ЗАТВЕРДЖУЮ

Заступник Міністра оборони України   
з питань цифрового розвитку, цифрових трансформацій і цифровізації

Катерина ЧЕРНОГОРЕНКО

“03” лютого 2024 року

ТИМЧАСОВИЙ ПОРЯДОК

реагування на інциденти кібербезпеки

в Управлінні інформаційних технологій та Центрі інновацій та розвитку оборонних технологій

1. 1. Вступ
   1. Тимчасовий порядок реагування на інциденти кібербезпеки в Управлінні інформаційних технологій та Центру інновацій та розвитку оборонних технологій (далі – Порядок) є документом що визначає вимоги до організації реагування на інциденти кібербезпеки (або кіберінциденти) в інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах (далі – ІКС), розпорядником яких є Управління інформаційних технологій (далі – УІТ) або Центр інновацій та розвитку оборонних технологій (далі - ЦІРОТ).
   2. Цей документ розроблений на основі Закону України “Про основні засади забезпечення кібербезпеки України”, постанови Кабінету Міністрів України   
      від 29 грудня 2021 року № 1426 “Про затвердження Положення   
      про організаційно-технічну модель кіберзахисту”, постанови Кабінету Міністрів України від 4 квітня 2023 року №299 “Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”, наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 3 липня 2023 року № 570 “Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі” та настанов NIST SP 800-61 “Computer Security Incident Handling Guide”.
2. Терміни та визначення
   1. У цьому Порядку терміни вживаються у такому значенні:

стандартна операційна процедура реагування на кіберінциденти (далі – стандартна операційна процедура або сценарій реагування) – документ, який визначає детальний порядок дій відповідальних осіб та/або команд   
щодо реагування на інциденти визначеного типу;

елемент ІКС– сервіси, комунікаційне обладнання, сервери, програмне   
або апаратне забезпечення, кінцеві пристрої тощо, що входять до складу ІКС;

дамп оперативної пам’яті – записаний у встановленому вигляді стан оперативної пам’яті елементу ІКС в певний момент часу з даними цього стану;

засіб захисту – засіб забезпечення захисту інформації або засіб кіберзахисту;

подія інформаційної безпеки – ідентифікований стан ІКС або її елементу,   
який вказує на можливе порушення політики безпеки або відмову засобів захисту, або інша, раніше невідома ситуація, яка може бути істотною   
для безпеки;

Операційний центр кібербезпеки (далі - ОЦК або SOC) – підрозділ відділу кібербезпеки та реагування на кіберінциденти ЦІРОТ, який здійснює виявлення кіберінцидентів та організацію заходів реагування на кіберінциденти.

Інші терміни вживаються в значеннях, наведених в Законі України   
“Про основні засади забезпечення кібербезпеки України”, постанові Кабінету Міністрів України від 29 грудня 2021 р. № 1426 “Про затвердження Положення про організаційно-технічну модель кіберзахисту”, постанові Кабінету Міністрів України від 4 квітня 2023 р. №299 “Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”.

1. Задачі
   1. Цей Порядок розроблений для вирішення наступних задач:

визначення основних етапів реагування на кіберінциденти в ІКС, розпорядником яких є УІТ або ЦІРОТ та ІКС, адміністрування та захист інформації яких виконує УІТ або ЦІРОТ;

визначення ролей та відповідальності учасників процесу реагування   
на кіберінциденти;

визначення правил класифікації кіберінцидентів;

визначення критичності кіберінцидентів та послідовності реагування   
на них.

* 1. Мета реагування на інциденти:

запобігання реалізації кіберінцидентів;

збереження або ефективне відновлення функціонування ІКС в разі реалізації кіберзагроз;

зниження частоти виникнення кіберінцидентів в ІКС.

* 1. Задачі реагування на інциденти кібербезпеки:

своєчасне виявлення кіберінцидентів;

реєстрація та облік кіберінцидентів;

збір та збереження електронних доказів;

організація заходів реагування на інциденти;

відновлення роботи ІКС в разі реалізації кіберзагроз.

1. Сфера застосування
   1. Дія цього Порядку розповсюджується на всі ІКС, розпорядником яких   
      є УІТ або ЦІРОТ та ІКС, адміністрування та захист інформації яких виконує УІТ або ЦІРОТ.
   2. Цей порядок є обов’язковим до виконання всіма підрозділами УІТ   
      та ЦІРОТ.
2. Підготовка та реагування на кіберінциденти
   1. Підготовка та реагування на кіберінциденти виконується силами кіберзахисту.
   2. Сили кіберзахисту складаються з:

служб захисту інформації (далі – СЗІ) ІКС;

адміністраторів ІКС;

SOC.

* 1. Задачі сил кіберзахисту розподіляються наступним чином:
     1. СЗІ ІКС:

здійснює заходи з ефективного захисту кіберпростору та протидії кібератакам;

організовує виконання заходів захисту інформації та кіберзахисту в ІКС;

організовує виконання заходів реагування на кіберінциденти в ІКС;

приймає участь в визначенні та погоджують заходи реагування   
на кіберінциденти в ІКС.

* + 1. Адміністратори ІКС:

забезпечує передачу подій інформаційної безпеки ІКС в систему збору   
та аналізу подій інформаційної безпеки;

здійснюють заходи з захисту інформації та кіберзахисту в ІКС;

здійснюють заходи з підготовки до реагування на кіберінциденти в ІКС;

здійснюють заходи з реагування на кіберінциденти;

здійснюють адміністрування засобів захисту.

* + 1. SOC:

здійснює постійний моніторинг кіберпростору для виявлення ознак кібератак та потенційних кіберзагроз;

здійснює постійний моніторинг подій інформаційної безпеки з метою виявлення кіберінцидентів;

організовує реагування на кіберінциденти;

визначає заходи реагування на кіберінциденти;

визначає причини та першоджерело кіберінциденту;

здійснює документування та облік кіберінцидентів;

здійснює адміністрування системи збору та аналізу подій інформаційної безпеки та системи реєстрації та управління кіберінцидентами.

* 1. Підготовка до реагування на кіберінциденти здійснюється шляхом вжиття заходів кіберзахисту, спрямованих на швидке виявлення кіберінцидентів   
     та захист від кіберзагроз. Вжиття заходів виконується силами кіберзахисту відповідно до визначених задач.

Заходи підготовки до реагування включають наступне:

впровадження засобів фільтрації мережевого трафіка (міжмережеві екрани);

впровадження засобів виявлення та запобігання вторгненням;

впровадження засобів захисту, в тому числі засобів захисту   
від зловмисного коду або шкідливого програмного забезпечення (далі – ШПЗ) та засобів реагування на інциденти;

регулярне оновлення сигнатур кібератак та антивірусних баз;

управління доступом до ІКС;

регулярне встановлення оновлень безпеки програмного забезпечення;

регулярне резервне копіювання конфігурацій ІКС та критичної інформації;

передача подій ІКС в систему збору та аналізу подій інформаційної безпеки;

періодичне перевірка периметру мереж та внутрішніх ресурсів   
для виявлення вразливостей програмного забезпечення;

моніторинг подій інформаційної безпеки;

тощо.

* 1. Перелік та послідовність заходів реагування залежать від типу та категорії кіберінциденту. Перелік, послідовність та відповідальні ролі за виконання заходів реагування визначаються в сценарії реагування.
  2. Для кожного типу кіберінциденту, в разі необхідності, розробляється окремий сценарій реагування. Сценарії реагування розробляються SOC, погоджується зі всіма виконавцями та затверджується начальником Управління інформаційних технологій.

У разі відсутності для зареєстрованого кіберінциденту затвердженого сценарію реагування послідовність та перелік заходів реагування визначаються типовою процедурою реагування на кіберінциденти (п.6 цього Порядку).

* 1. Для комунікації та взаємодії між SOC та СЗІ ІКС або черговими адміністраторами ІКС використовуються наступні канали комунікації:
* спільні чати або канали чергових змін SOC, СЗІ ІКС та адміністраторів ІКС у месенджері;
* персональні чати між черговими змін SOC, СЗІ ІКС та адміністраторів ІКС у месенджері;
* телефони;
* електронна пошта (групові або персональні адреси).

Інформація про кіберінцидент або задачі щодо реагування, що були отримані будь-яким каналом комунікації, є обов’язковою до опрацювання   
у визначений відповідним сценарієм реагування порядку та терміни (а у разі його відсутності п.6 цього Порядку).

1. Типова процедура реагування на кіберінциденти
   1. SOC здійснює постійний моніторинг подій інформаційної безпеки   
      в системі збору та аналізу подій інформаційної безпеки.

Для виявлення інциденту аналітики SOC аналізують:

події інформаційної безпеки, які згенеровані системою збору та аналізу подій;

повідомлення користувачів ІКС, які надійшли на адресу електронної пошти mil.cert@mod.gov.ua;

інформацію від інших суб’єктів забезпечення кібербезпеки.

* 1. При виявленні події інформаційної безпеки аналітик SOC аналізує виявлену подію, інші події та дані з різних ІКС, з метою підтвердження реалізації кіберінциденту.

В разі необхідності аналітик SOC уточнює інформацію та дані у СЗІ ІКС

* 1. Якщо в процесі аналізу підтверджується факт реалізації кіберінциденту,   
     то аналітик SOC реєструє кіберінцидент в системі реєстрації та управління кіберінцидентами.
  2. Аналітик SOC аналізує пов’язані з кіберінцидентом події та дані   
     для визначення джерела інциденту.

Якщо в ході аналізу інциденту аналітиком SOC визначені нові індикатори кіберзагроз, то вони публікуються аналітиком SОС в системі обміну інформацією про кіберзагрози (Malware Information Sharing Platform або MISP).

* 1. Аналітик SOC ідентифікує ІКС та/або елемент ІКС, в якому(яких)   
     був виявлений кіберінцидент та/або джерело кіберінциденту. Аналітик SOC ідентифікує підрозділ або контактну особу СЗІ ІКС.

Аналітик SOC інформує СЗІ ІКС про виявлений кіберінцидент та, у разі необхідності, спільно з СЗІ ІКС визначає елемент ІКС, в якому був виявлений кіберінцидент або який є першоджерелом кіберінциденту.

* 1. Аналітик SOC визначає тип та категорію кіберінциденту відповідно   
     до Таксономії інцидентів кібербезпеки, визначениій в Додатку 2.
  2. Аналітик SOC визначає критичність кіберінциденту відповідно   
     до Класифікації рівня критичності кіберінциденту, наведеної в Додатку 3.   
     У разі необхідності, аналітик SOC визначає рівень критичності кіберінциденту спільно з СЗІ ІКС.
  3. Аналітик SOC визначає перелік заходів, які необхідно виконати   
     для стримування кіберінциденту.

Заходи стримування можуть включати:

* ізоляція уражених систем, мережевих сегментів та пристроїв один   
  від одного та/або від систем і мережевих сегментів, які не були уражені;
* оновлення правил фільтрації мережевого трафіка на міжмережевих екранах;
* блокування несанкціонованого доступу, журналювання подій   
  щодо несанкціонованого доступу;
* блокування джерел поширення ШПЗ (в тому числі комп’ютерів, носіїв інформації, поштових шлюзів, web-сервісів тощо);
* 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 в разі потреби також   
  на неуражених системах/мережевих пристроях;
* блокування облікових записів користувачів, служб або застосунків;
* 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;
* створення образів операційної системи, носіїв інформації (дисків)   
  та/або оперативної пам’яті (далі – дампів), для збереження електронних доказів, та їх подальшого використання в рамках розслідування кіберінциденту;
* тощо.
  1. Аналітик SOC погоджує з СЗІ ІКС (у разі його відсутності з черговим адміністратором ІКС) перелік заходів, пріоритети, послідовність та строки   
     їх виконання. Строки виконання встановлюються аналітиком SOC в залежності від критичності та типу кіберінциденту.
  2. СЗІ ІКС (у разі його відсутності черговий адміністратор ІКС) організує виконання заходів стримування кіберінциденту адміністраторами ІКС   
     у визначені строки.
  3. Адміністратори ІКС після виконання заходів стримування кіберінциденту виконують заходи збору та збереження доказів, які були погоджені з СЗІ ІКС. Зібрані доказі передаються в SOC для подальшого аналізу.
  4. На основі аналізу кіберінциденту та пов’язаних з ним подій, результатів стримування та зібраних доказів аналітик SOC визначає першоджерело кіберінциденту та можливі наслідки кіберінциденту.
  5. Якщо при аналізі доказів не вдалось визначити першоджерело кіберінциденту, необхідно провести повторний аналіз обставин та зібраних доказів кіберінциденту для визначення першоджерела та виконати відповідні заходи стримування відповідно до пп.6.3-6.9 цього порядку.
  6. За результатами аналізу аналітик SOC спільно з СЗІ ІКС формує перелік заходів потрібних для усунення наслідків інциденту. Строки виконання встановлюються аналітиком SOC в залежності від критичності та типу кіберінциденту та погоджуються з СЗІ ІКС.

До заходів усунення наслідків кіберінциденту та відновлення працездатності ІКС відносяться наступні:

* перевірка усіх заражених середовищ (систем, мережевих сегментів, мережевих пристроїв, хостів, сховищ даних, тощо) на предмет вразливостей;
* повторне створення дампів елементів уражених середовищ;
* очищення систем від ШПЗ та/або його компонентів;
* відновлення систем використовуючи образи із системи резервного копіювання або до заводських налаштувань;
* часткове або повне відновлення технологічного, технічного, мережевого, іншого обладнання, що постраждало через інцидент, або його заміна   
  на нове;
* встановлення патчів та оновлень;
* зміну усіх паролів у скомпрометованих середовищах (системах/мережах);
* тощо.
  1. СЗІ ІКС організовує виконання заходів усунення наслідків кіберінциденту адміністраторами ІКС у визначені строки.
  2. Після виконання заходів усунення наслідків кіберінциденту адміністратори ІКС виконують заходи, необхідні для відновлення повноцінної роботи ІКС.

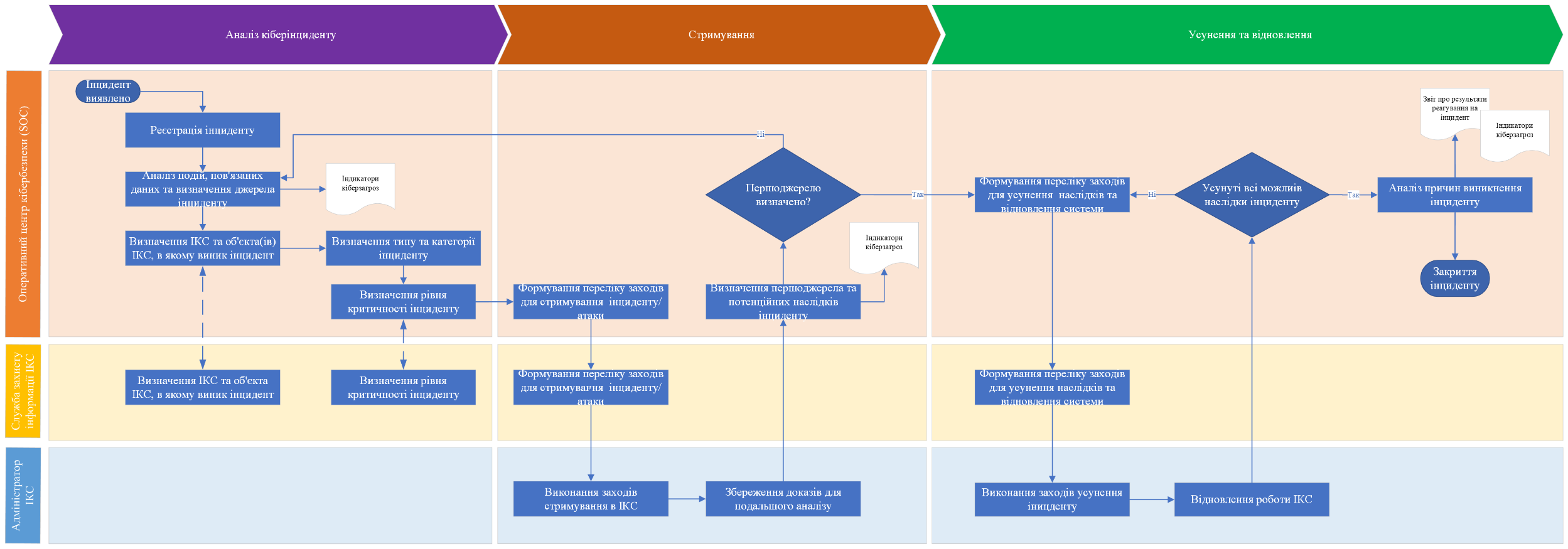
Заходи відновлення можуть включати:

* повторне підключення відновлених/нових систем до мереж;
* посилення безпеки периметра (наприклад, оновлення правил фільтрації трафіку на міжмережевих екранах, перегляд списків управління доступом до граничного маршрутизатора тощо);
* ретельне тестування систем, у тому числі виконання заходів безпеки;
* моніторинг дій щодо підозрілої поведінки;
* тощо.
  1. Якщо не всі можливі наслідки кіберінциденту було усунуто, то потрібно виконати повторний аналіз кіберінциденту та виконати відповідні заходи усунення наслідків кіберінциденту відповідно до пп. 6.10-6.13.
  2. Якщо всі можливі наслідки кіберінциденту було усунуто, то аналітик SOC проводить остаточний аналіз подій та даних, пов’язаних з кіберінцидентом.
  3. Якщо в процесі аналізу причин кіберінциденту були виявлені нові індикатори кіберзагроз, то аналітик SOC передає їх адміністраторам засобів захисту для застосування та публікації в системі обміну інформацією   
     про кіберзагрози (Malware Information Sharing Platform або MISP).
  4. Аналітик SOC визначає причини виникнення кіберінциденту, формує звіт про результати реагування на інцидент та закриває кіберінцидент в системі реєстрації та управління кіберінцидентами.

|  |  |
| --- | --- |
| Начальник відділу кібербезпеки та реагування на кіберінциденти Центру інновацій  та розвитку оборонних технологій |  |
| майор | Вадим НОВІКОВ |

Додаток 1

Блок-схема типової процедури реагування на інциденти кібербезпеки в ІКС



Додаток 2

Таксономія інцидентів кібербезпеки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код хх** | **Категорія інциденту** | **Код**  **хх** | **Тип інициденту** | **Опис типу інциденту** |
| 01. | Шкідливий (образливий) вміст (Abusive content) | 01 | Спам  (Spam) | Отримання небажаних повідомлень або великої кількості повідомлень (флуд) |
| 02. | Шкідливий  програмний  код (Malicious  Code) | 01 | Зараження шкідливим програмним забезпеченням (далі – ШПЗ)  (Malware infection) | У системі виявлено зловмисний комп’ютерний вірус  або зловмисний код. |
| 02 | Розповсюдження зловмисного коду  (Malware distribution) | Виявлені факти розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти,  що містять вкладення з ШПЗ або посилання на його завантаження |
| 03 | Командно-контрольний центр або C2  (Command & Control) | В ІКС виявлена 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 | Сніффінг  (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) |
| 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  (Information  Content  Security) | 01 | Несанкціонований доступ до інформації  (Unauthorised access to information) | Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації |
| 02 | Несанкціонована модифікація  (Unauthorised modification of information) | 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  *та не виправлених у встановлені строки* |
| 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 |

Додаток 3

Класифікація критичності інцидентів кібербезпеки

|  |  |  |
| --- | --- | --- |
| Рівень критичності | | Визначення |
| 0 | некритичний  (білий) | Інцидент не загрожує сталому, надійному та штатному режиму функціонування ІКС. Загроза/кібератака заблоковані засобами захисту. |
| 1 | низький  (зелений) | Інцидент безпосередньо загрожує сталому, надійному  та штатному режиму функціонуванню ІКС  або її елементу, але не загрожує виконанню функцій  та/або надання послуг МОУ, та/або захищеності (конфіденційності, цілісності і доступності) інформації, що ними обробляються. |
| 2 | середній  (жовтий) | Інцидент безпосередньо загрожує сталому, надійному  та штатному режиму функціонування ІКС, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації, що в ній обробляється, та/або виникають передумови для припинення виконання функцій  та/або надання послуг МОУ. |
| 3 | високий  (помаранчевий) | Інцидент безпосередньо загрожує сталому, надійному  та штатному режиму функціонування ІКС, порушується захищеність (конфіденційність, цілісність і доступність) інформації, що в ній обробляється, внаслідок чого виникають потенційні загрози для національної безпеки  і оборони, та/або виконання операцій сил оборону, припинення виконання функцій та/або надання послуг  в системі МОУ. |
| 4 | критичний  (червоний) | Інцидент безпосередньо загрожує сталому, надійному  та штатному режиму функціонування кількох ІКС, порушується захищеність (конфіденційність, цілісність  і доступність) інформації, що ними обробляються, внаслідок чого виникають реальні загрози  для національної безпеки і оборони, виконання операцій сил оборони.  Реагування на цьому рівні може потребувати залучення сил та засобів інших суб’єктів системи МОУ  та/або основних суб’єктів національної системи кібербезпеки. |
| 5 | надзвичайний  (чорний) | Інцидент безпосередньо загрожує сталому, надійному  та штатному режиму функціонування значної кількості ІКС МОУ, порушується захищеність (конфіденційність, цілісність і доступність) інформації, що в них обробляється, внаслідок чого виникають невідворотні загрози для повноцінного функціонування сектору безпеки та оборони держави, зрив операцій сил оборони або загроза життю громадян України. Інцидент може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів сил оборони та основних суб’єктів національної системи кібербезпеки та інших суб’єктів забезпечення кібербезпеки. |

Додаток 4

Пріоритет реагування на інциденти кібербезпеки

з однаковим рівнем критичності

|  |  |  |
| --- | --- | --- |
| **Пріоритет** | **Тип інциденту** | |
| 1 | 05. | Втручання (Intrusion) |
| 2 | 06. | Порушення доступності (Availability) |
| 3 | 07. | Порушення властивостей інформації (Information Content  Security) |
| 4 | 02. | Шкідливий програмний код (Malicious Code) |
| 5 | 04. | Спроби втручання (Intrusion Attempts) |
| 6 | 09. | Відома вразливість (Vulnerable) |
| 7 | 03. | Збір інформації зловмисником (Information Gathering) |
| 8 | 08. | Шахрайство (Fraud) |
| 9 | 01. | Шкідливий (образливий) вміст (Abusive content) |
| 10 | 10. | Інше (Other) |