він може застосовувати з урахуванням своїх спроможностей та відомих вразливостей системи, що має стати підґрунтям для виконання наступних заходів із кіберзахисту, з метою

запобігання можливому інформуванню зловмисника про майбутні кроки з його стримування (при врахуванні можливостей зловмисника треба виходити з найгіршого можливого сценарію).

4. Для команди реагування на кіберінциденти/кібератаки встановлюється градація заходів реагування відповідно до часу їх проведення (короткострокові, середньострокові, довгострокові) для визначення першочерговості цих заходів та ефективного розподілу ресурсів (часових, людських, матеріальних). Час та ресурси проведення таких заходів мають бути чітко визначеними та достатніми для досягнення кінцевої мети проведення кожного заходу реагування.

5. До головних заходів зі стримування належать:

ізоляція уражених систем, мереж, мережевих сегментів та пристроїв один від одного та/або від систем і мереж, які не були уражені. Необхідно врахувати операційні та/або бізнес-процеси та необхідність їх продовження (продовження надання послуг, наскільки це можливо);

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

оновлення фільтрів брандмауерів;

блокування несанкціонованого доступу, журналювання, ведення логів (створення лог-файлів) щодо несанкціонованого доступу; блокування джерел поширення ШПЗ (ШПЗ зловмисника);

встановлення 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 уражених системах/мережевих пристроях, через які може здійснюватися взаємодія зловмисника зі службами та сервісами уражених систем (наприклад, SSH, HTTP (HTTPS), SMTP, IMAP, FTP тощо), а також на неуражених 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.

6. Якщо будуть виявлені нові ознаки підозрілої поведінки та діяльності зловмисника, необхідно повернутися до етапу виявлення та аналізу, щоб повторно визначити заходи, необхідні для реагування на кіберінциденту/кібератаки. Після успішного стримування (тобто, якщо немає нових ознак підозрілої поведінки, діяльності зловмисника, мінімізовано наслідки впливу зловмисника та визначено усі джерела поширення ШПЗ (ШПЗ зловмисника)) необхідно зберегти електронні докази для використання у подальшій роботі уповноваженими органами та розслідування правоохоронними органами, а також повторно налаштувати інструменти з

виявлення кіберзагроз відповідно до отриманого досвіду і висновків та перейти до ліквідації наслідків і відновлення систем.

V. Етап усунення

1. Метою етапу усунення є відновлення штатного режиму функціонування 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. Перш ніж перейти до ліквідації наслідків, слід переконатися, що було враховано всі засоби постійного доступу до мережі, активність зловмисника стримана достатньою мірою, всі електронні докази було зібрано, а також чи можлива циклічність цих умов. Етап усунення також може передбачати посилення або модифікацію захисту систем/мереж (середовища захисних систем та пристроїв, призначених для захисту систем/мереж від несанкціонованого доступу, впливу ШПЗ (ШПЗ зловмисника)), якщо відома першопричина атаки та/або вектор початкового доступу. Заходи з ліквідації наслідків та відновлення можуть бути виконані одночасно. Перед початком заходів із ліквідації наслідків необхідна координація дій з постачальниками послуг, уповноваженими та правоохоронними органами, суб'єктами національної системи кібербезпеки.

3. Для виконання плану із ліквідації наслідків необхідно вжити заходів задля усунення всіх ознак підозрілої поведінки та запобігання присутності суб'єкта кіберзагрози (зловмисника) у середовищі. Також необхідно впевнитися, що електронні докази збережено відповідно до потреби. Слід зауважити, що зловмисники мають численні постійні бекдори до систем і мереж (дані про них) і можуть проникнути до неуражених зон, якщо їх усунення та ліквідація наслідків їхніх дій не організовані в належний спосіб і/або є недостатньо жорсткими. Саме тому плани з ліквідації наслідків мають бути добре сформульовані та скоординовані.

4. Заходи з усунення наслідків передбачають:

перевірку усіх 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 кіберінциденту/кібератаки (за необхідності – заміна такого обладнання на нове);

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);

встановлення патчів та оновлень;

зміну усіх 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.

5. Після виконання плану з ліквідації наслідків необхідно продовжувати дії з виявлення та аналізу, щоб спостерігати за будь-якими ознаками повторного проникнення зловмисника або використання нових методів доступу. Якщо після завершення заходів із ліквідації наслідків буде виявлено підозрілу поведінку або активність зловмисника, необхідно повернутися до етапу технічного аналізу або стримування та виконати повторно всі заходи реагування, доки не буде ідентифіковано справжній масштаб компрометації та початкові вектори зараження. Якщо нової активності зловмисника не виявлено, можна переходити до етапу відновлення.

VI. Етап відновлення

1. Метою етапу відновлення є пом'якшення наслідків від реалізації кіберзагроз та інших умов, якими скористався зловмисник.

На цьому етапі основними завданнями є підтвердження того, що усунення наслідків кіберінциденту/кібератаки було успішним, відбулися перебудова систем/мереж (зміна налаштувань пристроїв системи та/або мережевих пристроїв, їх структури у внутрішньому периметрі системи/мережі), повторне підключення систем/мереж, відтворення або виправлення інформації. Слід відновити нормальну роботу систем та функціональних процесів. Найважливішим аспектом відновлення є підвищена пильність й відповідні засоби контролю для підтвердження успішного виконання плану з відновлення та відсутності ознак зловмисної діяльності у середовищі.

2. Заходи з відновлення передбачають:

повторне підключення відновлених/нових систем до мереж;

посилення безпеки периметра (наприклад, нові переліки правил брандмауера, списки управління доступом до граничного маршрутизатора і правила доступу з нульовим рівнем довіри (Zero Trust));

ретельне тестування систем, у тому числі заходи безпеки;

моніторинг операцій щодо підозрілої поведінки.

3. З метою підтвердження відновлення штатного функціонування систем/мереж пропонується можливість проведення незалежного тесту (тестування на проникнення), аудиту та перегляду діяльності, пов'язаної із реагуванням, з використанням сил та засобів Держспецзв'язку або інших сил кіберзахисту.

VII. Етап аналізу ефективності заходів реагування на кіберінциденти/кібератаки

1. Метою етапу аналізу ефективності заходів реагування на кіберінциденти/кібератаки є документування інциденту (формування звіту щодо реагування на кіберінцидент/кібератаку), інформування керівництва суб'єкта забезпечення кібербезпеки, удосконалення захисних пристроїв систем/мереж, перегляд документації та політик для запобігання подібним інцидентам у майбутньому і застосування набутого досвіду для покращення управління майбутніми інцидентами.

2. Необхідно налаштувати детектори (сенсори), процедури сповіщення та збору даних з журналів (лог-файлів). За результатами роботи над кіберінцидентом/кібератакою необхідно доповнити та удосконалити елементи процедури виявлення в масштабах суб'єкта забезпечення кібербезпеки, визначити сегменти систем/мереж, що в майбутньому можуть бути використані зловмисником для власних цілей. Важливо також уважно відслідковувати усі наявні середовища на предмет наявності доказів постійної присутності зловмисника. За можливості суб'єкти забезпечення кібербезпеки, що мають операційні центри кібербезпеки (SOC – Security Operations Center) або використовують послуги таких центрів, повинні розглянути імітацію ТТП зловмисника, щоб переконатися, що нещодавно впроваджені заходи реагування ефективні для виявлення кібератаки/кіберінциденту або пом'якшення наслідків активності, що спостерігалася.

3. Необхідно підготувати остаточні звіти та внести зміни в документацію та політики вже після інциденту відповідно до чинного законодавства з урахуванням набутого досвіду. Необхідно співпрацювати з уповноваженими органами, щоб вжити додаткових дій (заходів) з реагування, та правоохоронними органами, щоб надати необхідні артефакти (електронні докази). Доцільно враховувати рекомендації уповноважених органів при коригуванні заходів із кіберзахисту, впроваджуючи їх у розроблені політики реагування. Важливо провести аналіз отриманого досвіду задля перегляду результативності та ефективності реагування на кіберінциденти/кібератаки.

4. Основні цілі етапу аналізу ефективності заходів реагування на кіберінциденти/кібератаки передбачають:

впевненість в усуненні та подоланні першопричин інциденту;

визначення проблем з програмним та апаратним забезпеченням, які необхідно розв'язати;

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

запровадження постійного перегляду й оновлення ролей персоналу суб'єкта забезпечення кібербезпеки, зон відповідальності та повноважень кожного фахівця (спеціаліста) суб'єкта забезпечення кібербезпеки;

визначення потреб у технічній підготовці, підготовці персоналу суб'єкта забезпечення кібербезпеки, відповідального за реагування на кіберінциденти/кібератаки;

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

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку
полковник Данило МЯЛКОВСЬКИЙ

Додаток 1
до Методичних рекомендацій
щодо реагування суб'єктами
забезпечення кібербезпеки на
різні види подій в кіберпросторі
(пункт 7 розділу I)

Загальні правила обміну інформацією про кіберінциденти
(Протокол TLP)

I. Загальні положення

1. Загальні правила обміну інформацією про кіберінциденти (Протокол TLP) (далі – Правила) розроблені на основі рекомендації Європейської агенції з кібербезпеки (ENISA Considerations on the Traffic Light Protocol[1]) та відповідають документу Форуму команд реагування та безпеки (FIRST Standards Definitions and Usage Guidance – версії 2.0 «Traffic Light Protocol»[2].

2. Правила призначені для використання основними суб'єктами національної системи кібербезпеки, іншими органами державної влади, зокрема секторальними органами у сфері захисту критичної інфраструктури, об'єктами критичної інфраструктури під час формування повідомлень про кіберінциденти.

3. Правила визначають спосіб маркування повідомлень про кіберінциденти з метою обмеження кола осіб – сторін інформаційного обміну, які можуть мати доступ до повідомлення. Вони розроблені для сприяння поширенню інформації та використовують чотири кольори для позначення того, яким чином повідомлення може в подальшому поширюватися стороною, яка отримує інформацію.

II. Терміни та визначення понять

У Правилах терміни вживаються в такому значенні:

кінцевий одержувач – група осіб, окремі особи або організація, для яких призначене повідомлення про кіберінциденти, сформоване стороною, що поширює інформацію;

клієнти організації – група осіб, окремі особи чи організації, які отримують послуги від організації;

Примітки

[1] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

[2] https://www.first.org/tlp/

організація – група осіб, яка пов’язана спільною політикою. Організація включає представників, що обмінюються інформацією;

спільнота – група осіб або окремі особи, які мають спільні цілі, практики та неформальні довірчі відносини. Така спільнота може охоплювати широке коло осіб, що можуть бути учасниками інформаційного обміну на рівні країни, сектору чи регіону;

сторона, яка поширює інформацію, – група осіб, окрема особа чи організація, що створює повідомлення про кіберінциденти та визначає маркування для нього відповідно до Правил;

учасники інформаційного обміну – група осіб, окремі особи або організації, які мають доступ до сформованих стороною, що поширює інформацію, повідомлень про кіберінциденти.

ІІІ. Використання Правил

1. Сторона, яка поширює інформацію, визначає маркування для повідомлення про кіберінциденти відповідно до цих Правил (далі – мітка TLP) та відповідає за те, що кінцеві одержувачі розуміють та можуть дотримуватися правил щодо спільного застосування Правил.

2. Якщо стороні, яка отримує інформацію, необхідно поширити інформацію більш широко, ніж передбачено маркуванням згідно з міткою TLP, вона повинна отримати дозвіл від сторони, яка поширює інформацію.

3. Мітки TLP, якими сторони інформаційного обміну повинні маркувати повідомлення про кіберінциденти, наведено у таблиці 1.

Таблиця 1

Мітки TLP

Мітка (колір)	Значення	Приклад
1	2	3
TLP:RED (ЧЕРВОНИЙ)	Не для поширення, тільки для кінцевого одержувача. Мітка **TLP:RED** використовується у випадках, коли інформація не може поширюватися для третьої сторони, і її несанкціоноване поширення може	Одержувачі не можуть поширювати інформацію з міткою **TLP:RED** іншим сторонам за межами конкретного кола осіб, зустрічі або розмови, в яких вона була спочатку розкрита. Зазвичай

Продовження додатка 1

1	2	3
	вплинути на репутацію або функціонування сторони, яка поширює інформацію. Застосовується виключно для обмеженого кола учасників інформаційного обміну та їх працівників, що визначається стороною, яка поширює інформацію	використовується під час поширення інформації за особистої зустрічі або прямим електронним листом кінцевому одержувачу. Мітка **TLP:RED** може застосовуватися для передачі повідомлень про кіберінцидент представникам основних суб'єктів національної системи кібербезпеки
TLP:AMBER (ЖОВТИЙ)	Обмежене поширення, доступне тільки серед представників організації, що є кінцевим одержувачем, або її клієнтів. Коли обмеження поширення повідомлення доступне виключно серед представників організації, що є кінцевим одержувачем, повідомлення маркується як **TLP:AMBER+STRICT**. Мітка **TLP:AMBER** використовується, коли для підвищення ефективності обробки інформації необхідна стороння підтримка або допомога, і водночас її несанкціоноване поширення створює репутаційні ризики або загрози для функціонування сторони, яка поширює інформацію, якщо вона поширюється за межі залучених організацій. Застосовується для обмеженого кола учасників інформаційного обміну, кінцевий одержувач може поширювати таку інформацію тільки серед представників своєї організації, а також передавати клієнтам або замовникам, яким необхідно знати цю інформацію, щоб захистити себе чи запобігти	Мітка **TLP:AMBER** або **TLP:AMBER+STRICT** може застосовуватися для передачі індикаторів компрометації до CERT-UA з метою інформування інших організацій про потенційні загрози

Продовження додатка 1

1	2	3
	подальшій шкоді (окрім повідомлень, що промарковані міткою **TLP:AMBER+STRICT)**	
TLP:GREEN (ЗЕЛЕНИЙ)	Обмежене поширення, доступне тільки для представників спільноти або сектору. Мітка **TLP:GREEN** використовується, коли інформація може підвищити обізнаність усіх учасників інформаційного обміну, а також представників інших організацій або секторів. Застосовується для поширення інформації з організаціями–партнерами у своєму секторі або у спільноті, але без поширення через засоби масової інформації, Інтернет, соціальні мережі. Інформація з міткою **TLP:GREEN** не може поширюватися за межами спільноти	Мітка **TLP:GREEN** використовується для підвищення колективної безпеки, може застосовуватися для обміну аналітичною інформацією та рекомендаціями щодо шкідливого програмного забезпечення або фішингових атак стосовно певного сектору
TLP:CLEAR (БІЛИЙ)	Необмежене поширення. Мітка **TLP:CLEAR** використовується, коли інформація несе мінімальний або нульовий прогнозований ризик неправильного використання з урахуванням загальноприйнятних правил публічного оприлюднення	Інформація з міткою **TLP:CLEAR** може поширюватися без обмежень з урахуванням вимог законодавства про авторське право

4. В електронних листах мітка TLP вказується у темі повідомлення та в листі безпосередньо перед інформацією, якою здійснюється обмін.

У паперових документах мітка TLP вказується у верхньому і нижньому колонтитулах кожної друкованої сторінки з урахуванням кольору мітки.

Мітка TLP позначається великими літерами: TLP:RED, TLP:AMBER, TLP:AMBER+STRICT, TLP:GREEN або TLP:CLEAR, шрифтом 12pt або більше.

5. Кольори, які мають використовуватися при маркуванні повідомлень мітками TLP, наведено в таблиці 2.

Продовження додатка 1

Таблиця 2

Кольори для міток TLP

Колірна модель		TLP:RED	TLP:AMBER	TLP:GREEN	TLP:CLEAR
1		2	3	4	5
RGB: font	R	255	255	51	255
	G	43	192	255	255
	B	43	0	0	255
RGB: background	R	0	0	0	0
	G	0	0	0	0
	B	0	0	0	0
CMYK: font	C	0	0	79	0
	M	83	25	0	0
	Y	83	100	100	0
	K	0	0	0	0
CMYK: background	C	0	0	0	0
	M	0	0	0	0
	Y	0	0	0	0
	K	100	100	100	100
Hex: font		#FF2B2B	#FFC000	#33FF00	# FFFFFF
Hex: background		#000000	#000000	#000000	#000000

6. Правила не призначені для позначення інформації, що становить державну, банківську таємницю та службову інформацію. Така інформація передається відповідно до законодавства України.

_____

Додаток 2
до Методичних рекомендацій
щодо реагування суб'єктами
забезпечення кібербезпеки на
різні види подій в кіберпросторі
(пункт 7 розділу I)

Перелік категорій і типів кіберінцидентів

1. Перелік категорій і типів кіберінцидентів (далі – Перелік) розроблений з використанням рекомендацій Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy, січень 2018 року) та спільного документа ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs).

2. Перелік призначений для впровадження єдиної таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

3. Перелік може застосовуватися суб'єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, наведених у цьому документі.

4. Суб'єкти забезпечення кібербезпеки при обміні та поширенні інформації про кіберінциденти, підготовці звітів і публічних повідомлень про кіберінциденти застосовують Перелік.

5. Коли на початковій стадії реагування кіберінцидент може бути віднесений до декількох категорій, вибирається категорія із більшим рівнем загрози.

6. Перелік категорій і типів кіберінцидентів наведено в Таблиці.

Таблиця

Код xx	Категорія інциденту	Код xx	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Отримання небажаних повідомлень або великої кількості повідомлень (флуд)

Продовження додатка 2

Код хх	Категорія інциденту	Код хх	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з ШПЗ або посилання на його завантаження
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами
		04	Шкідливе підключення	Malicious connection	Спроби з’єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов’язаних із активністю певної бот-мережі
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі за допомогою спеціального програмного забезпечення
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіка
		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою, спрямована на збір даних, може містити посилання на фішингові сайти)

Продовження додатка 2

Код xx	Категорія інциденту	Код xx	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації/доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, у сервіс, застосунок через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на штатний режим функціонування системи чи сервісу, що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо
		03	Збій	Outage, no malice	Збій у роботі системи чи її компоненту без зловмисного втручання
07.	Порушення властивостей інформації	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації

Продовження додатка 2

Код xx	Категорія інциденту	Код xx	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
	(Information Content Security)	02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність у системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту. Неможливо віднести до жодного іншого існуючого типу інциденту. У разі групування великої кількості однакових за характером інцидентів необхідно додавати новий тип інциденту

7. Приклади визначення коду для типу кіберінциденту:

ПРИКЛАД 1: Код інциденту: 01.01; Тип інциденту: Spam (Спам).

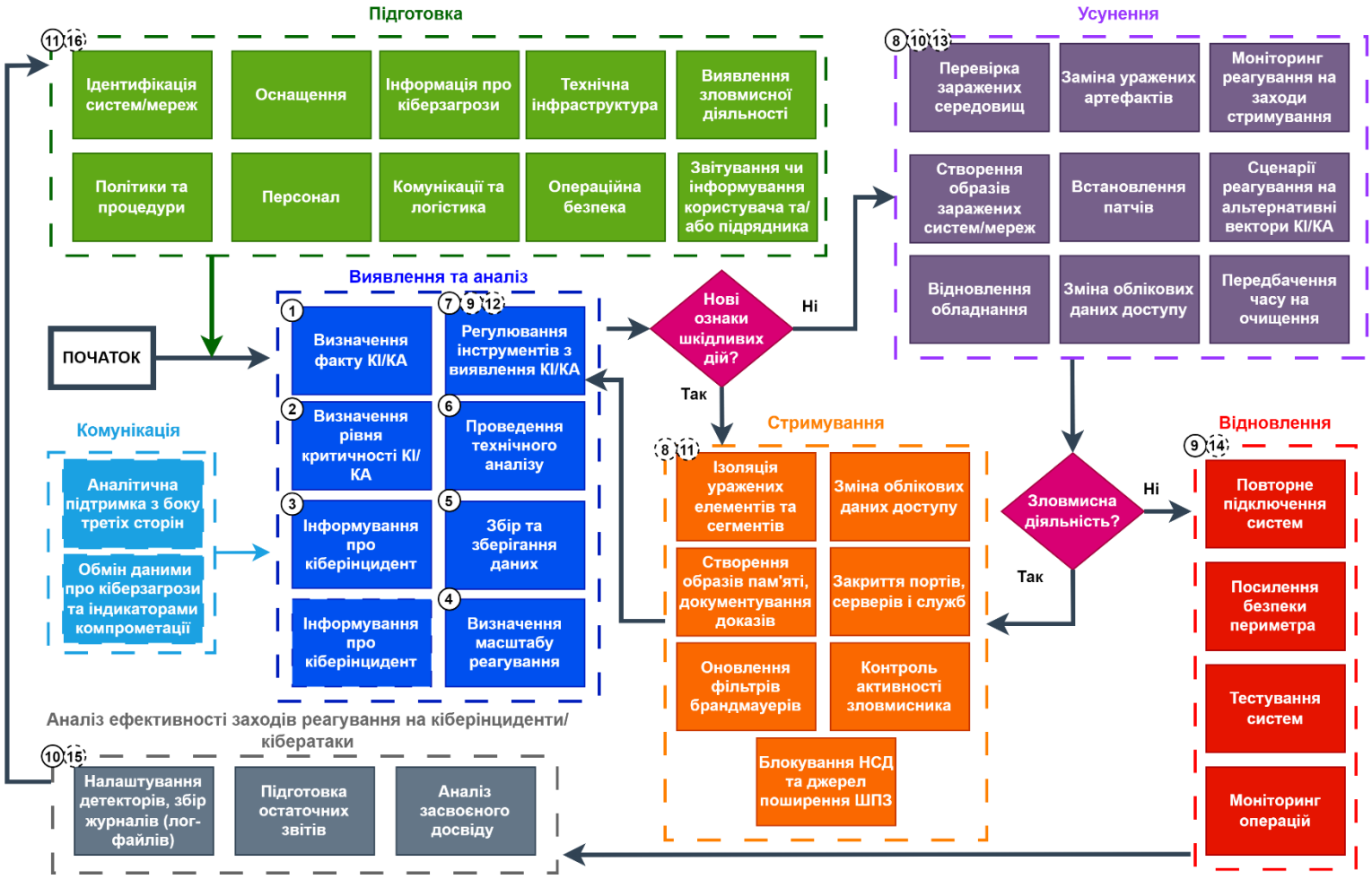
ПРИКЛАД 2: Код інциденту: 02.04; Тип інциденту: Malicious connection (шкідливе підключення).

Якщо інцидент віднесено до певної категорії, проте не визначено його тип, такий інцидент належить до Невизначеного інциденту та в подальшому при накопиченні великої кількості однакових за характером інцидентів необхідно додавати новий тип інциденту.

ПРИКЛАД 3: Код інциденту: 10.01; Тип інциденту: не визначено. Категорія: Abusive content.

Додаток 3
до Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій в кіберпросторі
(пункт 8 розділу I)

Послідовність заходів реагування на кіберінциденти/кібератаки



Додаток 4
до Методичних рекомендацій
щодо реагування суб'єктами
забезпечення кібербезпеки на
різні види подій у кіберпросторі
(пункт 9 розділу I)

Типовий перелік заходів із реагування на кіберінциденти/кібератаки для одночасного відстеження заходів до їх завершення

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
I. Етап виявлення та аналізу			
1. Визначення факту кіберінциденту/кібератаки			
1.1	Збір інформації щодо підозрілої поведінки		
1.2	Оцінка зібраної інформації, формулювання висновку щодо факту кіберінциденту/кібератаки		
2. Визначення категорії (рівня) критичності кіберінциденту/кібератаки			
2.1	Визначення показників відповідно до критеріїв критичності кіберінциденту/кібератаки		
2.2	Визначення категорії (рівня) критичності кіберінциденту/кібератаки		
3. Інформування про інцидент			
3.1	Призначення об'єднаної групи реагування на кіберінцидент/кібератаку (уповноваженого органу), який відповідатиме за координацію щодо інциденту		
3.2	Повідомлення CERT-UA про інцидент (інших сил кіберзахисту за потреби)		
3.3	Визначення категорії кіберінциденту/кібератаки		
4. Пріоритетизація кіберінциденту/кібератаки (за умови, якщо мають місце два та більше кіберінцидентів/кібератак)			
4.1	Визначення функціональних наслідків кіберінциденту/кібератаки		
4.2	Визначення інформаційних наслідків кіберінциденту/кібератаки		
4.3	Визначення впливу на відновлення після кіберінциденту/кібератаки		
4.4	Оцінка впливу кожного кіберінциденту/кібератаки та надання пріоритету реагування для кожного кіберінциденту/кібератаки		
5. Визначення масштабу проведення реагування на кіберінциденти/кібератаки			
5.1	Визначення типу і масштабу кіберінциденту/кібератаки		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
5.2	Оцінка оперативного або інформаційного впливу на завдання суб'єкта забезпечення кібербезпеки		
6. Збір і збереження даних			
6.1	Збір і збереження даних для перевірки (верифікації) інцидентів, категоризації, пріоритезації, пом'якшення наслідків, інформування/звітності та ідентифікації (атрибуції), а також потенційних електронних доказів		
6.2	Ведення обліку усіх електронних доказів		
7. Проведення технічного аналізу			
7.1	Розвиток технічного та контекстного розуміння кіберінциденту/кібератаки		
7.2	Формулювання гіпотез про мету та конкретні цілі зловмисника		
7.3	Оновлення масштабу роботи з інцидентом відповідно до просування розслідування та появи нової інформації. Повідомлення уповноваженого суб'єкта про останні результати і статус кіберінциденту/кібератаки		
7.4	Умова припинення. Технічний аналіз завершено, коли проведено перевірку (верифікацію) інциденту, визначено масштаб реагування, виявлено метод(и) постійного доступу до мережі, оцінено вплив (наслідки), сформульовано гіпотези про можливе використання ТТП та індикаторів компрометації		
8. Зіставлення подій та документування хронології			
8.1	Аналіз журналів (лог-файлів) для зіставлення даних щодо діяльності зловмисника		
8.2	Створення хронології інцидентів, де буде зафіксовано події, опис подій, дату та час для наявних випадків, впливів і джерел даних. Слідкування за оновленням інформації		
9. Визначення підозрілої поведінки			
9.1	Оцінка уражених систем та мереж на предмет наявності непомітної активності з поведінкою зловмисника, яка часто може виглядати як легітимна		
9.2	Визначення відхилень від встановленої базової активності (показників функціонування) (особливо важливо виявлення спроб використати справжні облікові дані та вбудовані можливості й інструменти у середовищі)		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
10. Визначення першопричин та сприятливих умов			
10.1	Визначення першопричин інциденту і збір інформації про вразливості системи та загрози, які в подальшому можуть бути використані для пошуку та інформування про подальші заходи з реагування		
10.2	Визначення і документування умов, які дозволили зловмиснику отримати доступ і проводити заходи (дії) в ураженому середовищі		
10.3	Оцінка мереж та систем на наявність змін, які могли бути внесені для обходу захисту та/або полегшення постійного доступу		
10.4	Визначення вектора кіберінциденту/кібератаки та збір інформації про методи доступу до середовища (наприклад, ШПЗ, використане зловмисником, RDP, VPN)		
10.5	Оцінка усіх скомпрометованих систем, користувачів, служб та мереж		
11. Збір індикаторів компрометації			
11.1	Перегляд наявної інформації (звітів) щодо розвідки кіберзагроз на наявність прецедентів подібної діяльності		
11.2	Аналіз інструментів зловмисника (оцінка інструментів та ресурсів для проведення короткострокових, середньострокових та довгострокових заходів реагування)		
11.3	Визначення і документування показників, які можна використовувати для кореляційного аналізу в мережі		
11.4	Надання вилученої інформації про загрози (індикатори, заходи протидії) командам реагування		
12. Аналіз загальних ТТП зловмисника			
12.1	Визначення методів отримання початкового доступу		
12.2	Визначення конфігурації управління зловмисника (порти, протоколи, профілі, домени, IP-адреси) (якщо отримання доступу здійснено або частково здійснено завдяки зловмисному програмному забезпеченню)		
12.3	Визначення методів, які використовував зловмисник, для виконання коду		
12.4	Оцінка скомпрометованих систем/мереж, хостів для визначення сегментів, через які може бути продовжене поширення ШПЗ (ШПЗ зловмисника)		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
12.5	Визначення методів переміщення зловмисника в загальній інфраструктурі (системах/мережах), а також методів, які використовував зловмисник для отримання доступу до віддалених хостів		
12.6	Визначення рівня доступу до облікових даних зловмисником та/або отримання нових прав/привілеїв		
12.7	Визначення методів отримання віддаленого доступу, облікових даних, які використовуються для автентифікації та підтвердження рівня прав/привілеїв користувачів		
12.8	Визначення (відслідковування) механізмів передавання даних на джерела зловмисника		
13. Перевірка і перегляд масштабів проведення процесу реагування на кіберінциденти/кібератаки			
13.1	Визначення нових потенційно уражених систем, пристроїв та пов’язаних з ними облікових записів		
13.2	Введення нових індикаторів компрометації та типових технічних рішень до інструментів з виявлення кіберінцидентів/кібератак		
13.2	Оновлення інформації та повідомлення про масштаб інциденту усіх залучених сторін		
14. Аналітична підтримка з боку третіх сторін (за потреби)			
14.1	Визначення необхідності в аналітичній підтримці з боку CERT-UA та інших сил кіберзахисту, правоохоронних органів для розслідування інциденту або реагування		
14.2	Координація і сприяння отримання доступу (якщо до заходів із реагування внесено аналітичну підтримку з боку третіх сторін)		
14.3	Координація заходів щодо реагування на кіберінциденти/кібератаки з постачальниками послуг, які надаються суб’єкту забезпечення кібербезпеки, для систем, розміщених за межами підрозділів цього суб’єкта		
15. Інструменти з налаштування			
15.1	Налаштування інструментів задля уповільнення темпу просування та зменшення часу очікування (постійне додавання індикаторів компрометації для захисту та/або виявлення підозрілої поведінки)		
15.2	Запровадження змін до інструментів для досягнення більшої точності. Налаштовуються інструменти, щоб зосередитися на тактиці, якої має дотримуватися зловмисник для		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
	досягнення оперативних цілей (наприклад, виконання коду, отримання доступу до облікових даних і горизонтального переміщення).		
II. Етап стримування			
16. Стримування активності (короткострокові засоби пом'якшення наслідків)			
16.1	Визначення відповідної стратегії стримування, включаючи: вимоги щодо збереження електронних доказів; доступність послуг (наприклад, підключення до мережі, безперервність надання послуг для клієнтів); обмеження ресурсів; тривалість кожного заходу стримування;		
16.2	Координація дії із CERT-UA, іншими силами кіберзахисту, правоохоронними органами, збір і збереження електронних доказів для проведення розслідування.		
16.3	Ізоляція уражених систем та мереж, включаючи периметр, внутрішню мережу, хости/кінцеві точки		
16.4	Закриття певних портів, серверів, служб. Оновлення фільтрів брандмауера		
16.5	Зміна паролів системного адміністратора, зміна закритих ключів і даних облікових записів служб/застосунків (за наявності підозри скасування привілейованого доступу)		
16.6	Блокування несанкціонованого доступу (журналювання, ведення логів щодо спроб несанкціонованого доступу), блокування джерел ШПЗ та вихідного трафіка на відомі IP-адреси зловмисника, а також ті, що можуть бути IP-адресами зловмисника (на основі аналізу)		
16.7	Встановлення правил блокування сервером доменних імен (DNS) відомих доменних імен зловмисника, а також тих, що можуть бути IP-адресами зловмисника (на основі аналізу)		
16.8	Запобігання підключенню скомпрометованих систем до інших систем у мережі		
16.9	Контроль активності зловмисника, збір додаткових електронних доказів і визначення ТТП зловмисника (за можливості – перенаправлення зловмисника до пісочниці)		
16.10	Моніторинг будь-яких ознак реагування зловмисника на заходи зі стримування		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
16.11	Повідомлення CERT-UA (інших сил кіберзахисту) та правоохоронних органів про оновлену хронологію і результати реагування		
16.12	Повторне визначення масштабу роботи з інцидентом та технічний аналіз (за наявності виявлених нових ознак підозрілої поведінки та/або діяльності зловмисника)		
16.13	Умова припинення. Збереження електронних доказів для використання у подальшій роботі або для розслідування правоохоронними органами (за потреби), налаштування інструментів з виявлення та перехід до ліквідації наслідків (за відсутності нових ознак зламу)		
III. Етап усунення			
17. Виконання плану із ліквідації наслідків			
17.1	Розробка плану ліквідації наслідків, який враховує сценарії для випадків, коли суб'єкт загрози (зловмисник) використає альтернативні вектори атак та численні механізми збереження загроз		
17.2	Повідомлення CERT-UA (інших сил кіберзахисту) та правоохоронних органів про стан запровадження заходів реагування на кіберінцидент/кібератаку, доки не буде завершено всі дії з ліквідації наслідків		
17.3	Видалення артефактів інциденту з уражених систем, мереж тощо		
17.4	Повторне створення образів (дампів) уражених систем із «чистих» резервних копій		
17.5	Відновлення апаратного забезпечення (якщо задіяно руткіти)		
17.6	Перевірка на предмет наявності ШПЗ (ШПЗ зловмисника) задля забезпечення видалення шкідливого програмного коду		
17.7	Проведення ретельного моніторингу будь-яких ознак реагування зловмисника на заходи з ліквідації наслідків кіберінциденту/кібератаки		
17.8	Передбачення достатньої кількості часу для переконання в тому, що всі системи очищено від усіх можливих механізмів збереження кіберзагроз (наприклад, бекдорів, оскільки зловмисники часто використовують декілька механізмів)		
17.9	Врахування усіх відповідних подій на кожному етапі реагування в хронологічному порядку		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
17.10	Виконання усіх дій, необхідних для ліквідації наслідків кіберінциденту/кібератаки, які передбачені планами (політиками) щодо реагування		
17.11	Продовження дій з виявлення та аналізу для спостереження за будь-якими ознаками повторного проникнення зловмисника або використання нових методів доступу після виконання плану з ліквідації наслідків		
17.12	Якщо після завершення заходів з ліквідації наслідків буде виявлено активність зловмисника, необхідно стримувати нову активність та повернутися до технічного аналізу (доки не буде ідентифіковано справжній масштаб компрометації та початкові вектори зараження)		
17.13	Перехід до відновлення (якщо ліквідацію наслідків виконано успішно)		
IV. Етап відновлення			
18. Виконання плану із відновлення			
18.1	Відновлення систем/мереж суб'єкта забезпечення кібербезпеки до рівня оперативного використання, відновлення завдань/бізнес-процесів		
18.2	Скасування всіх змін, внесених ШПЗ (ШПЗ зловмисника) під час кіберінциденту/кібератаки		
18.3	Зміна усіх паролів у скомпрометованих середовищах		
18.4	Впровадження багатофакторної автентифікації для всіх методів доступу до облікових записів, систем/мереж, послуг		
18.5	Встановлення оновлень та патчів		
18.6	Посилення безпеки периметра (наприклад, наборів правил брандмауера, списків управління доступом до граничного маршрутизатора, правил доступу з нульовим рівнем довіри (Zero Trust))		
18.7	Проведення ретельного тестування систем (включаючи оцінювання засобів контролю безпеки) для перевірки нормального функціонування систем		
18.8	Розгляд імітацій ТТП зловмисника для перевірки ефективності заходів реагування на кіберінциденти/кібератаки		
18.9	Перегляд усіх відповідних індикаторів кіберзагроз для забезпечення		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
	поінформованості про ситуацію щодо діяльності суб'єкта кіберзагрози (зловмисника)		
18.10	Врахування усіх подій, виконаних на етапі відновлення, для оновлення хронології кіберінциденту/кібератаки		
18.11	Виконання усіх дій для відновлення		
V. Етап аналізу ефективності заходів реагування на кіберінциденти/кібератаки			
19. Налаштування детекторів (сенсорів), сповіщень та збір журналів (лог-файлів)			
19.1	Додавання патчів/оновлень програмного забезпечення у масштабах установи для знешкодження (усунення) зловмисних ТТП зловмисників		
19.2	Продовження відслідковування середовища на предмет наявності доказів постійної присутності зловмисника (якщо такі можуть мати місце)		
20. Підготовка остаточних звітів			
20.1	Формування звіту за результатами реагування на кіберінцидент/кібератаку, інформування керівництва суб'єкта забезпечення кібербезпеки		
20.2	Оновлення документації та політик вже після інциденту відповідно до законодавства та політик		
20.3	Вивчення звіту за результатами реагування на кіберінцидент/кібератаку. Проведення детального покрокового огляду усього кіберінциденту/кібератаки командою реагування на кіберінцидент/кібератаку		
20.4	Співпраця із CERT-UA, іншими силами кіберзахисту та правоохоронними органами, щоб надати необхідні артефакти, та/або вжити додаткових дій з реагування		
21. Проведення розбору			
21.1	Проведення аналізу набутого досвіду з усіма залученими сторонами для оцінки наявних заходів безпеки та процесу управління кіберінцидентами/кібератаками, на які здійснювалось реагування		
21.2	Визначення, чи дотримувався процедур реагування на кіберінциденти/кібератаки суб'єкт забезпечення кібербезпеки (чи були вони достатніми для ліквідації наслідків кіберінциденту/кібератаки; унеможливлення		

Продовження додатка 4

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
	повторної реалізації кіберінциденту/кібератаки)		
21.3	Визначення політик та процедур, які потребують змін для запобігання виникненню подібних інцидентів у майбутньому		
21.4	Визначення шляхів покращення обміну інформацією із CERT-UA, іншими силами кіберзахисту та правоохоронними органами, іншими залученими сторонами під час реагування на кіберінцидент/кібератаку		
21.5	Визначення помилок у підготовці спеціалістів, що забезпечують реагування на кіберінцидент/кібератаку		
21.6	Визначення ролей, зон відповідальності, інтерфейсів і повноважень, що нечітко, неявно визначені або накладаються один на одного		
21.7	Визначення індикаторів кіберзагроз (компрометації), які слід відстежувати в майбутньому, щоб виявити подібні випадки		
21.8	Визначення, чи було програмне, апаратне та програмно-апаратне забезпечення суб'єкта забезпечення кібербезпеки правильно налаштованим та готовим для захисту та проведення заходів з реагування на кіберінцидент/кібератаку (якщо ні – визначення недоліків у підготовці до реагування та подальших дій з виправлення цих недоліків)		
21.9	Визначення додаткових інструментів чи ресурсів, необхідних для покращення виявлення та аналізу і пом'якшення наслідків майбутніх кіберінцидентів/кібератак		
21.10	Визначення недоліків у процесі планування реагування на кіберінциденти/кібератаки суб'єкта забезпечення кібербезпеки (якщо недоліків не виявлено, визначення, в який спосіб суб'єкт забезпечення кібербезпеки має намір запровадити ретельніше планування у сфері реагування на кіберінциденти/кібератаки)		

Додаток 5
до Методичних рекомендацій
щодо реагування суб'єктами
забезпечення кібербезпеки на
різні види подій у кіберпросторі
(пункт 1 розділу II)

Типовий перелік заходів підготовки до реагування на кіберінциденти/кібератаки для одночасного відстеження

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
1. Політики та процедури			
1.1	Документування плану реагування на кіберінциденти/кібератаки суб'єкта забезпечення кібербезпеки з процедурами для переведення на вищий/нижчий рівень та звітування про серйозні інциденти, а також про ті інциденти, що впливають на завдання суб'єкта забезпечення кібербезпеки		
1.2	Документування процедур (порядку дій) для призначення суб'єкта забезпечення кібербезпеки, який відповідатиме за координацію щодо кіберінциденту/кібератаки		
1.3	Визначення фахівців, які братимуть участь у реагуванні на кіберінциденти/кібератаки, та їхньої зони відповідальності		
1.4	Визначення власників систем та спеціалістів з безпеки інформаційних систем.		
1.5	Визначення IP-адрес системи, плану безпеки системи, межі системи/анклаву, важливої інформації щодо виконання завдань тощо		
1.6	Документування планів реагування (політик, інструкцій) на випадок виникнення надзвичайних ситуацій (для унеможливлення виникнення кіберінциденту/кібератаки на інформаційно-комунікаційних технологіях, програмних, програмно-апаратних засобах, інших технічних та технологічних засобах і обладнанні, що зазнало впливу цих ситуацій)		
2. Оснащення			
2.1	Запровадження можливостей виявлення та моніторингу, включаючи AV, EDR, DLP, IDPS, PCAP і SIEM, журнали (лог-файли), мережеві протоколи NetFlow тощо, щоб мати чітке уявлення про інфраструктуру (системи, мережі, хмарні платформи та мережі, хости)		
2.2	Встановлення показників штатного функціонування систем та мереж, зокрема тих, що безпосередньо впливають на		

Продовження додатка 5

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
	діяльність суб'єкта забезпечення кібербезпеки, визначення допустимих відхилень (похибок) від цих показників		
2.3	Запровадження систем виявлення вторгнень		
2.4	Забезпечення журналювання (ведення логів), зберігання цих журналів (лог-файлів) та управління ними		
3. Проведення навчання персоналу суб'єкта забезпечення кібербезпеки, який бере участь у реагуванні на кіберінциденти/кібератаки			
3.1	Проведення навчань і тренінгів для залученого персоналу суб'єкта забезпечення кібербезпеки в рамках підготовки до реагування на кіберінциденти/кібератаки		
3.2	Виконання вправ з відновлення системи для тестування систем відмовостійкості/резервного копіювання/відновлення		
4. Інформація про кіберзагрози			
4.1	Відстеження сповіщень про кіберзагрози чи вразливості від органів державної влади, CERT-UA, Департаменту кіберполіції Національної поліції України, офіційних джерел Держспецзв'язку, Служби безпеки України, Національного банку України, інших сил кіберзахисту, партнерів, вендорів, відкритих джерел		
4.2	Інтегрування каналів інформації про кіберзагрози (джерел інформації) в роботу підрозділів, що відповідають за реагування на кіберінциденти /кібератаки		
4.3	Аналіз повідомлень про підозрілу поведінку від користувачів, підрядників (виконавців)/постачальників послуг (або повідомлення чи звіти про кіберінциденти від інших внутрішніх або зовнішніх компонентів суб'єкта забезпечення кібербезпеки)		
4.4	Збір даних про кіберінциденти (індикатори. ТТП, контрзаходи), поширення цієї інформації іншим суб'єктам забезпечення кібербезпеки (відповідно до пункту 6 розділу І Рекомендацій)		
5. Операційна безпека			
5.1	Здійснення сегментації систем управління від інших систем, управління сенсорами (датчиками) та пристроями безпеки за допомогою засобів із віддаленим підключенням		

Продовження додатка 5

№ з/п	Захід реагування на кіберінциденти/кібератаки	Вжиті заходи	Дата вжиття заходів
5.2	Розроблення методів інформування користувачів про скомпрометовані (зламані) системи		
5.3	Використання захищеного середовища (ізольованого від інших систем та захищеного від впливу ШПЗ (ШПЗ зловмисника), програмного та апаратного забезпечення), призначеного для проведення моніторингу та заходів із реагування командою реагування на кіберінциденти/кібератаки		
5.4	Забезпечення надійності процесів резервного копіювання та відновлення в захищених системах		
5.5	Запровадження процесів діяльності команди реагування щодо приховування реагування на діяльність зловмисника (введення в оману, перенаправлення, імітація бездіяльності тощо)		
6. Технічна інфраструктура			
6.1	Створення безпечних середовищ для даних про кіберінциденти і звітності		
6.2	Застосування своїх можливостей для утримання, відтворення, аналізу та відновлення скомпрометованих хостів		
6.3	Впровадження інструментів для збору електронних доказів, створення образів пам’яті (дампів), сховищ для зберігання та журналів обліку електронних доказів		
6.4	Впровадження можливості оброблення/знешкодження зловмисного програмного забезпечення, аналіз програмного забезпечення в пісочниці, використання інших інструментів аналізу		
6.5	Впровадження та використання систем управління провадженнями (тікетами)		
7. Виявлення зловмисної діяльності			
7.1	Запровадження правил та сигнатур детекторів (датчиків) для постійного пошуку та виявлення індикаторів кіберзагроз		
7.2	Аналіз журналів (лог-файлів) та сповіщення на предмет підозрілої або зловмисної діяльності		

Додаток 6
до Методичних рекомендацій
щодо реагування суб'єктами
забезпечення кібербезпеки на
різні види подій в кіберпросторі
(пункт 6 розділу III)

Картка інформування про кіберінцидент/кібератаку

Примітка: *1. Для позначення потрібних варіантів підкреслити (обвести, виділити кольором) обраний варіант.* *2. Намагатися вказати якомога більше інформації, заповнивши відповідні поля.*

TLP				
RED	AMBER	AMBER + STRICT	GREEN	CLEAR
Дата та час виявлення кіберінциденту/кібератаки:	___..___._____ ___:___:___ GMT ____			

Заявник			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	
Суб'єкт забезпечення кібербезпеки:			

Джерело виявлення кіберінциденту/кібератаки			
Адміністратор	Користувач	Антивірусне ПЗ	EDR
IDS/IPS	Інше(вказати): _____ ___		

Запропонована категорія (рівень) критичності кіберінцидент/кібератаки	
0, некритичний (білий)	1, низький (зелений)
2, середній (жовтий)	3, високий (помаранчевий)
4, критичний (червоний)	5, надзвичайний (чорний)
Не вдалося визначити	

Отримана інформація
_____ _____ _____ _____ _____ _____ _____ _____ _____

Постраждалий суб'єкт забезпечення кібербезпеки	
Юридична назва:	
Адреса:	

Продовження додатка 6

Електронна адреса:		Номер телефону:	
Контактна особа 1			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	
Контактна особа 2			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	

Сектор (галузь) атакованого об'єкта			
Сектор безпеки і оборони	Органи державної влади	Органи місцевого самоврядування	Енергетичний сектор
Сфера електронних комунікаційних послуг	ІТ сектор	Транспортна галузь	Фінансовий сектор
Підприємства та організації відповідної форми власності	Засоби масової інформації	Інші критичні організації	Інше (вказати): _____ _____

Доменна зона			
UAGOV Український державний	UACOM Український недержавний	FGOV Закордонний державний	FCOM Закордонний недержавний

Відношення України до кіберінциденту/кібератаки			
Україна – об'єкт атаки	Україна – джерело атаки	Україна – елемент механізму атаки	не стосується території України
Інше(вказати): _____			

Категорія та тип кіберінциденту (відповідно до Переліку категорій та типів кіберінцидентів)

Код	*Категорія кіберінциденту*	*Код*	*Тип кіберінциденту*
01	Шкідливий (образливий) вміст (Abusive content)	01	Спам
02	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (ШПЗ)
		02	Розповсюдження ШПЗ
		03	Командно-контрольний центр (С2)
		04	Шкідливе підключення
03	Збір інформації зловмисником (Information Gathering)	01	Сканування
		02	Сніфінг
		03	Фішинг
04	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості
		02	Спроби авторизації/входу в систему
05	Втручання (Intrusion)	01	Компрометація облікового запису
		02	Компрометація системи

Продовження додатка 6

06	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні
		02	Саботаж/шкідливі дії
		03	Збій
07	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації
		02	Несанкціонована модифікація
08	Шахрайство (Fraud)	01	Шахрайський сайт
09	Відома вразливість (Vulnerable)	01	Вразливість
		03	Некоректна конфігурація
10	Інше (Other)	01	Невизначений інцидент

Дата та час початку кіберінциденту/кібератаки:	___.___._____ ___:___:___ GMT____

Чи пов'язаний цей (ця) кіберінцидент/кібератака з попередніми?

ТАК	НІ	ID пов'язаного кіберінциденту/кібератаки: _____	Невідомо

Короткий опис кіберінциденту/кібератаки

_____
_____
_____
_____
_____
_____
_____

Вплив на функціонування систем/мереж, сервіси (послуги)

Немає впливу взагалі	Немає впливу на сервіси (послуги)
Мінімальний вплив на некритичні сервіси (послуги)	Мінімальний вплив на критичні сервіси (послуги)
Значний вплив на некритичні сервіси (послуги)	Значний вплив на некритичні сервіси (послуги)
Втрата доступності некритичних сервісів (послуг)	Втрата доступності критичних сервісів (послуг)

Кількість скомпрометованих систем/мереж (ЕОМ)

1-10	10-50	Інше (вказати):_____	Невідомо

Тип скомпрометованої системи/мережі за функціоналом

Робочі станції	Сервер(и) додатків	Сервер(и) баз даних	Вебсервер(и)
Сервери доменних імен	Поштовий сервер	Брандмауер(и)	Мережеве обладнання
Інше(вказати):			

Об'єкт кібератаки

Тип (модель):	
Ім'я:	

Продовження додатка 6

Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			
CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок:			

Тип (модель):	
Ім'я:	
Операційна система:	
Дата встановлення ОС:	
Часова зона:	
Мережеві налаштування:	
Облікові записи:	
CVE:	CVE-____-____ CVE-____-____ CVE-____-____
Висновок:	

Тип (модель):	
Ім'я:	
Операційна система:	
Дата встановлення ОС:	
Часова зона:	
Мережеві налаштування:	
Облікові записи:	
CVE:	CVE-____-____ CVE-____-____ CVE-____-____
Висновок:	

Чи вирішено кіберінцидент/кібератаку?		**Чи потрібна допомога CERT-UA?**	
Так	Ні	Так	Ні

Чи повідомлялося про кіберінцидент/кібератаку іншим основним суб'єктам забезпечення кібербезпеки? Яким саме?

Так		Ні
Служба безпеки України	Міністерство оборони України та Генеральний штаб Збройних Сил України	Розвідувальні органи
Національний банк України	Національна поліція України	Національний

Продовження додатка 6

		координаційний центр кібербезпеки при РНБО України
Департамент кіберполіції Національної поліції України	Коментар: _____ _____	

Чи залучалися сторонні організації до вирішення кіберінциденту/кібератаки?			
Так		Ні	
Інший CERT, CSIRT, SOC	Антивірусні компанії	Обслуговуюча компанія, інтегратор, представник вендора	Інше (вказати): _____ _____
Коментар: _____ _____ _____ _____			

Результат впливу			
Витік даних	Злам (компрометація) системи	Втрата функціональності систем/сервісів	Інше (вказати): _____ _____

Від потенційного впливу кіберінциденту/кібератаки на державному рівні під загрозою			
Національна безпека	Сталість економіки	Національний імідж	Функціонування Уряду
Безпека персональних даних громадян	Інше: _____		

Індикатори компрометації		
Мережеві:		
IP/домен/URL/User Agent	Коментар	
Хостові:		
Шлях/команда/сервіс/заплановане завдання/гілка реєстру	Коментар	
Файлові:		
Хешсума файлу	Назва файлу	Коментар
MD5(приклад): [хешсума]		

Продовження додатка 6

Перелік отриманих даних		
Хешсума файлу	Назва файлу	Коментар
MD5(приклад): [хешсума]		

_____