Реагування на інциденти безпеки інформації

План лекції

Вступ
1. Система управління інформаційною безпекою
2. Управління інцидентами інформаційної безпеки
3. Реагування на інциденти інформаційної безпеки
Висновки

Рекомендована література

Основна

1. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Навчальний посібник для учасників тренінгу «Розробка та впровадження системи управління безпекою інформації». К.: ВАІТЕ, 2021. 138 с.

Допоміжна

2. 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).
3. ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT).
4. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling. Guide Recommendations of the National Institute of Standards and Technology. 79 p. (Aug. 2012).

Інформаційні ресурси в Інтернеті

5. http://dx.doi.org/10.6028/NIST.SP.800-61r2.
6. https://www.enisa.europa.eu/topics/incident-response.
7. https://learn.microsoft.com/en-us/security/operations/incident-response-overview.
8. https://www.techtarget.com/searchsecurity/tip/Incident-response-best-practices-for-your-organization.
9. https://www.incidentresponse.org/playbooks/.

Текст лекції

Вступ

Реалізація загроз (ризиків) інформаційної безпеки через наявні вразливості інформаційних систем призводить до впливу на інформаційні активи, що забезпечують діяльність організації, і при цьому система захисту інформації або система управління інформаційною безпекою має фіксувати події, які можуть бути квафіковані як інциденти інформаційної безпеки, що впливають на інформаційну діяльність організації (рис. 1).

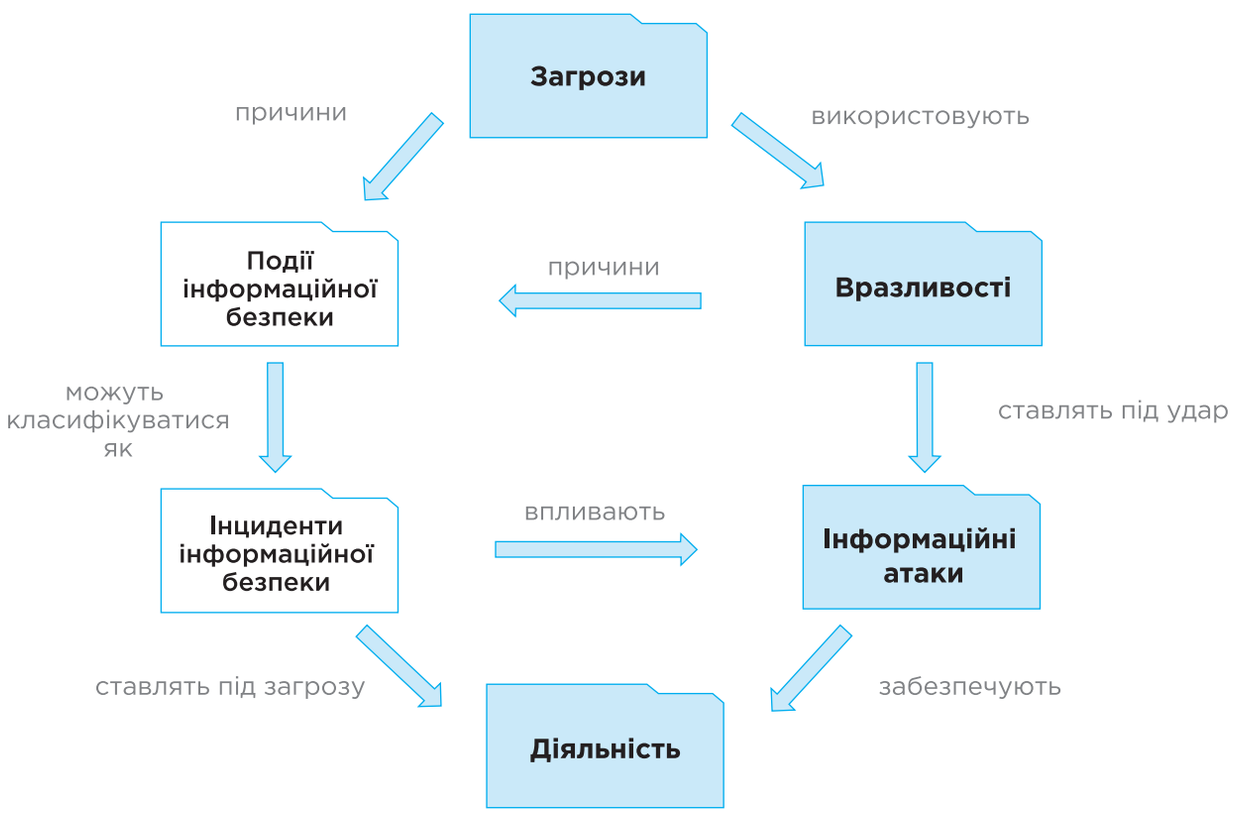

Рис. 1. Взаємозв'язок понять при виникненні інцидентів інформаційної безпеки за ДСТУ ISO/IEC 27035-1:2018

Реагування на інциденти інформаційної безпеки як системний процес є складовою системи управління інформаційною безпекою.

1. Система управління інформаційною безпекою

Закон України «Про захист інформації в інформаційно-комунікаційних системах» в ч. 2 ст. 8 визначає як умову обробки державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, застосування *комплексної системи захисту інформації* з підтвердженою відповідністю.

Відповідно до ч. 4 ст. 8 цього Закону державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі ***без*** *застосування комплексної системи захисту інформації* у разі виконання **всіх** таких умов:

- підтвердження відповідності *системи управління інформаційною безпекою* за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;
- використання для захисту інформації в системі *засобів криптографічного захисту інформації, які мають позитивний експертний висновок* за результатами державної експертизи у сфері криптографічного захисту інформації;
- жоден з елементів системи не може бути *розташований на територіях* України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами;
- *виконання особливих вимог,* встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Серія стандартів ДСТУ ISO/IEC 27xxx регламентує побудову та підтримання функціонування систем управління інформаційної безпеки (СУІБ).

Етапи побудови СУІБ у загальному вигляді можна представити так:

- *визначення сфери дії* СУІБ;
- *попередня перевірка відповідності* системи безпеки організації вимогам стандарту ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». На цьому етапі можуть бути застосовані й інші стандарти, у тому числі ДСТУ ISO/IEC 27004:2018 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання»;

- *оцінка ризиків інформаційної безпеки,* де основою для вибору відповідної методики є стандарт ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки»;
- *опис процедур та їх документування.* На цьому етапі описуються процеси у сфері управління та забезпечення безпеки, які потрібно виконати, а також формується відповідна документація;
- *впровадження процедур та відповідної документації;*
- *дослідна експлуатація* СУІБ;
- *сертифікація,* яка проводиться у формі аудиту, за результатами якого організація має отримати сертифікат про відповідність СУІБ вимогам ДСТУ ISO/IEC 27001:2015.

Для управління інформаційною безпекою у випадках реалізації ризиків, які призвели до виникнення інцидентів, з метою ефективного відновлення інформаційної безпеки, поширення інформації про події безпеки та слабкі місця (вразливості) згідно з ДСТУ ISO/IEC 27002:2015 необхідно впровадження підсистеми **управління інцидентами інформаційної безпеки та вдосконалення СУІБ.**

2. Управління інцидентами інформаційної безпеки

Реагування на інциденти інформаційної безпеки здійснюється в рамках управління інцидентами інформаційної безпеки та вдосконалення СУІБ, що передбачає наступні заходи безпеки:

a) визначення відповідальності керівництва організації та процедур реагування на інциденти інформаційної безпеки;
b) звітування про події інформаційної безпеки;
c) звітування щодо виявлених недоліків та вразливостей системи інформаційної безпеки;
d) оцінка подій інформаційної безпеки та прийняття рішень стосовно віднесення їх до інцидентів інформаційної безпеки;
e) реагування на інциденти інформаційної безпеки відповідно до встановлених процедур;
f) аналіз і зіставлення інцидентів інформаційної безпеки для визначення потреб у вдосконаленні або впровадженні додаткових заходів безпеки СУІБ;
g) ідентифікація, збирання, отримання і зберігання доказів для притягнення винних до різних видів юридичної відповідальності.

Визначення відповідальності керівництва щодо управління інцидентами інформаційної безпеки потрібно для забезпечення **розроблення та поширення** належним чином всередині організації **процедур:**

1) планування та підготовки реагування на інцидент;
2) моніторингу, виявлення, аналізу та звітування про події та інциденти інформаційної безпеки;

3) реєстрації діяльності щодо управління інцидентами;
4) збирання про інциденти інформації, яка може бути визнана в судовому процесі як доказ;
5) оцінювання й прийняття рішення щодо подій інформаційної безпеки та оцінювання слабких місць інформаційної безпеки;
6) реагування на інцидент, відновлення після інциденту, інформування зацікавлених сторін.

Визначені **процедури реагування на інциденти інформаційної безпеки** мають забезпечувати, що:

1) компетентний персонал всередині організації може реагувати на інциденти інформаційної безпеки;
2) запроваджена точка контакту (інформаційний канал) для звітування про виявлені інциденти інформаційної безпеки;
3) підтримуються відповідні комунікації з регуляторними органами та зовнішніми групами (центрами) з аналізу інцидентів інформаційної безпеки.

Процедури звітування мають включати:

1) шаблони звітів про події інформаційної безпеки;
2) процедури негайного реагування в разі події інформаційної безпеки, наприклад:
   a) реєстрація типу події: порушення чи відмова;
   b) реєстрація повідомлення на екрані;
   c) негайна реєстрація в точці контакту і тому подібне;
3) посилання на порядок дисциплінарного провадження стосовно працівників, які вчинили порушення безпеки;
4) порядок доведення до працівників, які повідомили про подію інформаційної безпеки, результатів реагування та аналізу події.

Звітування про події інформаційної безпеки повинно здійснюватися через визначені належні канали управління. Всі працівники організації та підрядники повинні бути поінформовані про їх відповідальність щодо якнайшвидшого звітування про будь-які події інформаційної безпеки через точку контакту за визначеними процедурами.

Подіями інформаційної безпеки, що потребують звітування, є:

a) неефективність заходів безпеки;
b) порушення цілісності, конфіденційності або очікуваної доступності;
c) людські помилки;
d) невідповідності політиці чи настановам;
e) порушення заходів фізичної безпеки;
f) несанкціоновані зміни системи;
g) збій програмного забезпечення чи апаратних засобів;
h) порушення доступу.

Звітуванню також підлягають будь-які виявлені або очікувані слабкі (вразливі) місця у системах чи послугах, що, відповідно, є **слабкими місцями інформаційної безпеки.** Процес звітування має бути якомога простішим, доступнішим і досяжним.

Необхідно попередити працівників та підрядників про заборону тестування слабких місць і розцінювання таких дій як потенційне зловживання системою, що тягне юридичну відповідальність.

Події інформаційної безпеки, інформація про які надходить через відповідну точку (місце) контакту до окремої команди реагування на інциденти інформаційної безпеки (ISIRT), мають бути **оцінені** за допомогою попередньо узгодженої кваліфікації **та прийнято рішення** стосовно **віднесення їх до інцидентів інформаційної безпеки.** Кваліфікація та пріоритизація подій і інцидентів допоможе оцінити їх вплив на стан безпеки організації. Результати оцінювання та прийняття рішення мають бути докладно записані для подальшої їх перевірки й посилання на них.

Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до визначених процедур і включати:

a) якнайшвидше збирання доказової інформації (цифрових слідів) для встановлення фактичних обставин та наслідків події;
b) за потреби – проведення криміналістичного дослідження зібраних доказових даних;
c) за потреби (якщо інцидент продовжує розвиватися) – ескалацію зусиль щодо зупинки небезпечних подій і відновлення безпеки;
d) забезпечення документування (реєстрації) всієї діяльності реагування на інцидент інформаційної безпеки;
e) інформування у визначених межах про існування інциденту всіх зацікавлених сторін, які мають знати про це;
f) ідентифікацію слабких місць (вразливостей) інформаційної безпеки, які були причиною або сприяли появі інциденту;
g) формальне закриття та звітування про інцидент по завершенні реагування.

Основною метою реагування на інцидент є повернення до вихідного рівня стану інформаційної безпеки.

Докладні настанови стосовно управління інцидентами інформаційної безпеки викладено в ДСТУ ISO/IEC 27035.

Після формального закінчення реагування на інцидент має бути проведений **аналіз** і зіставлення з іншими інцидентами інформаційної безпеки **для визначення потреб у вдосконаленні** або впровадженні додаткових заходів безпеки СУІБ. Для цього повинні бути механізми, які дозволяють кількісно оцінити й відслідкувати типи, обсяги й вартість інцидентів інформаційної безпеки.

За результатами аналізу інцидентів можна розробити типові сюжети подій інформаційної безпеки організації й використовувати їх у навчанні користувачів з питань безпеки.

Організація повинна **визначити** і при реагуванні на інциденти інформаційної безпеки використовувати **процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази** для притягнення до юридичної відповідальності осіб, які вчинили правопорушення у сфері інформаційної безпеки.

Процедури ідентифікації, збирання, отримання і зберігання доказів мають передбачати різні типи інформаційного середовища, обладнання, стану обладнання (наприклад, увімкнено чи вимкнено) і включати питання:

a) засторог на місці інциденту;
b) убезпечення потенційних цифрових доказів;
c) убезпечення персоналу;
d) ролей та відповідальності персоналу, якого стосуються пов'язані із доказами процеси;
e) компетентності персоналу, якого стосуються пов'язані із доказами процеси;
f) хронологічного документування виконуваних дій стосовно потенційних цифрових доказів;
g) інструктажу персоналу, якого стосуються пов'язані із доказами процеси.

Для посилення значущості й довіри до збережених потенційних цифрових доказів доречно розглянути можливі засоби підтвердження кваліфікації персоналу, наприклад, у вигляді сертифікації.

Потенційні цифрові докази інциденту можуть знаходитися за межами комп'ютерних систем організації та/або в інших юрисдикціях, тому необхідно враховувати вимоги як вітчизняного законодавства, так і інших юрисдикцій щодо повноважень зі збирання та отримання цифрових доказів за межами організації.

При неочевидності правової кваліфікації виявленої події інформаційної безпеки для збереження допустимості й належності в можливому судовому процесі потенційних доказів доцільно одразу залучати до розслідування представника юридичного відділу організації та правоохоронні органи.

Докладно процедури ідентифікації, збирання, отримання та зберігання цифрових доказів описано в настановах ДСТУ ISO/IEC 27037.

Прийняті державні стандарти України, які або безпосередньо регламентують управління інцидентами інформаційної безпеки, або впливають на цю діяльність, зазначені в ДСТУ ISO/IEC 27035-1:2018 через класифікацію фаз процесу розслідування інцидентів (рис. 2).

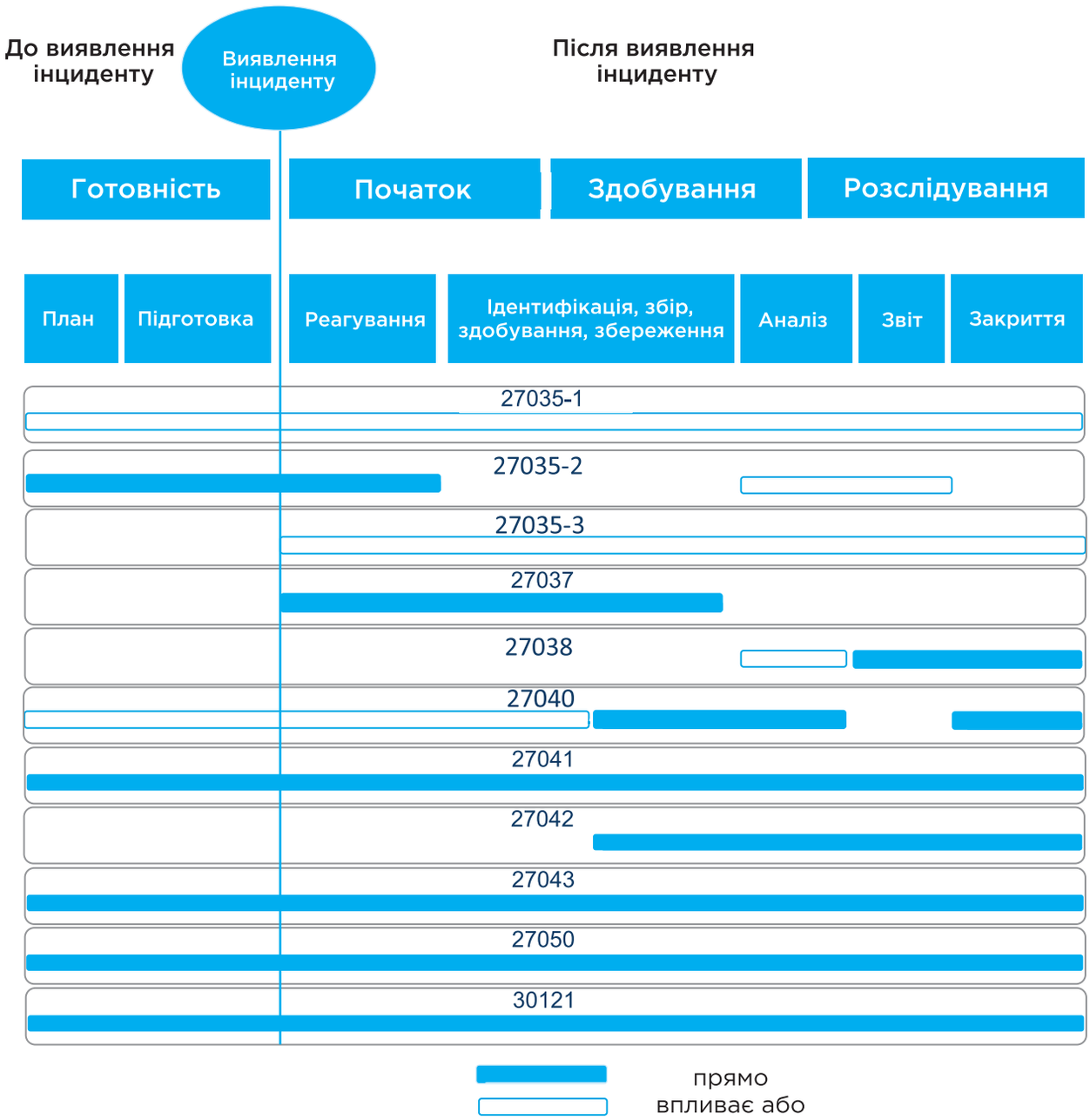

Рис. 2. ДСТУ ISO/IEC, які або безпосередньо регламентують управління інцидентами інформаційної безпеки, або впливають на цю діяльність

3. Реагування на інциденти інформаційної безпеки

Процес реагування на інциденти в кожній організації може відрізнятися залежно від організаційної структури, можливостей і накопиченого досвіду. Під час інциденту важливо наступне.

- **Зберігати спокій.** Інциденти можуть викликати надзвичайні емоції, які можуть завадити діяти відповідним чином. Потрібно зосередитись на слідуванні визначеним процедурам реагування.
- **Не завдавати шкоди.** Необхідно переконатись, що встановлені процедури реагування та їх виконання дозволяє уникнути втрати даних, критично важливих функцій інформаційної системи та доказів. Потрібно уникати дій, які можуть зашкодити відтворенню хронології подій, встановленню причин, а в подальшому – вдосконаленню системи захисту.
- **Залучати юридичний відділ (юриста).** Потрібна юридична кваліфікація інциденту як можливого правопорушення, яке потребує залучення правоохоронних органів і відповідного планування розслідування та процедур відновлення.
- **Обережно оприлюднювати інформацію про інцидент.** Поширення інформації про інцидент можливе тільки після узгодження з юридичним відділом (юристом).
- **За потреби отримувати допомогу.** При складних атаках потрібне залучення фахівців з глибокими знаннями та досвідом.

Слід зосередитися на тому, щоб була готовність до реагування на інциденти, які використовують поширені вектори атак, наприклад:

- **зовнішні/знімні носії.** Атака, що виконується зі знімного носія (наприклад, флешки, компакт-диска) або периферійного пристрою;
- **виснаження.** Атака, яка використовує методи «грубої сили» для компрометації, деградації або знищення систем, мереж або служб;
- **веб.** Атака, що виконується з веб-сайту або веб-додатку;
- **електронна пошта.** Атака, що виконується за допомогою електронного повідомлення або вкладення;
- **неналежне використання.** Будь-який інцидент, спричинений порушенням політики прийнятного використання організації авторизованим користувачем, за винятком вищезазначених категорій;
- **втрата або крадіжка обладнання.** Втрата або крадіжка комп'ютерного пристрою або носія інформації, що використовується організацією, наприклад, ноутбука або смартфона;
- **інше.** Атака, яка не підпадає під жодну з інших категорій.

Процедури реагування розроблюються на визначені типи інцидентів інформаційної безпеки для ISIRT і користувачів із задокументованими процесами та пов'язаними з ними обов'язками та розподілом ролей між призначеними особами для виконання різних видів діяльності (окремій особі може бути призначено більше однієї ролі, залежно від розміру, структури та характеру діяльності організації), наприклад, включаючи наступне:

- відключення ураженої системи, служби та/або мережі за певних обставин, що узгоджується за попередньою домовленістю з відповідним керівництвом IT та/або організації;

- залишення ураженої системи, служби та/або мережі підключеною та працюючою;
- моніторинг даних, що надходять від, до та всередині ураженої системи, служби та/або мережі;
- активація звичайних процедур резервного копіювання та управління кризами відповідно до політики безпеки системи, служби та/або мережі;
- здійснення моніторингу та забезпечення збереження електронних доказів, які потрібні для притягнення винних до дисциплінарної або іншої відповідальності;
- повідомлення деталей інциденту інформаційної безпеки визначеним внутрішнім і зовнішнім зацікавленим сторонам, наприклад, іншим групам реагування на інциденти та організаціям, інтернет-провайдерам, постачальникам програмного забезпечення, правоохоронним органам, клієнтам, ЗМІ та ін. Усі контакти та комунікації із зовнішніми сторонами мають бути задокументовані.

Найскладнішою частиною процесу реагування на інциденти є точне виявлення та оцінка можливих інцидентів – визначення того, чи стався інцидент, і якщо так, то який тип, ступінь і масштаб проблеми. Це завдання ускладнюється поєднанням трьох факторів:

- інциденти можуть бути виявлені за допомогою багатьох різних засобів, з різним рівнем деталізації та точності. Автоматизовані засоби виявлення включають мережеві та хостові системи виявлення вторгнень, антивірусне програмне забезпечення та аналізатори журналів. Про інциденти можуть повідомити користувачі. Деякі інциденти мають явні ознаки, які можна легко виявити, тоді як інші виявити майже неможливо;
- кількість потенційних ознак інцидентів, як правило, досить велика, наприклад, нерідко від сенсорів виявлення вторгнень надходить тисячі або навіть мільйони сповіщень на день;
- для ефективного аналізу даних, пов'язаних з інцидентами, необхідні глибокі спеціалізовані технічні знання та досвід.

Ознаки інциденту поділяються на дві категорії: *провісники (precursors) та індикатори (indicators).* **Провісник** – це ознака того, що інцидент може статися в майбутньому. **Індикатор** – це ознака того, що інцидент міг статися або може відбуватися зараз.

Більшість атак не мають жодних провісників, які можна було б ідентифікувати або виявити відносно цілі. Якщо провісники виявлені, організація може запобігти інциденту, змінивши політику безпеки. Прикладами провісників є:

- записи журналу веб-сервера, які свідчать про використання сканера вразливостей;
- анонс на спеціалізованих ресурсах нового експлойту, який експлуатує вразливість поштового сервера організації;
- погрози здійснити атаку на організацію.

У той час, як провісники зустрічаються відносно рідко, індикатори є дуже поширеним явищем. Існує безліч різних індикаторів, серед яких можна зазначити такі:

- сенсор системи виявлення мережевих вторгнень сповіщає про спробу переповнення буфера на сервері бази даних;
- антивірусне програмне забезпечення сповіщає про виявлення шкідливої програми;
- системний адміністратор бачить ім'я файлу з незвичними символами;
- у журналі аудиту з'являється запис зміни конфігурації хосту;
- у журналі аудиту застосунку зареєстровано кілька невдалих спроб входу з незнайомої віддаленої системи;
- адміністратор електронної пошти бачить велику кількість заблокованих листів з підозрілим вмістом;
- мережевий адміністратор помічає незвичне відхилення потоків мережевого трафіку від типових значень.

Основними джерелами провісників і індикаторів є:

- сповіщення спеціалізованих застосунків (IDPS, SIEM, антивіруси та ін.);
- записи журналів аудиту застосунків і сервісів операційних систем;
- мережевий трафік;
- публічна інформація про знайдені вразливості та розроблені експлойти;
- звіти внутрішніх користувачів організації та користувачів інших організацій.

Приклад шаблону звіту про події інформаційної безпеки наведений в табл. 1.

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
1. Дата події	3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)
2. Номер події (надається фахівцем ISIRT)	
4. РЕКВІЗИТИ ОСОБИ, ЯКА ЗВІТУЄ	
4.1. Ім'я та прізвище	4.2. Адреса
4.3. Організація	4.4. Відділ
4.5. Телефон	4.6. E-mail
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
5.1. Опис події: • Що сталося • Яким чином сталося • Чому так сталося • Які компоненти/активи піддались впливу • Оцінка впливу на діяльність організації • Будь-які виявлені вразливості	

6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
6.1. Дата та час події	
6.2. Дата та час виявлення події	
6.3. Дата та час повідомлення про подію	
6.4. Чи відповідь на цю подію усунула небезпеку?	ТАК ☐ НІ ☐ (позначте відповідне)
6.5. Якщо так. вкажіть, скільки часу тривала подія (у днях/годинах/хвилинах)	

Контрольний список реагування на інцидент (Incident Handling Checklist) у табл. 2 містить основні кроки реагування, які можуть відрізнятися залежно від інциденту. Наприклад, якщо відомо про те, що сталося, на основі аналізу індикаторів (1.1), може і не виникнути необхідності виконувати (1.2) або (1.3)

Таблиця 2. Контрольний список реагування на інцидент

	ДІЯ	ВИКОНАНО
	ВИЯВЛЕННЯ ТА АНАЛІЗ	
1.	Визначення факту інциденту	
1.1.	Аналіз провісників та індикаторів	
1.2.	Пошук відповідної інформації	
1.3.	Проведення досліджень (наприклад, пошукові системи, база знань)	
1.4.	Якщо має місце інцидент, то розпочати документування, розслідування та збирання доказів	
2.	Визначення пріоритетності реагування на основі відповідних факторів (функціональний і інформаційний вплив, зусилля з відновлення тощо)	
3.	Доведення інформації про інцидент до відповідного внутрішнього персоналу та зовнішніх організацій	
	ЛОКАЛІЗАЦІЯ, ЛІКВІДАЦІЯ ТА ВІДНОВЛЕННЯ	
4.	Здобуття, збереження, убезпечення та документування доказів	
5.	Локалізація інциденту	
6.	Ліквідація інциденту	
6.1.	Виявлення та усунення всіх вразливостей, які були використані	
6.2.	Видалення шкідливого програмного забезпечення, невідповідних даних та інших компонентів	
6.3.	Якщо виявлено більше уражених вузлів (наприклад, нові зараження шкідливим програмним забезпеченням), повтор кроків **Виявлення та аналізу** (1.1, 1.2), а потім – **Локалізація** (5) та **Ліквідація** (6) інциденту	

	ДІЯ	ВИКОНАНО
	ЛОКАЛІЗАЦІЯ, ЛІКВІДАЦІЯ ТА ВІДНОВЛЕННЯ	
7.	Відновлення після інциденту	
7.1.	Повернення уражених систем до стану операційної готовності	
7.2.	Підтвердження, що уражені системи функціонують нормально	
7.3.	За потреби – здійснення додаткового моніторингу для визначення подальших дій, пов'язаних з інцидентом	
	ДІЯЛЬНІСТЬ ПІСЛЯ ІНЦИДЕНТУ	
8.	Складання звіту про інцидент та плану подальших дій	
9.	Проведення наради з вивчення отриманих висновків (обов'язкова для великих інцидентів, необов'язкова в інших випадках)	

Висновки

Реагування на інциденти інформаційної безпеки як системний процес є складовою системи управління інформаційною безпекою.

Найскладнішою частиною процесу реагування на інциденти є точне виявлення та оцінка можливих інцидентів – визначення того, чи стався інцидент, і якщо так, то який тип, ступінь і масштаб проблеми.

Ознаки інциденту поділяються на дві категорії: *провісники (precursors) та індикатори (indicators).*

Основними джерелами провісників і індикаторів є:

- сповіщення спеціалізованих застосунків (IDPS, SIEM, антивіруси та ін.);
- записи журналів аудиту застосунків і сервісів операційних систем;
- мережевий трафік;
- публічна інформація про знайдені вразливості та розроблені експлойти;
- звіти внутрішніх користувачів організації та користувачів інших організацій.