NIST

Національний інститут стандартів і технологій
Міністерство торгівлі США

Спеціальне видання стандарту (SP) 800-61
Друга редакція

Керівні настанови щодо управління інцидентами, пов’язаними з комп’ютерною безпекою

Рекомендації Національного інституту стандартів і технології США

Пол Чіхонскі
Том Мілар
Тім Гранс
Карен Скарфоне

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Спеціальне видання стандарту NIST (SP) 800-61 Друга редакція

Керівні настанови щодо управління інцидентами, пов’язаними з комп’ютерною безпекою

Рекомендації Національного інституту стандартів і технології США

Пол Чіхонскі
Відділення комп'ютерної безпеки, Лабораторія інформаційних технологій
Національний інститут стандартів і технологій США, Гейтесбург, штат Меріленд

Том Мілар
Комп’ютерна команда екстреної готовності Сполучених Штатів, Відділення національної кібербезпеки
Міністерство національної безпеки (Департамент внутрішньої безпеки)

Тім Гранс
Відділення комп'ютерної безпеки, Лабораторія інформаційних технологій
Національний інститут стандартів і технологій США, Гейтесбург, штат Меріленд

Карен Скарфоне
Компанія «Scarfone Cybersecurity»

http://dx.doi.org/10.6028/NIST.SP.800-

КОМП’ЮТЕРНА БЕЗПЕКА

Серпень 2012 року

Міністерство торгівлі США

Ребекка Бланк, в.о. Міністра торгівлі США

Національний інститут стандартів і технологій США

Патрік Д. Галлахер,
заступник Міністра торгівлі США та директор Національного інституту стандартів і технологій

Звіти про технології комп’ютерних систем

Лабораторія інформаційних технологій (ITL) при Національному інституті стандартів і технологій США сприяє розвитку економіки США та покращенню добробуту населення шляхом технічного управління інфраструктурою країни у сфері обчислень і стандартизації. ITL розробляє тести, методи тестувань, нормативні дані, проводить дослідно-експериментальні роботи й виконує технічний аналіз із метою забезпечення розроблення та продуктивного використання інформаційних технологій. Серед обов'язків ITL – розроблення управлінських, адміністративних, технічних і фізичних стандартів та рекомендацій / керівних настанов щодо раціонального убезпечення та захисту даних у Федеральних інформаційних системах, які не належать до інформації, пов'язаної з державною безпекою. У спеціальному виданні звітів серії 800 описуються науково-дослідницька діяльність ITL, керівні настанови та роз'яснювальна діяльність, присвячені інформаційній безпеці, а також окреслюється співпраця із промисловістю, урядом та науковими організаціями.

Уповноважений орган, що видав документ

Це видання було створено NIST в рамках його обов'язків, передбачених Федеральним законом США про управління інформаційною безпекою (FISMA), Публічний закон (P.L.) 107-347. NIST відповідає за розроблення стандартів та керівних настанов у сфері інформаційної безпеки, включаючи мінімальні вимоги до Федеральних інформаційних систем, але такі стандарти й настанови не застосовуються до національних систем безпеки без отримання окремого погодження від компетентних посадових осіб Федеральних органів, які керують роботою таких систем. Ці керівні настанови відповідають вимогам Директиви A-130, виданої Відділом із питань управління та бюджету (OMB), Розділ 8b(3), *Убезпечення інформаційних систем відомств та агентств*, котрі проаналізовано в Директиві A-130, Додаток IV: *Аналіз ключових розділів*. Додаткову інформацію надано у Директиві A-130, Додаток III, *Безпека федеральних автоматизованих інформаційних ресурсів*.

Жодне положення цього видання не може розглядатись як таке, що суперечить стандартам та настановам, обов'язковим до виконання Федеральними органами відповідно до вповноваженого рішення Міністра торгівлі. Крім того, ці настанови не можуть розглядатись як такі, що змінюють або замінюють чинні повноваження Міністра торгівлі, начальника OMB або іншої посадової особи Федерального органу. Це видання може використовуватися недержавними організаціями на добровільній основі, і на нього не поширюється дія авторського права на території Сполучених Штатів Америки. Проте, NIST буде вдячний за посилання на автора.

Спеціальне видання стандарту 800-61 Національного інституту стандартів і технологій США Друга редакція Нац. ін-т. станд. технол. Спец. публ. 800-61, Друга редакція, 79 сторінок (серпень 2012 року) CODEN: NSPUE2

http://dx.doi.org/10.6028/NIST.SP.800-

Зауваження щодо цього видання можна подавати за адресою:

Національний інститут стандартів і технологій США
До уваги: Відділення комп'ютерної безпеки, Лабораторія інформаційних технологій, 100 Б'юро Драйв (Внутрішній поштовий код 8930), Гейтесбург, штат Меріленд 20899-8930

Стислий виклад змісту

Реагування на інциденти, пов’язані з комп’ютерною безпекою, стало важливою складовою програм інформаційних технологій (IT). Оскільки ефективне реагування на інциденти – це складний процес, створення успішного потенціалу реагування на інциденти вимагає значного планування та ресурсів. Це видання допомагає організаціям у створенні потенціалу реагування на інциденти, пов’язані з комп’ютерною безпекою, а також в ефективному та результативному управлінні інцидентами. Це видання містить рекомендації щодо управління інцидентами, зокрема щодо аналізу даних, пов’язаних із інцидентом, та визначення відповідного алгоритму реагування на кожен інцидент. Цих керівних настанов можна дотримуватися незалежно від певних апаратних платформ, операційних систем, протоколів або застосунків.

Ключові слова

інцидент, пов’язаний з комп'ютерною безпекою; управління інцидентами; реагування на інцидент; інформаційна безпека

Подяка

Автори, Пол Чіхонскі з Національного інституту стандартів і технологій (NIST), Том Мілар з Комп'ютерної команди екстреної готовності Сполучених Штатів (US-CERT), Тім Гранс з NIST і Карен Скарфоне з компанії «Scarfone Cybersecurity» хочуть подякувати своїм колегам, які переглядали проєкти цього документа та зробили свій внесок до його технічного змісту, зокрема Джону Банхарту з NIST; Браяну Аллену, Марку Остіну, Браяну де Вінгерту, Ендрю Фуллеру, Крісу Халленбеку, Шерону Кіму, Мішелю Квону, Лі Року, Ріхарду Штрузе та Ренді Вікерсу з US-CERT; а також Маркосу Осорно з Лабораторії прикладної фізики Університету Джонса Гопкінса. Особливі слова подяки автори висловлюють Бренту Логану з US-CERT за його допомогу із графікою. Автори також хочуть подякувати експертам з безпеки Саймону Берсону, Антону Чувакіну (компанія «Gartner»), Фреду Коену (компанія «Fred Cohen & Associates»), пану Маріано М. дель Ріо (компанія «SIClabs»), Джейку Евансу (компанія «Tripwire»), Уолтеру Хаузеру (Орган регулювання соліситорів [SRA]), Паносу Кампанакісу (компанія «Cisco»), Кетлін Моріарті (корпорація «EMC»), Девіду Шваленбергу (Агентство національної безпеки) і Уесу Янгу (Центр обміну й аналізу інформації в рамках дослідницько-навчального нетворкінгу [REN-ISAC]), а також представникам корпорації «Blue Glacier Management Group», Центрам із контролю та профілактики захворювань, Міністерству енергетики США, Державному департаменту США та Федеральному авіаційного управлінню США за їхні особливо цінні коментарі та пропозиції.

Автори також хочуть висловити вдячність особам, котрі долучилися до створення попередніх редакцій цього видання. Особливу подяку автори висловлюють Браяну Кіму з компанії «Booz Allen Hamilton», який є співавтором оригінальної редакції; Келлі Мейсон з компанії «Blue Glacier Management Group», яка була співавторкою першої редакції; а також Ріку Аєрсу, Чаду Блумквісту, Вінсенту Ху, Пітеру Меллу, Скотту Роузу, Муруджі Супайї, Гері Стоунбернеру та Джону Уеку з NIST; Дону Бенаку і Майку Вітту з US-CERT; а також Дебрі Беннінг, Піту Коулману, Алексіс Ферінга, Трейсі Гласс, Кевіну Кулкіну, Браяну Лерду, Крісу Мантойфелю, Рону Річі та Марку Стівенсу з компанії «Booz Allen Hamilton» за надану ними важливу й цінну допомогу під час написання документа, а також Рону Банерджі та Джину Шульцу за роботу над попереднім проєктом документа. Автори також хочуть висловити свою подяку експертам з безпеки Тому Бакстеру (NASA), Марку Брюну (Університет Індіани), Браяну Керрієру (CERIAS, Університет Пердью), Еогану Кейсі, Джонні Девісу-молодшому (Міністерство у справах ветеранів США), Джиму Дункану (корпорація «BB&T»), Діну Фаррінгтону (банк «Wells Fargo»), Джону Хейлу (Університет Талси), Джорджії Кілкрес (Координаційний центр CERT [CERT®/CC]), Барбарі Ласвелл (CERT®/CC), Паскалю Меньє (CERIAS, Університет Пердью), Джеффу Мерфі (Університет штату Нью-Йорк у Баффало), Тодду О'Бойлу (MITRE), Марку Роджерсу (CERIAS, Університет Пердью), Стіву Ромігу (Університет штату Огайо), Робін Руфл (CERT®/CC), Джину Шульцу (Національна лабораторія ім. Лоуренса в Берклі), Майклу Сміту (US-CERT), Холту Соренсону, Юджину Спаффорду (CERIAS, Університет Пердью), Кену ван Віку і Марку Зайчеку (CERT®/CC), а також представникам Міністерства фінансів США за їхні особливо цінні коментарі та пропозиції.

Зміст

Зміст **6**

Перелік рисунків **8**

Перелік таблиць **9**

Преамбула **1**

1. Вступ **5**
1.1 Уповноважений орган, що видав документ 5
1.2 Мета і сфера застосування 5
1.3 Цільова аудиторія 5
1.4 Структура документа 5

2. Розбудова потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою **7**
2.1 Події та інциденти 7
2.2 Необхідність реагування на інциденти 7
2.3 Створення політики, плану та порядку реагування на інциденти 9
2.3.1 Елементи політики 9
2.3.2 Елементи плану 9
2.3.3 Елементи порядку 10
2.3.4 Обмін інформацією зі сторонніми особами / третіми сторонами 10
2.3.4.1 Засоби масової інформації 11
2.3.4.2 Органи правопорядку 12
2.3.4.3 Організації, котрим звітують щодо інцидентів 13
2.3.4.4 Інші треті сторони 14
2.4 Структура команди реагування на інциденти 15
2.4.1 Моделі команди 15
2.4.2 Вибір моделі команди 17
2.4.3 Особовий склад, котрий бере участь у реагуванні на інциденти 19
2.4.4 Залежності в межах організацій 21
2.5 Послуги команд реагування на інциденти 22
2.6 Рекомендації 23

3. Управління інцидентами **25**
3.1 Підготування 25
3.1.1 Підготування до управління інцидентами 26
3.1.2 Попередження інцидентів 28
3.2 Виявлення та аналіз 30
3.2.1 Вектори атак 30
3.2.2 Ознаки інциденту 31
3.2.3 Джерела прекурсорів та індикаторів 32
3.2.4 Аналіз інциденту 34
3.2.5 Документація щодо інциденту 37
3.2.6 Пріоритезація інцидентів 38
3.2.7 Повідомлення про інцидент 40
3.3 Стримування, ліквідація наслідків та відновлення 41
3.3.1 Вибір стратегії стримування 41

3.3.2 Збір доказів та управління ними 42
3.3.3 Визначення хостів, що атакують 43
3.3.4 Ліквідація наслідків та відновлення 44
3.4 Заходи після інциденту 45
3.4.1 Засвоєний досвід 45
3.4.2 Використання даних, зібраних про інцидент 46
3.4.3 Зберігання доказів 49
3.5 Контрольний список з управління інцидентами 49
3.6 Рекомендації 51

4. Координація та обмін інформацією 54
4.1 Координація 54
4.1.1 Співпраця в рамках координації дій 55
4.1.2 Договори щодо обміну даними та вимоги до звітності 57
4.2 Технології обміну інформацією 57
4.2.1 Спеціальні 57
4.2.2 Частково автоматизовані 58
4.2.3 Міркування щодо безпеки 58
4.3 Обмін детальною інформацією 59
4.3.1 Інформація щодо наслідків для бізнесу 59
4.3.2 Технічна інформація 60
4.4 Рекомендації 61
A.1 Підготування запитань до сценарію 62
Виявлення та аналіз: 62
Стримування, ліквідація наслідків та відновлення 62
Заходи після інциденту 63
Загальні запитання: 63
A.2 Сценарії 64
Сценарій № 2: Зараження «хробаком» і агентом розподіленої атаки на відмову в обслуговуванні (DDoS) 64
Сценарій № 3: Викрадені документи 65
Сценарій № 4: Зламаний сервер бази даних 65
Сценарій № 5: Невідоме вилучення даних 65
Сценарій № 6: Несанкціонований доступ до документів щодо оплати праці 66
Сценарій № 7: Хост, що зникає 66
Сценарій № 8: Злам під час віддаленої роботи 67
Сценарій № 9: Анонімна загроза 68
Сценарій № 10: Файлообмінні мережі 68
Сценарій № 11: Невідомі бездротові точки доступу 68
B.1 Основні елементи даних 69
B.2 Елементи даних для куратора інциденту 70
Організації реагування на інциденти 74
Специфікації обміну даними, котрі стосуються управління інцидентами 75
1. Що таке інцидент? 76
2. Що таке управління інцидентами? 76
3. Що таке реагування на інциденти? 76
4. Що таке команда реагування на інциденти? 76
5. Які послуги надає команда реагування на інциденти? 76
6. Кого слід повідомити та кому слід звітувати про інциденти? 77
7. Як слід повідомляти/звітувати про інциденти? 77
8. Яку інформацію слід надати, повідомляючи/звітуючи про інцидент? 77

9. Як швидко команда реагування на інцидент реагує на повідомлення/звіт про інцидент? 78
10. Коли особі, яка була залучена до інциденту, слід звернутися до органів правопорядку? 78
11. Що робити людині, яка виявила атаку на систему? 78
12. Що треба робити людині, до якої звернулися ЗМІ із запитаннями щодо інциденту? 78
Технічні зміни: 80
Видалення: 80
Друга редакція Остаточна – серпень 2012 року Правки від редактора: 80
Технічні зміни: 80

Перелік рисунків

Рисунок 2-1.Комунікації зі сторонніми особами / третіми сторонами 10
Рисунок 3-1.Життєвий цикл реагування на інциденти 21
Рисунок 3-2.Життєвий цикл реагування на інциденти (виявлення та аналіз) 25
Рисунок 3-3.Життєвий цикл реагування на інциденти (стримування, ліквідація наслідків та відновлення) 35
Рисунок 3-4.Життєвий цикл реагування на інциденти (заходи після інциденту) 38
Рисунок 4-1.Координація реагування на інциденти 46

Перелік таблиць

Таблиця 3-1.Поширені джерела прекурсорів та індикаторів 27
Таблиця 3-2.Категорії функціональних наслідків 33
Таблиця 3-3.Категорії інформаційних наслідків 33
Таблиця 3-4.Категорії зусиль для забезпечення можливостей відновлення 33
Таблиця 3-5.Контрольний список з управління інцидентами 42
Таблиця 4-1.Співпраця в рамках координації дій 47

Преамбула

Реагування на інциденти, пов'язані з комп'ютерною безпекою, стало важливою складовою програм інформаційних технологій (IT). Атаки, пов'язані з кібербезпекою, стали не тільки численнішими та різноманітнішими, але й більш згубними та руйнівними. Досить часто з'являються нові типи інцидентів, пов'язаних із безпекою. Зменшити кількість інцидентів можна за допомогою превентивних заходів, заснованих на результатах оцінювання ризиків, хоча не всім інцидентам можна запобігти. Отже, для швидкого виявлення інцидентів, мінімізації втрат і руйнувань, виправлення слабких сторін, якими скористалися зловмисники, а також відновлення надання IT-послуг необхідно розбудовувати потенціал реагування на інциденти. Тому це видання містить рекомендації щодо управління інцидентами, зокрема щодо аналізу даних, пов'язаних із інцидентом, та визначення відповідного алгоритму реагування на кожен інцидент. Цих керівних настанов можна дотримуватися незалежно від певних апаратних платформ, операційних систем, протоколів або застосунків.

Оскільки ефективне реагування на інциденти – це складний процес, створення успішного потенціалу реагування на інциденти вимагає значного планування та ресурсів. Надзвичайно важливо постійно проводити моніторинг атак. Вирішальне значення має встановлення чіткого порядку для пріоритезації процесу управління інцидентами, як і впровадження ефективних методів збору, аналізу даних та звітування про них. Також надзвичайно важливо налагодити відносини та встановити відповідні засоби комунікації з іншими внутрішніми групами (наприклад, відділом кадрового забезпечення, юридичним відділом) та із зовнішніми групами (наприклад, іншими командами реагування на інциденти, правоохоронними органами).

Це видання допомагає організаціям у створенні потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою, а також в ефективному та результативному управлінні інцидентами. Ця редакція видання, тобто друга редакція, оновлює матеріали у всьому виданні, щоб відобразити зміни, які відбулися в атаках та інцидентах. Розуміння загроз та виявлення сучасних атак на ранніх стадіях є визначальним для запобігання подальшим компрометаціям, а активний обмін інформацією між організаціями щодо ознак цих атак є дедалі ефективнішим способом їх виявлення.

Виконання вимог та рекомендацій, наведених нижче, має сприяти ефективному та результативному реагуванню на інциденти федеральними відомствами та установами.

Організаціям потрібно створити, забезпечити й використовувати офіційний потенціал реагування на інциденти. Федеральне законодавство вимагає від федеральних органів, відомств та агенцій повідомляти про інциденти до офісу Комп'ютерної команди екстреної готовності Сполучених Штатів (US-CERT) у складі Міністерства національної безпеки (Департаменту внутрішньої безпеки [DHS]).

Відповідно до вимог Федерального закону США про управління інформаційною безпекою (FISMA) федеральні органи, відомства та агенції зобов'язані створити потенціал реагування на інциденти. Кожен федеральний цивільний орган повинен призначити з US-CERT основну та додаткову контактну установу/особу (так звану «точку контакту», скорочено POC) і повідомляти про всі інциденти відповідно до політики органу щодо реагування на інциденти. Кожен орган несе відповідальність за визначення того, в який спосіб він виконуватиме ці вимоги.

Створення потенціалу реагування на інциденти має передбачати такі дії:

- Створення політики та плану реагування на інциденти
- Розроблення порядку для обробки інцидентів та звітування
- Визначення рекомендацій щодо комунікацій зі сторонніми особами / третіми сторонами стосовно інцидентів
- Вибір структури команди та моделі кадрового забезпечення
- Налагодження зв'язків і встановлення комунікацій між командою реагування на інциденти та іншими групами, як внутрішніми (наприклад, юридичний відділ), так і зовнішніми (наприклад, правоохоронні органи)
- Визначення того, які послуги має надавати команда реагування на інциденти
- Кадрове забезпечення та навчання команди реагування на інциденти.

Організації мають зменшити частоту інцидентів шляхом ефективного захисту мереж, систем і застосунків.

Часто менш витратним і ефективнішим є попередження проблем, а не реагування на них після виникнення. Отже, запобігання інцидентам є важливим доповненням до потенціалу реагування на інциденти. Якщо засобів контролю безпеки буде недостатньо, може статися велика кількість інцидентів. Це може призвести до перевантаження ресурсів і можливостей для реагування, що спричинить несвоєчасне або неповне відновлення і, можливо, більшу шкоду та більш тривалий період обслуговування та недоступності даних. Управління інцидентами може відбуватися більш ефективно, якщо організації доповнять свій потенціал реагування на інциденти достатнім рівнем ресурсів, щоб активно підтримувати безпеку мереж, систем і застосунків. Це передбачає навчання ІТ-персоналу з питань дотримання стандартів безпеки організації та ознайомлення користувачів із політиками та порядком належного використання мереж, систем і застосунків.

Організації повинні задокументувати свої рекомендації / керівні настанови щодо взаємодії з іншими організаціями стосовно інцидентів.

У рамках управління інцидентами організації потрібно буде комунікувати зі сторонніми особами / третіми сторонами, такими як інші команди реагування на інциденти, правоохоронні органи, ЗМІ, постачальники та організації, котрі постраждали внаслідок атак. В зв'язку з тим, що ці комунікації часто мають відбуватися швидко, організації повинні заздалегідь визначити рекомендації / керівні настанови, які стосуються комунікацій, щоб потрібним особам надавалася лише відповідна інформація.

Загалом, організації мають бути готові впоратися з будь-якими інцидентами, але повинні сфокусуватися на тому, щоб бути готовими до інцидентів, які використовують поширені вектори атак.

Є незліченна кількість способів, як можуть відбуватися інциденти, тому неможливо розробити покрокові інструкції для управління кожним окремим інцидентом. У цьому виданні на основі поширених векторів атак визначено кілька типів інцидентів; ці категорії не призначені для надання остаточної класифікації інцидентів, а скоріше для використання їх як основи для визначення більш конкретного порядку управління інцидентами. Різні типи інцидентів вимагають різних стратегій реагування. Вектори атаки включають:

- **Зовнішній/знімний носій:** Атака, здійснена зі знімного носія (наприклад, флеш-накопичувача, компакт-диска) або периферійного пристрою.
- **Виснаження:** Атака, що використовує методи «грубої сили» для компрометації, погіршення або знищення систем, мереж або служб.
- **Вебресурс:** Атака, здійснена з вебсайту або вебзастосунку.
- **Електронна пошта:** Атака, здійснена через електронний лист або файл, прикріплений до електронної пошти.
- **Неналежне використання:** Будь-який інцидент, що виник у результаті порушення авторизованим користувачем затвердженої політики безпеки організації, за винятком вищевказаних категорій.
- **Втрата або викрадення обладнання:** Втрата або викрадення комп'ютерного пристрою або носія, котрий використовується організацією, наприклад ноутбука чи смартфона.
- **Інше:** Атаки, які не вписуються в інші категорії.

Організації мають наголошувати на важливості виявлення та аналізу інцидентів у всій організації.

В організації щодня можуть виникати мільйони можливих ознак інцидентів, які, перш за все, реєструються за допомогою журналювання і програмного забезпечення, що сприяє комп'ютерній безпеці. Автоматизація необхідна для виконання початкового аналізу даних і відбору тих подій, які варто дослідити вже персоналу, який переглядає дані журналу. Для автоматизації процесу аналізу велике значення може мати програмне забезпечення, що виявляє кореляції між подіями. Однак ефективність процесу залежить від якості даних, котрі надходять до нього. Організаціям необхідно встановити стандарти і порядок журналювання, щоб забезпечити збір належної інформації журналами та програмним забезпеченням, яке сприяє безпеці, а також систематичний перегляд даних.

Організаціям необхідно створити письмові рекомендації щодо пріоритезації інцидентів.

Пріоритезація процесу управління окремими інцидентами є критично важливим аспектом прийняття рішень у процесі реагування на інциденти. Ефективний обмін інформацією може допомогти організації визначити ситуації, які є більш критичними та потребують негайної уваги. Інциденти потрібно пріоритезувати на основі відповідних чинників, таких як функціональні наслідки інциденту (наприклад, поточні та ймовірні майбутні негативні наслідки для напрямів діяльності), інформаційні наслідки інциденту (наприклад, вплив на конфіденційність, цілісність і доступність інформації організації), а також можливість відновлення після інциденту (наприклад, час і типи ресурсів, які необхідно витратити на відновлення після інциденту).

Організаціям необхідно використовувати досвід, засвоєний за результатами інцидентів, щоб отримати користь від них.

Після того, як організація впоралася із серйозним інцидентом, їй необхідно провести нараду щодо засвоєного досвіду для перевірки ефективності процесу управління інцидентами і визначення необхідного поліпшення наявних засобів контролю та практик безпеки.
Наради щодо засвоєного досвіду також можна періодично проводити для менш серйозних інцидентів, якщо час і ресурси дозволяють. Інформацію, накопичену під час усіх нарад щодо засвоєного досвіду, слід використовувати для виявлення та виправлення слабких сторін системи та недоліків у політиках та порядку. Звіти про подальшу діяльність, створені для кожного врегульованого інциденту, можуть бути важливими не лише з погляду доказів, але й для довідкової інформації, яку можна використати в рамах управління майбутніми інцидентами та під час навчання нових учасників команди.

1. Вступ

1.1 Уповноважений орган, що видав документ

Це видання було створено Національним інститутом стандартів і технологій США (NIST) в рамках його обов'язків, передбачених Федеральним законом США про управління інформаційною безпекою (FISMA) від 2002 року, Публічний закон (P.L.) 107-347.

NIST відповідає за розроблення стандартів та рекомендацій / керівних настанов, включаючи мінімальні вимоги, з метою належного убезпечення інформації для всіх операцій та активів органів, відомства та установ, але такі стандарти й настанови не застосовуються до національних систем безпеки. Ці керівні настанови відповідають вимогам Директиви A-130, виданої Відділом із питань управління та бюджету (OMB), Розділ 8b(3), Убезпечення інформаційних систем відомств та агентств, котрі проаналізовано в Директиві A-130, Додаток IV: Аналіз основних розділів. Додаткову інформацію представлено в Директиві A-130, Додаток III.

Ці керівні настанови було підготовлено для використання Федеральними органами. Вони можуть використовуватися недержавними організаціями на добровільній основі, і на них не поширюється дія авторського права, хоча бажано додавати посилання на джерело.

Жодне положення цього документа не може розглядатись як таке, що суперечить стандартам та настановам, обов'язковим до виконання Федеральними органами, крім того, ці керівні настанови не можуть розглядатись як такі, що змінюють або замінюють чинні повноваження Міністра торгівлі, директора OMB або іншої посадової особи Федерального органу.

1.2 Мета і сфера застосування

Це видання має на меті допомогти організаціям зменшити ризики від інцидентів, пов'язаних із комп'ютерною безпекою, надаючи практичні рекомендації щодо ефективного та результативного реагування на інциденти. Воно містить вказівки щодо створення ефективної програми реагування на інциденти, але основна увага в цьому документі приділена виявленню, аналізу, визначенню пріоритетів та вирішенню інцидентів. Організаціям рекомендується адаптувати рекомендовані настанови та рішення, щоб відповідати конкретним представленим у документі вимогам щодо безпеки та потреб, пов'язаних із поточними завданнями.

1.3 Цільова аудиторія

Цей документ створено для команд реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT), системних адміністраторів і адміністраторів мережі, персоналу служби безпеки, персоналу технічної підтримки, керівників з інформаційної безпеки (CISO), начальників інформаційних управлінь (CIO), менеджерів програм із комп'ютерної безпеки та інших осіб, які відповідають за підготовку до інцидентів, пов'язаних із безпекою, або реагування на них.

1.4 Структура документа

Наступна частина цього документа складається з таких розділів та додатків:

- У розділі 2 обговорюється необхідність реагування на інциденти, окреслюються можливі структури команди реагування на інциденти та висвітлюються інші групи в організації, які можуть брати участь в управлінні інцидентами.
- У розділі 3 розглянуто основні кроки з управління інцидентами та надано поради щодо того, як ефективніше управляти інцидентами, зокрема щодо виявлення та аналізу інцидентів.

- У розділі 4 розглянуто необхідність координації реагування на інциденти та обміну інформацією.
- У Додатку A наведено сценарії реагування на інциденти та запитання, котрі можна використати в обговореннях під час круглих столів на тему реагування на інциденти.
- У Додатку B наведено списки полів даних, які запропоновано збирати для кожного інциденту.
- У Додатках C і D наведено термінологічний словник і перелік скорочень відповідно.
- У Додатку E визначено ресурси, котрі можуть бути корисними для планування та реагування на інциденти.
- У Додатку F представлено часті запитання про реагування на інциденти.
- У Додатку G наведено основні кроки, яких слід дотримуватися під час врегулювання криз, які виникли через інциденти, пов’язані з комп’ютерною безпекою.
- Додаток H містить журнал змін із переліком суттєвих змін із моменту попередньої редакції.

2. Розбудова потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою

Розбудова потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRC), передбачає кілька важливих рішень і дій. Перш за все слід створити визначення терміну «інцидент» для конкретної організації, щоб термін у всьому обсязі був зрозумілим. Організація має вирішити, які послуги повинна надавати команда реагування на інциденти, розглянути, які структури та моделі команд можуть надавати ці послуги, а також обрати й запровадити одну або кілька команд реагування на інциденти. Важливою частиною створення команди є створення політики, плану та порядку реагування на інциденти, щоб реагування на інциденти виконувалося ефективно, результативно та послідовно, а також щоб команда мала повноваження робити те, що необхідно. План, політика та порядок повинні відображати взаємодію команди з іншими командами в організації, а також зі сторонніми особами / третіми сторонами, такими як правоохоронні органи, ЗМІ та інші організації, що займаються реагуванням на інциденти. У цьому пункті наведено не лише рекомендації, що мають допомагати організаціям, які створюють потенціал реагування на інциденти, а й поради щодо підтримки та покращення наявного потенціалу.

2.1 Події та інциденти

Подія – це будь-яке явище, що спостерігається в системі або мережі. Події включають такі явища, як підключення користувача до загального файлового ресурсу, отримання сервером запиту щодо вебсторінки, відправлення користувачем електронної пошти та блокування брандмауером спроби підключення. *Небажані події* – це події з негативними наслідками, такі як помилка чи збій системи, «флуд» пакетами, несанкціоноване використання системних привілеїв, несанкціонований доступ до конфіденційних даних та запуск шкідливого програмного забезпечення, котре знищує дані. Ці керівні настанови розглядають лише ті небажані події, що пов'язані з комп'ютерною безпекою, а не ті, які спричинені природними катастрофами, збоями в електропостачанні тощо.

Інциденти, пов'язані з комп'ютерною безпекою – це порушення або неминуча загроза порушення[1] політики комп'ютерної безпеки, політики прийнятного користування або стандартних методів забезпечення захисту програм. Приклади інцидентів[2] включають:

- Зловмисник дає команду ботнету надсилати до вебсервера велику кількість запитів на з'єднання, що призводить до його збою.
- Користувачів обманом змушують відкрити вкладений до листа «квартальний звіт», надісланий електронною поштою, котрий насправді є шкідливим програмним забезпеченням; запуск цього файлу заразив їхні комп'ютери та встановив з'єднання із зовнішнім хостом.
- Зловмисник отримує доступ до конфіденційних даних та погрожує, що вони будуть оприлюднені, якщо організація не заплатить визначену суму грошей.
- Користувач розголошує конфіденційну інформацію стороннім особам або спричиняє витік конфіденційної інформації за допомогою служб файлообмінних мереж.

2.2 Необхідність реагування на інциденти

Атаки часто ставлять під загрозу персональну інформацію та бізнес-дані, і дуже важливо швидко та ефективно реагувати на випадки порушення безпеки. Концепція реагування на інциденти, пов'язані з комп'ютерною безпекою, набула широкого визнання та впровадження.

Однією з переваг наявності потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою, є те, що він підтримує систематичне реагування на інциденти (тобто дотримання послідовної методології управління інцидентами) з метою вжиття відповідних заходів. Реагування на інциденти допомагає персоналу мінімізувати викликані інцидентами втрати або спричинене ними викрадення інформації та порушення роботи служб. Ще однією перевагою реагування на інцидент є можливість використовувати інформацію, отриману під час управління інцидентами, щоб краще підготуватися до управління майбутніми інцидентами, а також забезпечити більший рівень захисту систем і даних. Потенціал реагування на інциденти також допомагає належно вирішувати правові питання, що можуть виникнути під час інцидентів.

Окрім того, що є ділові причин для створення потенціалу реагування на інциденти, Федеральні відомства та установи також повинні дотримуватися законів, нормативно-правових актів і політик, що спрямовані на скоординований, ефективний захист від загроз безпеці інформації. Головними серед цих нормативних документів є такі:

- Директива № A-130, Додаток III,[3] видана OMB у 2000 році, яка наказує федеральним органам «забезпечити наявність потенціалу для надання користувачам допомоги у разі виникнення в системі інциденту, пов'язаного з безпекою, та обміну інформацією про поширені вразливості та загрози. Такий потенціал має передбачати обмін інформацією з іншими організаціями... і повинен допомагати органу, відомству чи установі у вчиненні відповідних юридичних дій відповідно до інструкцій, настанов чи вказівок Міністерства юстиції».

- Федеральний закон США про управління інформаційною безпекою – FISMA (від 2002 року),[4] який вимагає, щоб органи, відомства чи установи мали затверджені «процедури виявлення, звітування та реагування на інциденти, пов'язані з безпекою», а також створює централізований Федеральний центр із питань інцидентів, пов'язаних з інформаційною безпекою, покликаний, серед іншого:

  - «Своєчасно надавати технічну допомогу операторам інформаційних систем органів, відомств чи установ … включаючи інструкції, настанови чи вказівки щодо виявлення і управління інцидентами, пов'язаними з інформаційною безпекою...

  - Готувати й аналізувати інформацію про інциденти, які загрожують безпеці інформації...

  - Інформувати операторів інформаційних систем органів, відомств чи установ про поточні та потенційні загрози безпеці інформації, а також про вразливості....».

- Федеральні стандарти обробки інформації (FIPS) 200, *Мінімальні вимоги до безпеки федеральної інформації та федеральних інформаційних систем*[5], від березня 2006 року, які відповідно визначають мінімальні вимоги до безпеки федеральної інформації та федеральних інформаційних систем, включаючи реагування на інциденти. Конкретні вимоги визначено в Спеціальному виданні стандарту (SP) NIST 800-53, *Рекомендовані заходи контролю для федеральних інформаційних систем та організацій*.

- Меморандум OMB M-07-16, *Захист інформації, що дає змогу ідентифікувати особу, і реагування на порушення в цій сфері*[6], від травня 2007 року, який містить рекомендації щодо звітування про інциденти, пов'язані з безпекою, в яких є інформація, що дає змогу ідентифікувати особу (PII)

---

1 «Неминуча загроза порушення» стосується тих ситуацій, коли організація має фактичні підстави вважати, що має відбутися конкретний інцидент. Наприклад, персонал, який працює з антивірусним програмним забезпеченням, може отримати інформаційний бюлетень від постачальника програмного забезпечення з попередженням про нове шкідливе програмне забезпечення, котре швидко поширюються інтернетом.

2 В подальшому у цьому документі терміни «інцидент» та «інцидент, пов'язаний з комп'ютерною безпекою» є взаємозамінними.

2.3 Створення політики, плану та порядку реагування на інциденти

У цьому пункті обговорюються політики, плани та порядок, пов'язані з реагуванням на інциденти, при цьому акцент зроблено на взаємодії зі сторонніми особами / третіми сторонами.

2.3.1 Елементи політики

Політика реагування на інциденти носить індивідуальний характер та залежить від особливостей організації. Однак більшість політик включають кілька однакових основних елементів:

- Формулювання зобов'язань вищого керівництва
- Мета та завдання політики
- Сфера застосування політики (на кого і на що поширюється її дія та за яких обставин)
- Визначення інцидентів, пов'язаних із комп'ютерною безпекою, та термінів, які стосуються цієї тематики
- Організаційна структура та визначення функцій, відповідальності та обсягу повноважень. Ця частина має включати повноваження команди реагування на інциденти щодо конфіскації або відключення обладнання та контролювати ситуацію на предмет підозрілої діяльності; вимоги щодо інформування / подання звітності про певні типи інцидентів; вимоги та інструкції щодо зовнішньої комунікації та обміну інформацією (наприклад, якою інформацією можна ділитися, з ким, коли, і з використанням яких каналів); а також точки первинного передавання інформації та передавання її на вищій рівень у процесі управління інцидентами
- Пріоритезація або оцінювання ступеня тяжкості наслідків інцидентів
- Показники ефективності (котрі обговорюються в пункті 3.4.2)
- Форми звітності та зворотного зв'язку.

2.3.2 Елементи плану

В організацій має бути офіційний, сфокусований та скоординований підхід до реагування на інциденти, включаючи план реагування на інциденти, в якому викладено дорожню карту для реалізації потенціалу з реагування на інциденти. Кожній організації потрібен план, який відповідатиме її унікальним вимогам, що стосуються місії, розміру, структури та функцій організації. План має передбачати необхідні ресурси та підтримку управління. План реагування на інциденти має включати такі елементи:

- Місія
- Стратегії та цілі
- Затвердження вищим керівництвом
- Організаційний підхід до реагування на інциденти

[3] http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
[4] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[5] http://csrc.nist.gov/publications/PubsFIPS.html
[6] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

- Як саме команда реагування на інциденти, буде спілкуватися з іншими підрозділами та персоналом організації, а також з іншими організаціями
- Метрики для вимірювання можливостей реагування на інцидент та ефективності заходів із реагування
- Дорожня карта для забезпечення належного рівня розвитку й удосконалення можливостей реагування на інциденти
- Як програма вписується в організацію загалом.

Місія, стратегії та цілі організації у сфері реагування на інциденти повинні допомогти у визначенні структури побудови її потенціалу з реагування на інциденти. У плані також має бути обговорена структура програми реагування на інциденти. У пункті 2.4.1 розглянуто типи структур.

Як тільки організація розробила план і він був затверджений керівництвом, організація повинна реалізовувати план і переглядати його принаймні раз на рік, щоб переконатися, що організація дотримується дорожньої карти для забезпечення належного рівня розвитку й удосконалення можливостей реагування на інциденти і виконання своїх цілей щодо реагування на інциденти.

Як тільки організація розробила план і він був затверджений керівництвом, організація повинна реалізовувати план і переглядати його принаймні раз на рік, щоб переконатися, що організація дотримується дорожньої карти для забезпечення належного рівня розвитку й удосконалення можливостей реагування на інциденти і виконання своїх цілей щодо реагування на інциденти.

2.3.3 Елементи порядку

Порядок повинен ґрунтуватися на політиці та плані реагування на інциденти. Типовий порядок дій (SOP) – це розмежування конкретних технічних процесів, технологій/методів, контрольних списків і форм, котрі використовуються командою реагування на інциденти. SOP повинен бути достатньо вичерпним та детальним, щоб гарантувати, що в операціях реагування відображаються пріоритети організації. Більше того, дотримання стандартизованих відповідей має звести до мінімуму помилки, особливо ті, що можуть виникнути внаслідок стресових ситуацій під час управління інцидентами. SOP необхідно перевірити, щоб упевнитись у його точності та корисності, а потім розповсюдити його серед усіх учасників команди. Необхідно забезпечити навчання для користувачів SOP; документи SOP можна використовувати як навчальний інструмент. Запропоновані елементи SOP представлено в розділі 3.

2.3.4 Обмін інформацією зі сторонніми особами / третіми сторонами

Організаціям часто потрібно комунікувати зі сторонніми особами / третіми сторонами щодо інциденту, і у відповідних випадках вони повинні це робити, наприклад звертатися до правоохоронних органів, надсилати запити ЗМІ та залучати сторонніх спеціалістів. Є й інший приклад: обговорення інцидентів з іншими причетними сторонами, зокрема з інтернет-провайдерами (ISP), постачальниками вразливого програмного забезпечення або іншими командами реагування на інциденти.
Організації також можуть проактивно ділитися відповідною інформацією щодо індикаторів інцидентів з колегами, щоб покращити виявлення та аналіз інцидентів. Команді реагування на інциденти необхідно обговорити питання обміну інформацією зі службою зв'язків із громадськістю, юридичним відділом та керівництвом організації до того, як станеться інцидент, щоб встановити політику та порядок обміну інформацією. В іншому випадку конфіденційну інформацію щодо інцидентів можуть отримати сторонні особи, що може призвести до додаткових порушень чи збоїв та фінансових втрат.

Команда має задокументувати всі контакти та комунікації зі сторонніми особами / третіми сторонами для встановлення відповідальності та отримання доказів.

У наступних пунктах представлено рекомендації щодо комунікацій із кількома типами сторонніх осіб / третіх сторін, як це показано на рисунку 2-1. Двосторонні стрілки вказують на те, що будь-яка сторона може ініціювати спілкування. Див. Розділ 4 для отримання додаткової інформації про комунікації зі сторонніми особами / третіми сторонами, і пункт 2.4 для ознайомлення з інформацією щодо комунікацій за участю аутсорсерів, які долучаються до реагування на інциденти.

Рисунок 2-1. Комунікації зі сторонніми особами / третіми сторонами

2.3.4.1 Засоби масової інформації

Команда управління інцидентами має встановити порядок комунікації зі ЗМІ, який відповідатиме політиці організації щодо взаємодії зі ЗМІ та розголошення інформації.[7] Організації часто вважають за доцільне призначити єдиний «контактний пункт» (POC) і принаймні одну резервну контактну особу/установу для обговорення інцидентів із представниками ЗМІ. Нижче наведено дії, яких рекомендовано вживати для підготовки цих призначених контактних осіб, їх також слід розглянути для підготовки інших осіб, котрі можуть комунікувати зі ЗМІ:

- Проводьте навчання щодо взаємодії зі ЗМІ стосовно інцидентів Такі тренінги повинні включати важливість нерозголошення конфіденційної інформації, зокрема технічних подробиць щодо контрзаходів, які можуть допомогти іншим зловмисникам, а також окреслювати позитивні аспекти повного та ефективного донесення важливої інформації до громадськості.
- Визначте порядок для короткого ознайомлення фахівців із зв'язків зі ЗМІ (прессекретарів тощо) щодо проблемних питань та чутливих моментів конкретного інциденту, перш ніж починати обговорювати його зі ЗМІ.
- Інформуйте про поточний стан справ щодо інциденту, щоб комунікації зі ЗМІ були послідовними та актуальними.
- Нагадайте всім працівникам загальний порядок роботи із запитами від ЗМІ.
- Під час вправ із вирішення інцидентів проводьте пробні інтерв'ю та пресконференції. Нижче наведено приклади запитань, які можна задати фахівцям із зв'язків зі ЗМІ:
  - Хто здійснив атаку на вашу установу/організацію? Чому?
  - Коли це сталося? Як саме це сталося? Це сталося через те, що у вас недостатні методи забезпечення захисту програмного та апаратного забезпечення?
  - Наскільки масштабним є цей інцидент? Яких заходів ви вживаєте, щоб визначити, що саме сталося, та попередити такі ситуації у майбутньому?
  - Які наслідки має цей інцидент? Чи стався витік будь-якої інформації, що дає змогу ідентифікувати особу (PII)? Якими є орієнтовні витрати на ліквідацію наслідків інциденту?

2.3.4.2 Органи правопорядку

Однією з причин того, що у багатьох випадках провадження щодо інцидентів, пов'язаних із безпекою, не доходять до відповідних вироків суду, є те, що деякі організації не звертаються в належний спосіб до органів правопорядку. Розслідуваннями інцидентів займаються декілька рівнів органів правопорядку: зокрема, у Сполучених Штатах, це федеральні слідчі органи (наприклад, Федеральне бюро розслідувань [ФБР] і Секретна служба США), окружні прокуратури, правоохоронні органи штату та місцеві органи правопорядку (наприклад, на рівні округу). До процесу також можуть залучатися органи правопорядку з інших країн, наприклад у випадку атак, здійснених з або спрямованих на організації чи населені пункти за межами США. Крім того, в кожному органі чи відомстві є Управління генерального інспектора (OIG) для розслідування порушень закону. Команда реагування на інциденти має познайомитися із закріпленими за ними представниками різних органів правопорядку до того, як станеться інцидент, щоб обговорити умови, за яких їх слід повідомляти про інциденти, як звітувати про них, які докази слід збирати та в який спосіб.

[7] Наприклад організація може надавати перевагу тому, щоб у всіх обговореннях інцидентів зі ЗМІ брали участь працівники її служби зв'язків із громадськістю та юридичного відділу.

До органів правопорядку слід звертатися через призначених осіб у спосіб, що відповідає вимогам закону та порядку, затвердженому в установі/організації. Багато установ та організацій вважають, що краще призначити одного учасника команди реагування на інциденти контактною особою (POC), відповідальною за комунікації з органами правопорядку. Така особа повинна бути ознайомлена з порядком подання звітності для всіх відповідних органів правопорядку і добре володіти інформацію, щоб рекомендувати, до якого органу слід звернутися, якщо такий є. Слід мати на увазі, що зазвичай організації не потрібно повідомляти одразу кілька установ, оскільки це може призвести до спорів про підслідність. Команда реагування на інциденти повинна розуміти, які потенційні спори про підслідність можуть виникнути (наприклад, фізичне місцезнаходження – на організацію, головний офіс якої знаходиться в одному штаті та яка має сервер, розташований у другому штаті, здійснено атаку з боку системи, розміщеної в третьому штаті, котру віддалено використовував зловмисник з четвертого штату).

2.3.4.3 Організації, котрим звітують щодо інцидентів

Відповідно до вимог FISMA федеральні органи, відомства та агенції зобов'язані повідомляти про інциденти Комп'ютерній команді екстреної готовності Сполучених Штатів (US-CERT),[8] котра становить єдиний урядовий центр підтримки федеральної влади у сфері підготування рішень із забезпечення захисту цивільних комп'ютерних мереж федеральної виконавчої влади. US-CERT не замінює наявні в органах чи установах команди реагування; скоріше, команда посилює зусилля федеральної влади, виступаючи в ролі координаційного центру для боротьби з інцидентами. US-CERT аналізує інформацію, надану відомством чи установою, для визначення тенденцій та індикаторів атак; їх легше розпізнати, якщо переглядати дані багатьох організацій, а не лише однієї організації.

Кожен орган повинен призначити (спільно з US-CERT) основну та додаткову POC і повідомляти про всі інциденти відповідно до політики органу щодо реагування на інциденти. Організації повинні створити порядок, де вказано, хто має повідомляти про інциденти та як вони мають повідомляти про інциденти. Вимоги, категорії та терміни інформування US-CERT про інциденти наведено на вебсайті US-CERT.[9] Усі федеральні органи, відомства та агенції повинні переконатися, що їхній порядок реагування на інциденти відповідає вимогам щодо звітності, яка подається до US-CERT, і що працівники належно дотримуються порядку.

Рекомендується, щоб усі організації повідомляли про інциденти до відповідних CSIRT. Якщо організація не має власної CSIRT, до якої можна звернутися, вона може повідомляти про інциденти іншим організаціям, включаючи Центри обміну й аналізу інформації (ISAC). Однією з функцій цих галузевих організацій із приватного сектору є обмін важливою інформацією, пов'язаною з комп'ютерною безпекою, між своїми учасниками. Декілька ISAC були сформовані для таких галузей, як зв'язок, електроенергетика, фінансові послуги, інформаційні технології, дослідження та освіта.[10]

---

8 http://www.us-cert.gov/

9 http://www.us-cert.gov/federal/reportingRequirements.html

10 Див. вебсайт Національна рада ISAC за посиланням http://www.isaccouncil.org/, щоб переглянути перелік ISAC.

2.3.4.4 Інші треті сторони

В організації може виникнути бажання обговорити інциденти з іншими групами, зокрема з тими, що перераховані нижче. В рамках звернення до цих третіх сторін організація може захотіти працювати через US-CERT або її ISAC як «надійного представника» для посередництва у взаєминах. Існує висока ймовірність, що інші стикаються зі схожими проблемами, і довірений представник може гарантувати, що будь-які подібні закономірності будуть виявлені та враховані.

- **Інтернет-провайдери (ISP) організації** Щоб заблокувати масштабну мережеву атаку або відстежити її походження, організації може знадобитися допомога від свого провайдера.
- **Власники адрес, з яких здійснюється атака.** Якщо атаки здійснюються з адресного простору IP сторонньої організації, команда з управління інцидентами може захотіти поспілкуватися з контактними особами, призначеними відповідальними за питання безпеки, щоб організація могла попередити їх або попросити зібрати докази. Наполегливо рекомендується організувати координацію таких комунікацій з US-CERT або ISAC.
- **Постачальники програмного забезпечення.** Команда з управління інцидентами може захотіти поспілкуватися про підозрілу діяльність із постачальником програмного забезпечення. Таке спілкування може включати запитання щодо значення певних записів журналу або відомих помилок першого роду (хибно позитивних) для певних сигнатур виявлення атак/втручання, де може знадобитися розкриття мінімальної інформації про інцидент. У деяких випадках може знадобитися надати додаткову інформацію, наприклад тоді, коли є підозра, що сервер було зламано через невідому вразливість програмного забезпечення. Маючи на меті допомогти організаціям зрозуміти поточне середовище загроз, постачальники програмного забезпечення також можуть надавати інформацію про відомі їм загрози (наприклад, про нові атаки).
- **Інші команди реагування на інциденти.** В організації може статися інцидент, подібний до тих, котрі розглядаються іншими командами; активний обмін інформацією може сприяти більш ефективному та результативному управлінню інцидентами (наприклад, він може забезпечити завчасне інформування, підвищення рівня готовності, підвищення поінформованості щодо ситуації). Такі групи як Форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою (FIRST)[11], Урядовий форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою (GFIRST)[12], а також Робоча група з питань боротьби з фішингом (APWG)[13] не є командами реагування на інциденти, але вони сприяють обміну інформацією між командами реагування на інциденти.

[11] http://www.first.org/
[12] GFIRST спеціально для федеральних відомств та установ. (http://www.us-cert.gov/federal/gfirst.html)
[13] http://www.antiphishing.org/

- **Треті сторони, які постраждали від інцидентів.** Інцидент може впливати безпосередньо на треті сторони, наприклад стороння організація може зв'язатися з організацією і заявити, що один із користувачів організації атакує її. Інший випадок, коли сторонні особи / треті сторони можуть постраждати – це якщо зловмисник отримує доступ до конфіденційної інформації про них, наприклад до інформації про кредитну картку. У деяких юрисдикціях організації зобов'язані сповістити всі сторони, котрі постраждали від такого інциденту. Незалежно від обставин, організації бажано сповістити про інцидент сторонніх осіб / третіх сторін, які постраждали від інциденту, до того, як це зроблять ЗМІ чи інші сторонні організації. Керівникам слід бути обережними та надавати лише відповідну інформацію – сторони, які постраждали від інциденту, можуть просити надати подробиці службового розслідування, котрі не можна розголошувати публічно.

  Меморандум OMB M-07-16, *Захист інформації, що дає змогу ідентифікувати особу, і реагування на порушення в цій сфері*, вимагає від федеральних органів та установ розробити та впровадити політику інформування про витік інформації, що дає змогу ідентифікувати особу (PII).[14] Фахівці, що займаються управлінням інцидентами, повинні розуміти, як мають відрізнятися їхні дії щодо управління інцидентами у ситуаціях, коли є підозра на витік персональних даних, наприклад з'являється інформування додаткових сторін або повідомлення сторін у коротші строки. У Меморандумі OMB M-07-16 наведено конкретні рекомендації щодо політики інформування про витік PII. Крім того, Національна конференція законодавчих зборів штатів (NCSL) має перелік законів про інформування щодо зламів та порушень у сфері державної безпеки.[15]

2.4 Структура команди реагування на інциденти

У всіх, хто виявляє або підозрює, що за участі організації стався інцидент, має бути можливість звернутися до команди реагування на інциденти. Залежно від масштабності інциденту та наявності персоналу, один або кілька учасників команди потім будуть займатися управлінням інцидентом. Фахівці, що займаються управлінням інцидентом, аналізують дані щодо інциденту, визначають наслідки інциденту і вживають відповідних заходів, щоб обмежити наслідки атаки та відновити нормальні послуги. Успіх команди реагування на інциденти залежить від участі та співпраці окремих людей по всій організації. У цьому пункті визначено таких осіб, обговорено моделі команд реагування на інциденти та надано поради щодо вибору відповідної моделі.

2.4.1 Моделі команди

Серед можливих структур команди реагування на інциденти слід відзначити такі:

- **Централізована команда реагування на інциденти.** Одна команда реагування на інциденти займається управлінням інцидентами по всій організації. Ця модель ефективна з погляду обчислювальних ресурсів для невеликих організацій, а також для організацій з мінімальним географічним розмаїттям.

- **Розгалужені команди реагування на інциденти.** В організації є кілька команд реагування на інциденти, кожна з яких відповідає за певний логічний або фізичний сегмент організації. Ця модель ефективна для великих організацій (наприклад, одна команда на один підрозділ), а також для організацій зі значними обчислювальними ресурсами, що розташовані віддалено (наприклад, одна команда на географічний регіон, одна команда на головний офіс). При цьому, команди мають бути частиною єдиного скоординованого органу, щоб процес реагування на інцидент був послідовним по всій організації, а між командами був обмін інформацією. Це набуває особливого значення, оскільки кілька команд можуть бачити складові одного й того самого інциденту або займатися управлінням подібними інцидентами.

Координаційна група. Команда реагування на інциденти консультує інші команди, хоча вони не підпорядковуються їй. Наприклад команда, що працює для відомства загалом, може допомагати командам окремих органів/установ. Цю модель можна розглядати як CSIRT для інших CSIRT. В зв'язку з тим, що в центрі уваги цього документа централізована та розгалужені CSIRT, в ньому детально не розглядається модель координаційної групи.[16]

Команди реагування на інциденти також можуть використовувати будь-яку з трьох моделей кадрового забезпечення:

- **Наймані працівники.** Організація виконує всю роботу з реагування на інциденти, маючи обмежену технічну та адміністративну підтримку з боку підрядників.
- **Частковий аутсорсинг.** Частину своєї роботи з реагування на інциденти організація передає на аутсорсинг.
  У пункті 2.4.2 обговорюються основні чинники, які слід враховувати під час аутсорсингу. Незважаючи на те, що обов'язки з реагування на інциденти можна багатьма способами розділити між організацією та одним або кількома аутсорсерами, є деякі аспекти співпраці, які вже вважаються загальноприйнятою практикою:
  - Найбільш поширений варіант співпраці полягає в тому, що організація передає на аутсорсинг безперервний, тобто 24 години на добу, 7 днів на тиждень (24/7), моніторинг датчиків виявлення атак/втручання, брандмауерів (фаєрволів) та інших засобів безпеки сторонньому постачальнику послуг з управління інформаційною безпекою (MSSP). MSSP визначає та аналізує підозрілу діяльність і повідомляє команді реагування на інциденти організації про кожен виявлений інцидент.
  - Деякі організації виконують базові операції з реагування на інциденти всередині компанії та звертаються до підрядників із проханням допомогти з управлінням інцидентами, особливо із тими, котрі є більш серйозними або поширеними.
- **Повний аутсорсинг.** Організація повністю передає свою роботу з реагування на інциденти на аутсорсинг, як правило, підряднику на місці. Цю модель найчастіше використовують, коли організації потрібна команда реагування на інциденти, яка працюватиме на місці повний робочий день, але сама організація не має достатньої кількості кваліфікованих працівників, які можуть цим займатися. Передбачається, що в організації будуть співробітники, які контролюватимуть і здійснюватимуть нагляд за роботою аутсорсера.

14 http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
15 http://www.ncsl.org/default.aspx?tabid=13489
16 Інформацію щодо моделі Координаційної групи, а також багато інформації щодо інших моделей команди можна знайти у документі CERT®/CC, який називається *Організаційні моделі для команд реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT)* (http://www.cert.org/archive/pdf/03hb001.pdf).

2.4.2 Вибір моделі команди

Зазначені далі чинники організації повинні враховувати під час вибору відповідної структури та моделі кадрового забезпечення для команди реагування на інциденти:

- **Потреба у тому, щоб команда була доступна 24/7.** Більшості організацій потрібно, щоб персонал, залучений до реагування на інциденти, був доступний 24/7. Зазвичай це означає, що фахівцям з управління інцидентами можуть зателефонувати, але це також може означати, що потрібна їх присутність на місці. Доступність у режимі реального часу – це найкращий варіант для реагування на інцидент, оскільки чим довше триває інцидент, тим більше можливостей для пошкодження та збитків. Під час роботи з іншими організаціями часто потрібно, щоб була контактна особа, з якою можна зв'язатися у режимі реального часу, наприклад для відстеження атаки до її джерела.

- **Учасники команди із повною або частковою зайнятістю.** Організації з обмеженим фінансуванням, недостатнім кадровим забезпеченням чи потребами реагування на інциденти можуть співпрацювати лише з учасниками команди реагування на інциденти, які працюють неповний робочий день, що фактично є здебільшого віртуальною командою реагування на інциденти. У цьому випадку команду реагування на інциденти можна розглядати як свого роду добровільну пожежну охорону. Коли виникає надзвичайна ситуація, з учасниками команди оперативно зв'язуються, і ті, хто може допомогти, допомагають. Наявна команда, наприклад служба IT-підтримки, може діяти як перша POC для звітування про інциденти. Співробітників служби підтримки можна навчити проводити початкове розслідування та збір даних, а потім попереджати команду реагування на інцидент, якщо виявиться, що стався серйозний інцидент.

- **Моральний дух працівників.** Для більшості учасників команди робота з реагування на інциденти сповнена стресу, так само, як і обов'язки щодо виклику за вимогою. Через це поєднання учасники команди реагування на інциденти відчувають надмірний стрес. Багатьом організаціям також буде важко знайти охочих, досвідчених і кваліфікованих людей, які будуть у доступі, для участі у наданні підтримки, зокрема цілодобової. Розподіл обов'язків, зокрема зменшення обсягу адміністративної роботи, за виконання якої відповідають учасники команди, може значно підвищити моральний дух.

- **Витрати.** Витрати є основним чинником, особливо якщо працівники повинні бути на місці 24/7. Організації можуть не передбачити у бюджеті витрати, пов'язані з реагуванням на інциденти, наприклад достатнє фінансування для навчання та підтримки навичок. В зв'язку з тим, що команда реагування на інциденти працює з багатьма аспектами IT, її учасникам потрібні набагато ширші знання ніж більшості працівників у сфері IT. Вони також повинні розуміти, як використовувати інструменти реагування на інциденти, такі як програмне забезпечення для цифрової криміналістики. Інші витрати, якими можна знехтувати, стосуються фізичної безпеки робочих зон команди та механізмів комунікації.

- **Експертні знання персоналу.** Управління інцидентами вимагає спеціальних знань і досвіду в кількох технічних областях; «широта» та «глибина» необхідних знань залежить від рівня критичності ризиків організації. Аутсорсери можуть володіти глибшими знаннями щодо виявлення зламів/вторгнень, криміналістики, вразливостей, експлойтів та інших аспектів безпеки, ніж співробітники організації. Крім того, MSSP можуть співставляти події, які стаються у різних клієнтів, щоб вони могли ідентифікувати нові загрози швидше ніж будь-який окремо взятий клієнт.

При цьому, технічний персонал організації зазвичай має набагато кращі знання про середовище організації ніж аутсорсер, що може бути корисно для виявлення помилок першого роду (хибно позитивних), пов'язаних із поведінкою, характерною для організації, і критичністю цілей. У пункті 2.4.3 викладено додаткову інформацію про рекомендовані навички учасників команди.

Розглядаючи питання про аутсорсинг, організації повинні пам'ятати про такі питання:

- **Поточна та майбутня якість роботи.** Організації повинні враховувати не тільки поточну якість (так звану «ширину», тобто спектр, та «глибину», тобто повноту) роботи аутсорсера, але й зусилля, спрямовані на забезпечення високого рівня якості майбутньої роботи, наприклад мінімізацію плинності кадрів та професійного вигорання персоналу, а також забезпечення надійної навчальної програми для нових працівників. Організації мають подумати про те, як вони могли б провести об'єктивне оцінювання якості роботи аутсорсера.

- **Розподіл обов'язків.** Часто організації не хочуть надавати аутсорсеру повноваження приймати оперативні рішення для середовища загалом (наприклад, щодо відключення вебсервера). Важливо, щоб відповідні дії для цих точок прийняття рішень було задокументовано. Наприклад одна з моделей із частковим аутсорсингом вирішує цю проблему так: аутсорсер передає дані про інцидент внутрішньоорганізаційній команді разом із рекомендаціями щодо подальшого вирішення інциденту. Внутрішньоорганізаційна команда в кінцевому підсумку приймає оперативні рішення, а аутсорсер за потреби продовжує надавати підтримку.

- **Конфіденційна інформація, яка стала відомою підряднику.** Обмежити витік інформації можна за допомогою розподілу відповідальності за реагування на інциденти та обмеження доступу до конфіденційної інформації. Наприклад підрядник може визначити, який ідентифікатор користувача був використаний під час інциденту (наприклад, ID 123456), але не знати, яка саме особа пов'язана з цим ідентифікатором користувача. Далі працівники організації можуть взяти розслідування на себе. Угоди про нерозголошення інформації (NDA) – це один із можливих варіантів захисту від розкриття конфіденційної інформації.

- **Відсутність знань щодо питань, характерних для організації.** Точний аналіз і пріоритезація інцидентів залежать від спеціальних знань про середовище організації. Організація має надавати аутсорсеру документи, що визначають, які саме інциденти її турбують, які ресурси є критично важливими та яким має бути рівень реагування за різних обставин. Ці документи повинні регулярно оновлюватися. Організація також має повідомляти про всі зміни та оновлення, внесені до її IT-інфраструктури, налаштувань мережі та систем. В іншому випадку, підрядник повинен спробувати максимально точно здогадатися, як слід обробляти кожен інцидент, що неминуче призведе до невірного управління інцидентами та розчарування з обох сторін. Відсутність знань щодо питань, характерних для організації, також можуть становити проблему, коли реагування на інциденти не передається на аутсорсинг, але комунікації між групами чи командами на слабкому рівні, або якщо організація просто не проводить збір потрібної інформації.

- **Відсутність кореляції.** Взаємозв'язок, тобто кореляція, між багатьма джерелами даних дуже важливий. Якщо система виявлення вторгнень фіксує спробу атаки на вебсервер, але аутсорсер не має доступу до журналів сервера, вона може бути не в змозі визначити, чи була атака успішною. Для того, щоб бути ефективним, аутсорсеру знадобляться права віддаленого привілейованого адміністративного контролю для критично важливих систем і журналів засобів безпеки через захищений канал. Це збільшить витрати на адміністрування, запровадить додаткові точки доступу та підвищить ризик несанкціонованого розкриття конфіденційної інформації.

- **Управління інцидентами у кількох місцях.** Результативна робота з реагування на інциденти часто вимагає фізичної присутності на об'єктах організації. Якщо аутсорсер знаходиться за межами організації, слід зважити, де знаходиться аутсорсер, як швидко він може організувати приїзд команди реагування на інциденти на будь-який об'єкт та скільки це буде коштувати. Необхідно продумати, як відбуватимуться візити на місця; можливо, є певні об'єкти або зони, де не слід дозволяти працювати аутсорсеру.

- **Підтримка навичок реагування на інциденти всередині компанії.** Організації, які віддають реагування на інциденти повністю на аутсорсинг, повинні намагатися підтримувати базові навички реагування на інциденти всередині компанії. Можуть виникнути ситуації, коли аутсорсер буде недоступний, тому організація повинна бути готова самостійно управляти інцидентами. Водночас, технічний персонал організації повинен усвідомлювати значення, потенційні технічні наслідки та вплив рекомендацій аутсорсера.

2.4.3 Особовий склад, котрий бере участь у реагуванні на інциденти

За реагування на інциденти повинен відповідати один працівник з одним або кількома призначеними заступниками. У випадку моделі з повним аутсорсингом ця особа контролює та оцінює роботу аутсорсера. В усіх інших моделях зазвичай є менеджер групи (команди) та один або кілька заступників, які беруть на себе повноваження за відсутності менеджера команди. Менеджери, як правило, виконують різноманітні завдання, зокрема виступають як ланка, що налагоджує зв'язок із вищим керівництвом та іншими групами та організаціями, вирішуючи кризові ситуації та забезпечуючи необхідний персонал, ресурси та навички для команди. Менеджери повинні бути технічно підготовленими та мати відмінні навички спілкування, зокрема вміти спілкуватися з низкою груп аудиторії. Менеджери несуть головну відповідальність за забезпечення належного виконання заходів із реагування на інциденти.

Окрім менеджера команди та заступника, деякі команди також мають керівника з технічних питань – людину з сильними технічними навичками та досвідом у сфері реагування на інциденти, яка бере на себе нагляд і головну відповідальність за якість технічної роботи команди. Позицію керівника з технічних питань не слід плутати з позицією керівника з питань управління інцидентом. Великі групи (команди) часто призначають керівника з питань управління інцидентом (так званого лідера з питань інциденту) основною контактною особою (POC) для управління конкретним інцидентом; лідер з питань інциденту несе відповідальність за роботу з управління інцидентом. Залежно від розміру команди реагування на інциденти та масштабності інциденту, лідер з питань інциденту може фактично не виконувати жодних операцій з безпосереднього управління інцидентом, а скоріше координувати діяльність фахівців, що займаються управлінням інцидентом та його обробкою, збирати інформацію від цих фахівців, надавати оновлену інформацію щодо інциденту іншим групам та забезпечувати задоволення потреб команди.

Учасники команди реагування на інциденти повинні мати чудові технічні навички, зокрема адміністрування системи, адміністрування мережі, програмування, технічної підтримки або виявлення вторгнень. У кожного учасника команди мають бути гарні навички вирішення проблем та здатність до критичного мислення.

Немає потреби. щоб кожен учасник команди був технічним експертом – значною мірою це буде продиктоване практичними міркуваннями та наявністю фінансування, – але повинна бути принаймні одна висококваліфікована особа в кожній ключовій області технологій (наприклад, з операційних систем та застосунків, які часто атакують). Водночас, може бути корисно, щоб деякі учасники команди спеціалізувалися на певних технічних областях, таких як виявлення вторгнень в мережу, аналіз шкідливого програмного забезпечення або криміналістика. Часто також буває корисно залучати технічних спеціалістів, які зазвичай не є частиною команди, на тимчасовій основі.

Важливо протидіяти професійному вигоранню персоналу, даючи їм можливості для навчання та зростання. Нижче наведено пропозиції щодо формування та підтримки навичок:

- Передбачте достатнє фінансування для підтримки, підвищення та розширення знань у технічних областях та дисциплінах у галузі безпеки, а також щодо менш технічної тематики, як-от правові аспекти реагування на інциденти. Цей пункт має включати відрядження персоналу на конференції, а також заохочення їх до участі в конференціях чи стимулювання працівників до цього в інший спосіб, забезпечення технічною літературою, яка сприяє глибшому розумінню технічних аспектів, і час від часу залучення зовнішніх експертів (наприклад, підрядників) із глибокими технічними знаннями у необхідних сферах, наскільки це дозволяє фінансування.

- Давайте учасникам команди можливість виконувати інші завдання, наприклад створювати навчальні матеріали, проводити семінари (воркшопи) з підвищення обізнаності у сфері безпеки та проводити дослідження.

- Розгляньте можливість ротації персоналу до команди реагування на інциденти та з неї, а також беріть участь в обмінах, під час яких учасники команди тимчасово обмінюються функціональними обов’язками з іншими колегам (наприклад, з адміністраторами мережі), щоб здобути нові технічні навички.

- Підтримуйте достатнє кадрове забезпечення, щоб не потрібно було відкликати учасників команди з відпочинку (наприклад, з відпустки).

- Створіть програму наставництва, щоб старший технічний персонал міг допомогти менш досвідченим працівникам навчитися управляти інцидентами.

- Розробіть сценарії для управління інцидентами й організуйте обговорення серед учасників команди щодо того, як вони управлятимуть тими чи іншими інцидентами. У Додатку А наведено набір сценаріїв і перелік запитань, які слід використовувати під час обговорення сценаріїв.

Окрім технічних знань, учасники команди реагування на інциденти повинні мати також інші навички. Визначальними є навички роботи в команді, оскільки для успішного реагування на інциденти необхідні співпраця та координація. У кожного учасника команди також мають бути належні комунікативні навички. Важливі й розмовні навички, оскільки команда буде взаємодіяти з найрізноманітнішими людьми, а навички писемного мовлення мають велике значення, коли учасники команди готують роз'яснення та порядок. Незважаючи на те, що не всі в команді повинні володіти гарними навичками писемного та усного мовлення, принаймні кілька людей у кожній команді повинні ними володіти, щоб команда могла на належному рівні представляти себе перед іншими.

2.4.4 Залежності в межах організацій

Важливо ідентифікувати інші структурні підрозділи / команди в організації, участь яких може знадобитися під час управління інцидентами, щоб можна було налагодити співпрацю з ними до того, як вона знадобиться. Будь-яка команда реагування на інцидент покладається на знання, досвід, судження та здібності інших, зокрема:

- **Керівництво.** Керівництво визначає політику реагування на інциденти, бюджет і кадрове забезпечення. В кінцевому підсумку керівництво несе відповідальність за координацію реагування на інциденти між різними зацікавленими сторонами, мінімізацію шкоди та звітування перед Конгресом, OMB, Рахунковою палатою США (GAO) та іншими сторонами.
- **Інформаційна безпека.** На певних етапах управління інцидентами (запобігання, стримування, ліквідація наслідків та відновлення) можуть знадобитися працівники, які займаються питаннями інформаційної безпеки – зокрема щоб змінити засоби контролю безпеки мережі (наприклад, набори правил брандмауера).
- **IT-підтримка.** Технічні експерти у галузі IT (наприклад, адміністратори системи та мережі) не тільки мають необхідні навички для надання підтримки, але й зазвичай найкраще розуміють технологію, з якою вони працюють на щодень. Саме це розуміння може допомогти впевнитись, що для ураженої системи будуть вжиті відповідні дії, наприклад доцільність від'єднання системи, котру атакували.
- **Юридичний відділ.** Експерти з юридичних питань мають переглянути плани реагування на інциденти, політику та порядок, щоб забезпечити їх відповідність закону та федеральним розпорядчим документам, включаючи право на конфіденційність. Більше того, якщо є підстави вважати, що інцидент може мати юридичні наслідки, включаючи збір доказів, переслідування підозрюваного або судовий позов, або якщо може виникнути потреба в меморандумі про взаєморозуміння (МпВ або MoU) або в інших обов'язкових для виконання угодах, що передбачають обмеження відповідальності за обмін інформацією, слід звернутися за вказівками до головного юрисконсульта або до працівників юридичного відділу.
- **Відділ зв'язків із громадськістю та засобами масової інформації.** Залежно від природи та наслідків інциденту може виникнути потреба в інформуванні ЗМІ та, відповідно, громадськості.
- **Відділ кадрів (відділ по роботі з персоналом).** Якщо у спричиненні інциденту підозрюють працівника, може бути залучений відділ по роботі з персоналом, наприклад для надання допомоги у дисциплінарному провадженні.
- **Відділ планування безперервності роботи.** Організації повинні забезпечити синхронізацію політик і порядку реагування на інциденти та процесів безперервності роботи. Інциденти, пов'язані з комп'ютерною безпекою, підривають стійкість бізнесу організації. Фахівці з планування безперервності роботи мають знати, які бувають інциденти та їхні наслідки, щоб вони могли відповідно узгодити оцінювання наслідків для бізнесу, оцінювання ризиків та план забезпечення безперервності роботи. Більше того, оскільки фахівці з планування безперервності роботи мають великий досвід у мінімізації порушення функціонування під час критичних обставин, їхня участь може бути цінною при плануванні реагування на певні ситуації, зокрема відмови в обслуговуванні (DoS).

- **Відділ організації безпеки та адміністративно-господарського забезпечення.** Деякі інциденти, пов'язані з комп'ютерною безпекою, відбуваються через порушення фізичної безпеки або включають скоординовані логічні та фізичні атаки. Під час управління інцидентами команді реагування на інциденти також може знадобитися доступ до різних приміщень наприклад для отримання доступу до робочої станції, яку зламали зловмисники, в закритому офісі.

2.5 Послуги команд реагування на інциденти

Основне завдання команди реагування на інциденти – це власне реагування на інциденти, але ситуації, коли команда виконує лише реагування на інцидент, трапляються досить рідко. Нижче наведено приклади інших послуг, які може запропонувати команда:

- **Виявлення вторгнень.** Перший рівень команди реагування на інциденти часто бере на себе відповідальність за виявлення вторгнень.[17] Для команди це, як правило, виграшна ситуація, оскільки знання, які вона отримує про технології виявлення вторгнень, допомагають персоналу аналізувати інциденти швидше і точніше.

- **Розповсюдження роз'яснень.** Команда може видавати внутрішньоорганізаційні роз'яснення чи рекомендації щодо нових вразливостей та загроз.[18] Коли це доречно, слід використовувати автоматизовані методи для поширення інформації; наприклад коли до Національної бази даних вразливостей (NVD) додаються нові вразливості, інформація розповсюджується через XML- та RSS-канали.[19] Найбільш необхідними роз'яснення стають, коли виникають нові загрози, такі як резонансні соціальні або політичні події (наприклад, весілля знаменитостей), котрі зловмисники, ймовірно, використають у своїй соціальній інженерії. З метою уникнення дублювання зусиль та суперечливої інформації розповсюджувати роз'яснення щодо комп'ютерної безпеки в організації повинен лише один підрозділ.

  Навчання та обізнаність. Навчання та обізнаність є так званими мультиплікаторами, які помножують ресурси – чим більше користувачі й технічний персонал знають про виявлення інцидентів, звітування та реагування на них, тим меншим буде виснаження команди реагування на інциденти. Цю інформацію можна розповсюдити багатьма засобами: на семінарах, вебсайтах, в інформаційних розсилках, на плакатах і навіть за допомогою наклейок на моніторах і ноутбуках.

- **Обмін інформацією.** Команди реагування на інциденти часто беруть участь у групах обміну інформацією, таких як ISAC або регіональні партнерства. Отже, команди реагування на інциденти часто керують процесом обміну інформацією про інциденти в організації. Це включає роботу щодо узагальнення інформації, пов'язаної з інцидентами, ефективний обмін цією інформацією з іншими організаціями, а також забезпечення обміну відповідною інформацією всередині підприємства.

---

17 Див.NIST SP 800-94, *Посібник щодо систем виявлення та запобігання атакам/вторгненням (IDPS)* для отримання додаткової інформації щодо технологій IDPS. Його можна знайти за посиланням: .http://csrc.nist.gov/publications/PubsSPs.html#800-94

18 Команди повинні впевнитись, що формулювання в роз'ясненнях чи рекомендаціях не будуть звинувачувати жодну особу чи організацію у проблемах безпеки. Команди повинні зустрітися з юридичними радниками, щоб обговорити можливу необхідність включення до роз'яснень пункту відмови від відповідальності, вказуючи, що команда та організація не несуть відповідальності щодо точності інформації у роз'ясненнях. Це найбільш доречно, коли роз'яснення можуть надсилатися підрядникам, постачальникам та іншим стороннім особам, які не працюють в організації та є користувачами її обчислювальних ресурсів.

19 http://nvd.nist.gov/

2.6 Рекомендації

Основні рекомендації щодо організації потенціалу з управління інцидентами комп'ютерної безпеки, представлені в цьому пункті, наведено нижче.

- **Створіть офіційний потенціал реагування на інциденти.** Організації повинні бути готові швидко та ефективно реагувати на злам захисту інформації та комп'ютерної безпеки. Відповідно до вимог Федерального закону США про управління інформаційною безпекою (FISMA), федеральні органи, відомства та агенції зобов'язані створити потенціал реагування на інциденти.

- **Створіть політику реагування на інцидент.** Політика реагування на інциденти виступає основою програми реагування на інциденти. Вона визначає, які події вважаються інцидентами, встановлює організаційну структуру для реагування на інциденти, визначає розподіл ролей та зон відповідальності, а також, серед інших моментів, перераховує вимоги до звітування про інциденти.

- **Розробіть план реагування на інциденти на основі політики реагування на інцидент.** План реагування на інциденти забезпечує дорожню карту для реалізації програми реагування на інциденти на основі політики організації. У плані зазначено як короткострокові, так і довгострокові цілі програми, включаючи метрики (індикатори) для вимірювання програми. План реагування на інциденти також повинен вказувати, наскільки часто слід проводити навчання фахівців, що займаються управлінням інцидентом, і вимоги до фахівців з управління інцидентами.

- **Розробіть порядок реагування на інциденти.** Порядок реагування на інциденти містить детальні кроки для реагування на інциденти. Порядок має охоплювати всі фази процесу реагування на інциденти. Порядок повинен ґрунтуватися на політиці та плані реагування на інциденти.

- **Встановіть політику та порядок щодо обміну інформацією про інциденти.** Організації потрібно повідомляти про відповідні подробиці інциденту стороннім особами / третім сторонам, таким як ЗМІ, органи правопорядку та організації, котрим звітують щодо інцидентів. Команді реагування на інциденти необхідно обговорити це зі службою із зв'язків з громадськістю, юридичним відділом та керівництвом організації, щоб встановити політику та порядок обміну інформацією. Команда має дотримуватися чинної політики організації щодо взаємодії із ЗМІ та іншими сторонніми особами / третіми сторонами.

- **Надайте відповідній організації відповідну інформацію про інциденти.** Федеральні цивільні органи, відомства та агенції зобов'язані повідомляти про інциденти до US-CERT; інші організації можуть зв'язатися з US-CERT та/або зі своїми ISAC. Звітування корисне, оскільки US-CERT та ISAC використовують дані, представлені у звітах, для надання інформації щодо нових загроз і тенденцій інцидентів сторонам, які звітують.

- **Враховуйте відповідні чинники при виборі моделі команди реагування на інциденти.** Організації повинні ретельно зважувати переваги та недоліки кожної можливої моделі структури команди та моделі кадрового забезпечення в контексті потреб організації та наявних ресурсів.

- **Для команди реагування на інциденти відбирайте людей із відповідними навичками.** Надійність та кваліфікація команди значною мірою залежать від технічних навичок її учасників та їхніх здібностей до критичного мислення. Критично важливі технічні навички включають адміністрування системи, адміністрування мережі, програмування, технічну підтримку та виявлення вторгнень.

  Робота в команді та навички комунікації також необхідні для ефективного управління інцидентами. Усі учасники команди повинні пройти необхідне навчання.

- **Визначте інші структурні підрозділи / команди в організації, участь яких може знадобитися під час управління інцидентами.** Будь-яка команда реагування на інцидент покладається на знання, досвід, судження та здібності інших команд, зокрема керівництва, фахівців з інформаційної безпеки, ІТ-підтримки, юридичного відділу, служби зв'язків із громадськістю та відділу адміністративно-господарського забезпечення.

- **Визначте, які послуги має надавати команда.** Незважаючи на те, що основним завданням команди є реагування на інциденти, більшість команд виконують додаткові функції. Приклади включають моніторинг датчиків виявлення атак/втручання, розповсюдження роз'яснень щодо безпеки та навчання користувачів щодо безпеки.

3. Управління інцидентами

Процес реагування на інциденти має кілька етапів. Початковий етап передбачає створення та проведення навчання для команди реагування на інциденти, а також придбання необхідних інструментів і ресурсів. Під час підготування організація також намагається обмежити кількість інцидентів, які можуть виникнути, вибираючи та впроваджуючи перелік дій, тобто засобів контролю, на основі результатів оцінювання ризиків. При цьому, після впровадження цих дій неминуче зберігатиметься залишковий ризик. Отже, виявлення порушень цілісності безпеки необхідно, щоб попереджати організації щоразу, коли трапляються інциденти. Відповідно до градації інциденту, організація може пом'якшити наслідки інциденту, стримуючи його та в кінцевому підсумку відновлюючись після нього. Під час цього етапу часто необхідно повернутися до виявлення та аналізу, наприклад під час ліквідації інциденту з використанням зловмисного програмного забезпечення перевірити, чи інші хости не заражені зловмисним програмним забезпеченням. Після того, як управління інцидентом належно проведене, організація видає звіт, у якому детально описуються причина і витрати на ліквідацію наслідків інциденту, а також кроки, які організація має вжити для запобігання майбутнім інцидентам. У цьому пункті детально описано основні етапи процесу реагування на інциденти – підготування, виявлення та аналіз, стримування, ліквідація наслідків та відновлення, а також заходи після інциденту.
Рисунок 3-1 ілюструє життєвий цикл реагування на інциденти.

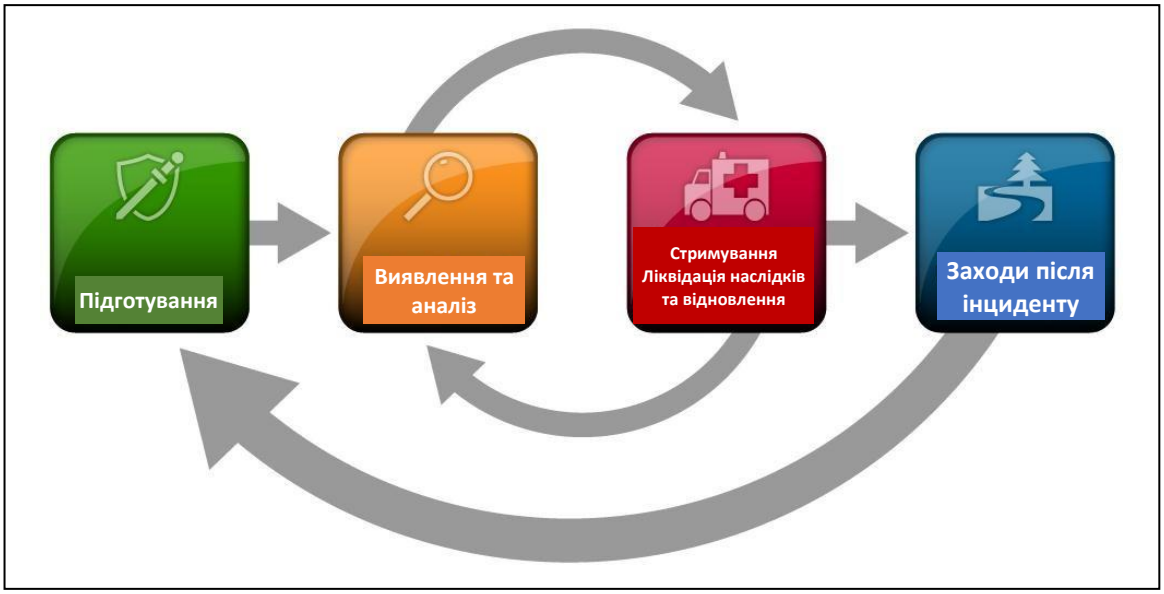

Рисунок 3-1. Життєвий цикл реагування на інциденти

3.1 Підготування

Методології реагування на інциденти, як правило, наголошують на підготуванні – не лише на створенні потенціалу реагування на інциденти, щоб організація була готова реагувати на інциденти, але й на запобіганні інцидентам шляхом забезпечення достатнього рівня безпеки систем, мереж і застосунків. Незважаючи на те, що команда реагування на інциденти, як правило, не відповідає за запобігання інцидентам, вона є фундаментальною частиною успіху програм реагування на інциденти. У цьому пункті представлено основні поради щодо підготування до інцидентів та щодо запобігання інцидентам.

3.1.1 Підготування до управління інцидентами

У переліках, представлених нижче, наведено приклади доступних інструментів і ресурсів, які можуть бути корисними під час управління інцидентами. Ці переліки мають бути відправною точкою для обговорення того, які інструменти та ресурси потрібні фахівцям з управління інцидентами в організації. Наприклад, смартфони – це один зі способів забезпечити стійкі механізми комунікацій та координації у надзвичайних ситуаціях. Організація повинна мати декілька (окремих і різних) механізмів комунікації та координації на випадок відмови одного механізму.

Комунікації та засоби фахівців з управління інцидентами:

- **Контактна інформація** щодо учасників команди та інших осіб в організації та за її межами (основні та резервні контакти), наприклад органи правопорядку та інші команди реагування на інциденти; інформація може включати номери телефонів, адреси електронної пошти, відкриті ключі шифрування (відповідно до програмного забезпечення для шифрування, яке описане нижче) та інструкції щодо підтвердження особи
- **Інформація щодо виклику за вимогою** для інших команд в організації, включаючи інформацію про передавання даних на вищій рівень
- **Механізми звітування чи інформування про інциденти**, такі як номери телефонів, адреси електронної пошти, онлайн-форми та безпечні системи обміну миттєвими повідомленнями, які користувачі можуть використовувати для інформування про підозру, що стався інцидент; принаймні один механізм повинен дозволяти людям повідомляти про інциденти анонімно
- **Система відстеження проблем** для відстеження інформації про інцидент, статус тощо.
- **Смартфони**, котрими користуються учасники команди для надання підтримки в неробочий час і спілкування на місці
- **Програмне забезпечення для шифрування**, яке використовується для комунікацій між учасниками команди, всередині організації та зі сторонніми особами / третіми сторонами; у випадку федеральних органів, відомств та установ програмне забезпечення має використовувати перевірений FIPS алгоритм шифрування[20]
- **Оперативний центр** для централізованого зв'язку та координації; якщо приміщення оперативного центру не потрібне на постійній основі або є непрактичним, команда повинна створити порядок проведення закупівель для організації тимчасового оперативного центру, коли це необхідно
- Захищене складське приміщення для зберігання доказів та інших конфіденційних матеріалів

Апаратне та програмне забезпечення для аналізу інцидентів:

- **Цифрові криміналістичні робочі станції[21] та/або пристрої резервного копіювання** для створення образів дисків, збереження файлів журналів та інших відповідних даних про інцидент
- Ноутбуки для таких видів діяльності, як аналіз даних, аналіз пакетів і написання звітів
- **Запасні робочі станції, сервери та мережеве обладнання або віртуалізовані еквіваленти**, які можна використовувати для багатьох цілей, наприклад для відновлення резервних копій і випробування зловмисних програм

- Порожній знімний носій
- **Портативний принтер**, щоб друкувати копії файлів журналів та інших доказів з немережевих систем
- **Аналізатори трафіку, або сніфери, та аналізатори протоколів** для захоплення та аналізу трафіку мережі
- **Цифрове криміналістичне програмне забезпечення** для аналізу образів дисків
- **Знімний носій** з надійними версіями застосунків, котрі будуть використовуватися для збору доказів із систем
- **Обладнання та матеріали для збору доказів**, включаючи записні книжки в твердій обкладинці, цифрові камери, обладнання для звукозапису, бланки для відстеження руху речових доказів, слідчі валізи та бирки для речових доказів, а також стрічку для маркування доказів, щоб зберегти докази для можливих юридичних дій

Ресурси для аналізу інциденту:

- **Переліки портів**, включаючи порти, які частіше за все використовують, і порти із троянськими програмами
- **Документація** для операційних систем, застосунків, протоколів, а також «антивірусних» продуктів та продуктів для виявлення вторгнень
- **Діаграми мережі та списки критично важливих активів**, наприклад сервери баз даних
- Поточний базовий рівень для очікуваних дій в мережі, системі та застосунках
- **Криптографічні хеші** критично важливих файлів[22] для прискорення аналізу інцидентів,

перевірки та ліквідації наслідків

Програмне забезпечення для пом'якшення наслідків інцидентів:

- **Доступ до образів** із «чистими» файлами для встановлення ОС і застосунків для відновлення й оновлення

Багато команд реагування на інциденти створюють так званий «набір парашутиста», який є переносним кейсом, що містить матеріали, котрі можуть знадобитися під час розслідування. «Набір парашутиста» повинен завжди бути підготовлений для роботи. «Набори парашутиста» містять багато тих самих предметів та інструментів, які перераховані вище у маркерних списках. Наприклад кожен «набір парашутиста» зазвичай включає ноутбук із завантаженим на нього відповідним програмним забезпеченням (наприклад, аналізатори трафіку, тобто сніфери, засоби цифрової криміналістики). Інші важливі матеріали включають пристрої резервного копіювання, чисті носії, а також основне мережеве обладнання та кабелі. Оскільки мета «набору парашутиста» полягає в тому, щоб сприяти швидшому реагуванню, команда не має позичати інструменти та засоби з «набору парашутиста».

---

[20] FIPS 140-2, *Вимоги до безпеки для криптографічних модулів*, .http://csrc.nist.gov/publications/PubsFIPS.html

[21] Цифрова криміналістична робоча станція спеціально розроблена, щоб допомогти фахівцям, які займаються управлінням інцидентами, в отриманні та аналізі даних. Ці робочі станції зазвичай містять набір зовнішніх (знімних) жорстких дисків, які можна використовувати для зберігання доказів.

[22] Проєкт «Національна довідкова бібліотека програмного забезпечення» (National Software Reference Library або NSRL) веде записи хешів для різних файлів, зокрема дані щодо операційних систем, застосунків та файлів із графічними зображеннями. Хеші можна завантажити за посиланням .http://www.nsrl.nist.gov/

Кожен фахівець з управління інцидентами повинен мати доступ щонайменше до двох обчислювальних пристроїв (наприклад, ноутбуків). Один ноутбук, наприклад той, що із «набору парашутиста», слід використовувати для аналізу трафіку, аналізу зловмисного програмного забезпечення та всіх інших дій, які можуть зашкодити ноутбуку, який їх виконує. Перш ніж використовувати цей ноутбук для іншого інциденту, його слід очистити і перевстановити все програмне забезпечення. Слід зазначити, що оскільки це ноутбук спеціального призначення, він, імовірно, використовує програмне забезпечення, відмінне від стандартних корпоративних інструментів і конфігурацій, і, коли це можливо, фахівцям з управління інцидентами слід дати можливість вказувати основні технічні вимоги до цих ноутбуків спеціального призначення для проведення розслідування. Окрім ноутбука для проведення розслідування кожен фахівець з управління інцидентами також повинен мати стандартний ноутбук, смартфон чи інший комп'ютерний пристрій для написання звітів, прочитання електронної пошти та виконання інших обов'язків, не пов'язаних з аналізом інцидентів на практиці.

Вправи з моделюванням інцидентів також можуть бути дуже корисними для підготовки персоналу до управління інцидентами; для отримання додаткової інформації про вправи див. NIST SP 800-84 [23] і Додаток А – для інформації про приклади сценаріїв вправ.

3.1.2 Попередження інцидентів

Підтримка достатньо низької кількості інцидентів дуже важлива для захисту бізнес-процесів організації. Якщо засобів контролю безпеки буде недостатньо, може статися велика кількість інцидентів, що перевантажить команду реагування на інциденти. Це може призвести до повільного і неповного реагування, що призведе до більших негативних наслідків для бізнесу (наприклад, більшої шкоди та більш тривалого періоду обслуговування та недоступності даних).

Надання конкретних порад щодо захисту мереж, систем і застосунків не входить до тематики цього документа. Незважаючи на те, що команди реагування на інциденти, як правило, не несуть відповідальності за безпеку ресурсів, вони можуть виступати за впровадження надійних практик безпеки. Команда реагування на інциденти може виявити проблеми, про які організація в іншому випадку не дізналася б; команда може відігравати визначальну роль в оцінюванні ризику та навчанні, виявляючи прогалини. Інші документи вже містять рекомендації щодо загальних понять безпеки і керівних настанов щодо операційної системи та застосунків.[24] Натомість, у наступному тексті наведено короткий огляд деяких основних методичних рекомендацій для захисту мереж, систем і застосунків:

[23] *Посібник щодо програм тестування, навчання та тренування для планів і можливостей IT,* http://csrc.nist.gov/publications/PubsSPs.html#800-84

[24] http://csrc.nist.gov/publications/PubsSPs.htmlнадає посилання на Спеціальні видання стандартів NIST з комп'ютерної безпеки, які включають документи про основи безпеки операційної системи та застосунків.

- **Оцінювання ризиків.** Періодичне оцінювання ризиків систем і застосунків має визначати, до яких ризиків призводять комбінації загроз і вразливостей.[25] Це повинно включати розуміння відповідних загроз, включаючи загрози, характерні для організації. Для всіх ризиків має бути проведена пріоритезація, і ризики можна пом'якшити, передати або прийняти, доки не буде досягнуто обґрунтованого загального рівня ризику. Ще одна перевага регулярного оцінювання ризику полягає в тому, що визначаються критично важливі ресурси, а це допомагає персоналу зосередитися на моніторингу цих ресурсів та заходах реагування.[26]

- **Безпека хостів.** Усі хости повинні бути належно захищені за допомогою стандартних налаштувань. Додатково до того, що на кожному хості мають бути належно налаштовані засоби для усунення вразливостей (патчі), хости також повинні бути налаштовані на дотримання принципу найменших привілеїв – надання користувачам лише тих прав доступу, що необхідні для виконання завдань, на які вони уповноважені. На хостах має бути увімкнений аудит і має відбуватися журналювання важливих подій, пов'язаних із безпекою. Безпеку хостів та їх налаштування слід постійно контролювати.[27] Багато організацій використовують Протокол автоматизації управління даними безпеки (SCAP)[28], виражені контрольні списки щодо налаштування операційної системи та застосунків для допомоги у безперебійному й ефективному захисті хостів.[29]

- **Безпека мережі.** Периметр мережі має бути налаштований так, щоб забороняти будь-яку діяльність, яка прямо не дозволена. Це включає в себе захист усіх точок підключення, таких як віртуальні приватні мережі (VPN) і виділені підключення з іншими організаціями.

- **Запобігання зловмисному програмному забезпеченню.** Програмне забезпечення для виявлення та припинення дії зловмисного програмного забезпечення має бути впроваджене по всій організації. Захист від зловмисного програмного забезпечення слід впровадити на рівні хоста (наприклад, операційні системи сервера та робочої станції), на рівні сервера програм (наприклад, сервер електронної пошти, вебпроксі) і на рівні клієнта програми (наприклад, клієнти електронної пошти, клієнти сервісів миттєвих повідомлень).[30]

- **Обізнаність і навчання користувачів.** Користувачі мають бути ознайомлені з політикою та порядком щодо належного використання мереж, систем і застосунків. Відповідним досвідом, засвоєним з попередніх інцидентів, також слід поділитися з користувачами, щоб вони могли побачити, як їхні дії можуть вплинути на організацію. Підвищення поінформованості користувачів щодо інцидентів має зменшити їх частоту. Слід провести навчання IT-персоналу, щоб фахівці могли підтримувати свої мережі, системи та застосунки відповідно до стандартів безпеки організації.

---

25 Рекомендації щодо оцінювання ризику доступні у NIST SP 800-30, *Керівні настанови щодо оцінювання ризиків*, за посиланням .http://csrc.nist.gov/publications/PubsSPs.html#800-30-Rev1

26 Інформацію про визначення критично важливих ресурсів представлено у FIPS 199, *Стандарти категоризації безпеки федеральної інформації та федеральних інформаційних систем*, за посиланням .http://csrc.nist.gov/publications/PubsFIPS.html

27 Для отримання додаткової інформації щодо безперервного моніторингу, див. NIST SP 800-137, *Безперервний моніторинг інформаційної безпеки для федеральних інформаційних систем і організацій* (http://csrc.nist.gov/publications/PubsSPs.html#800-137).

28 Додаткову інформацію щодо SCAP можна дізнатися у NIST SP 800-117 Перша редакція, *Посібник щодо прийняття та використання Протоколу автоматизації управління даними безпеки (SCAP) Версія 1.2* (http://csrc.nist.gov/publications/PubsSPs.html#800-117).

29 NIST має репозиторій із контрольними переліками вимог щодо безпеки за посиланням .http://checklists.nist.gov/

30 Додаткову інформацію щодо запобігання зловмисному програмному забезпеченню можна отримати в NIST SP 800-83, *Посібник щодо запобігання та управління інцидентами з використанням зловмисного програмного забезпечення* (http://csrc.nist.gov/publications/PubsSPs.html#800-83).

3.2 Виявлення та аналіз

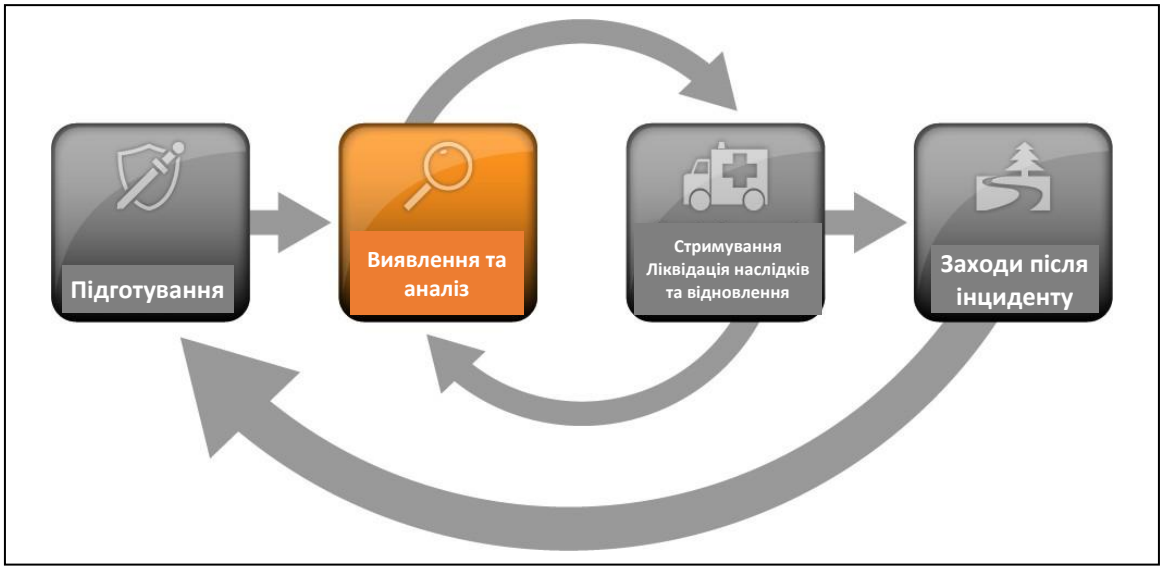

Рисунок 3-2. Життєвий цикл реагування на інциденти (виявлення та аналіз)

3.2.1 Вектори атак

Є незліченна кількість способів, як можуть відбуватися інциденти, тому неможливо розробити покрокові інструкції для управління кожним окремим інцидентом. Загалом, організації мають бути готові впоратися з будь-якими інцидентами, але повинні сфокусуватися на тому, щоб бути готовими до інцидентів, які використовують поширені вектори атак. Різні типи інцидентів вимагають різних стратегій реагування. Наведені нижче вектори атаки не призначені для надання остаточної класифікації інцидентів; скоріше, вони просто надають перелік загальних методів атаки, які можуть бути використані як основа для визначення більш конкретного порядку управління інцидентами.

- **Зовнішній/знімний носій:** Атака, здійснена зі знімного носія або периферійного пристрою, наприклад поширення зловмисного коду на систему із зараженого USB-флеш-накопичувача.
- **Виснаження:** Атака, що використовує методи «грубої сили» для компрометації, погіршення або знищення систем, мереж або служб (наприклад, DDoS-атака, спрямована на погіршення або заборону доступу до служби або застосунку; атака із використанням «грубої сили», спрямована на механізм автентифікації, такий як паролі, CAPTCHA, або цифрові підписи).
- **Вебресурс:** Атака, здійснена з вебсайту або вебзастосунку, наприклад атака з міжсайтовим скриптингом, що використовується для викрадення облікових даних або переходу на сайт, який використовує вразливість браузера та встановлює зловмисне програмне забезпечення.
- **Електронна пошта:** Атака, здійснена через електронний лист або файл, прикріплений до електронної пошти, наприклад, код експлойту, замаскований під прикріплений документ, або посилання на зловмисний вебсайт у основному тексті повідомлення електронної пошти.
- **Використання фіктивних осіб:** Атаки, що передбачають заміну чогось сприятливого чи корисного на щось шкідливе, наприклад спуфінг, атаки через посередника або атаки «людина посередині», шахрайські точки бездротового доступу та атаки з додаванням мови структурованих запитів (SQL) – усі вони включають видавання себе за іншу особу.

- **Неналежне використання:** Будь-який інцидент, що виник у результаті порушення авторизованим користувачем затвердженої політики безпеки організації, за винятком вищевказаних категорій. Наприклад користувач встановлює програмне забезпечення для обміну файлами, що призводить до витоку конфіденційних даних, або користувач здійснює незаконні дії в системі.
- **Втрата або викрадення обладнання:** Втрата або викрадення комп'ютерного пристрою або носія, котрий використовується організацією, наприклад ноутбука, смартфона або токена автентифікації.
- **Інше:** Атаки, які не вписуються в інші категорії.

Цей пункт сконцентрований на методичних рекомендаціях управління інцидентами будь-якого типу. До сфери застосування цього видання не входять деталізовані поради на основі векторів атаки; такі рекомендації буде представлено в окремих виданнях, що стосуються інших питань управління інцидентами, таких як NIST SP 800-83 щодо запобігання та управління інцидентами з використанням зловмисного програмного забезпечення.

3.2.2 Ознаки інциденту

Найскладнішою частиною процесу реагування на інцидент для багатьох організацій є точне виявлення та оцінювання можливих інцидентів – визначення того, чи насправді стався інцидент, і, якщо так, тип, розмах і масштабність проблеми. Цей процес є таким складним через поєднання трьох чинників:

- Інциденти можна виявити багатьма різними способами, рівень деталізації та точності також може відрізнятися. Можливості автоматизованого виявлення включають IDPS на базі мережі та хоста, антивірусне програмне забезпечення та аналізатори журналів. Інциденти також можна виявити вручну, наприклад розглядаючи проблеми, про які повідомляють користувачі. У деяких інцидентів ознаки явні, їх можна легко виявити, тоді як інші виявити майже неможливо.
- Потенційних ознак інцидентів, як правило, дуже багато – наприклад організація нерідко отримує тисячі або навіть мільйони сповіщень від детекторів (датчиків) виявлення атак/втручань на день. (див. пункт 3.2.4 для отримання інформації про аналіз таких сповіщень.)
- Для правильного та ефективного аналізу даних, пов'язаних з інцидентами, необхідні глибокі спеціалізовані технічні знання та великий досвід.

Ознаки інциденту поділяються на дві категорії: прекурсори та індикатори. *Прекурсор* – це ознака того, що інцидент може статися в майбутньому. *Індикатор* – це ознака того, що інцидент, можливо, вже стався або, можливо, відбувається саме зараз.

З погляду цілі, більшість атак не мають жодних прекурсорів, які можна ідентифікувати або виявити. Якщо ж прекурсори виявлено, в організації може з'явитися можливість запобігти інциденту шляхом зміни заходів убезпечення, для захисту цілі від атаки. Мінімально можливий варіант – коли організація уважніше стежить за всім, що пов'язане з ціллю. Прикладами прекурсорів є:

- Записи журналу вебсервера, які показують використання сканера вразливостей
- Оголошення про новий експлойт, ціллю якого є вразливість поштового сервера організації
- Погроза з боку групи, яка стверджує, що вона нападе на організацію.

Тоді як прекурсори трапляються порівняно рідко, індикатори дуже поширені. Існує надто багато типів індикаторів, щоб усі без винятку перерахувати, але деякі приклади наведено нижче:

- Детектор (датчик) виявлення вторгнень у мережу попереджає про спробу переповнення буфера на сервері бази даних.
- Сповіщення антивірусного програмного забезпечення, коли воно виявляє, що хост заражений зловмисним програмним забезпеченням.
- Адміністратор системи бачить назву файлу з незвичайними символами.
- Хост записує у своєму журналі зміни конфігурації, які потребують ведення контролю.
- Застосунок реєструє кілька невдалих спроб входу з незнайомої віддаленої системи.
- Адміністратор електронної пошти бачить велику кількість відхилених електронних листів із підозрілим вмістом.
- Адміністратор мережі помічає незвичне відхилення від типових потоків мережевого трафіку.

3.2.3 Джерела прекурсорів та індикаторів

Для визначення прекурсорів та індикаторів використовується багато різних джерел, серед яких найпоширенішими є сповіщення програмного забезпечення, що сприяє комп'ютерній безпеці, журнали, відкрита інформація та люди. У таблиці 3-2 представлено поширені джерела прекурсорів та індикаторів для кожної категорії.

Таблиця 3-1. Поширені джерела прекурсорів та індикаторів

Джерело	Опис
Сповіщення	
IDPS	Продукти систем виявлення та запобігання атакам/вторгненням (IDPS) ідентифікують підозрілу активність і записують відповідні дані щодо неї, включаючи дату і час виявлення атаки, тип атаки, IP-адреси відправника та отримувача, а також ім'я користувача (за необхідності та якщо воно відоме). Більшість продуктів IDPS ґрунтуються на сигнатурному аналізі, використовуючи базу сигнатур атак для виявлення зловмисної діяльності; сигнатури повинні оновлюватися, щоб можна було виявляти нові види атак. Програмне забезпечення IDPS часто видає помилки першого роду (хибно позитивні) – сповіщає користувача, що відбувається зловмисна діяльність, хоча насправді її не було. Аналітики повинні вручну перевіряти сповіщення IDPS, уважно переглядаючи записи із допоміжними даними або одержуючи дані, пов'язані зі сповіщеннями, з інших джерел.[31]
SIEM	Продукти систем управління інформацією та подіями безпеки (SIEM) подібні до продуктів IDPS, але вони генерують сповіщення на основі аналізу даних журналу (див. нижче).
Антивірусне та антиспамове програмне забезпечення	Антивірусне програмне забезпечення виявляє різні форми небажаного (шкідливого) програмного забезпечення, видає сповіщення та запобігає зараженню (модифікації) хостів зловмисним кодом. Сучасні антивірусні продукти ефективні для зупинки багатьох варіантів шкідливого програмного забезпечення, якщо їхні сигнатури оновлюються. Антиспамове програмне забезпечення використовується для виявлення спаму та запобігання його потраплянню до поштових скриньок користувачів. Спам може містити зловмисне програмне забезпечення, фішингові атаки та інший шкідливий вміст, тому сповіщення від антиспамового ПЗ можуть свідчити про спроби атаки.
Програмне забезпечення для перевірки файлів на предмет порушень цілісності	Програмне забезпечення для перевірки файлів на предмет порушень цілісності може виявити модифікації, внесені у важливі файли під час інцидентів. Воно використовує алгоритм хешування для отримання криптографічної хеш-суми для кожного визначеного файлу. Якщо файл змінено і перераховується хеш-сума, існує надзвичайно висока ймовірність того, що нова хеш-сума не відповідатиме старій хеш-сумі. За допомогою регулярного перерахунку хеш-сум та порівняння їх із попередніми значеннями, можна виявити зміни/модифікації у файлах.

Моніторингові сервіси від третіх сторін	Треті сторони пропонують широкий спектр моніторингових сервісів (служб) на умовах оформлення підписки. Прикладом є сервіси з виявлення шахрайства, які сповіщають організацію, якщо її IP-адреси, доменні імена тощо пов'язані з поточними інцидентами, до яких так чи інакше залучені інші організації. Існують також безкоштовні «чорні списки» з подібною інформацією, що оновлюються в режимі реального часу. Іншим прикладом моніторингового сервісу від третьої сторони є список розсилання сповіщень CSIRC; такі списки часто доступні лише іншим командам реагування на інциденти.
Журнали	
Журнали операційної системи, служб і застосунків	Журнали операційних систем, служб і застосунків (зокрема дані, пов'язані з аудитом безпеки) часто набувають дуже великого значення, коли стається інцидент, наприклад у них можна побачити до яких облікових записів було отримано доступ і які саме дії були виконано. Організації повинні вимагати базовий рівень журналювання для всіх систем і рівень вище базового для критично важливих систем. Журнали можна використовувати для аналізу за допомогою співвіднесення інформації про події. Залежно від інформації про подію можна створити сповіщення, що вказує на інцидент. У пункті 3.2.4 обговорюється значення централізованого журналювання.
Журнали мережевих пристроїв	Журнали мережевих пристроїв, таких як брандмауери (фаєрволи) та маршрутизатори, зазвичай не є основним джерелом прекурсорів чи індикаторів. Незважаючи на те, що ці пристрої зазвичай налаштовані на реєстрацію спроб заблокованого підключення, вони надають мало інформації про характер такої активності. Утім, вони можуть бути цінними для визначення мережевих тенденцій та для кореляції з подіями, виявленими іншими пристроями.
Потоки трафіку в мережах	Потік трафіку в мережі – це окремий сеанс зв'язку, який відбувається між хостами. Маршрутизатори та інші мережеві пристрої можуть надавати інформацію про потік трафіку, яку можна використовувати для виявлення аномальної активності мережі, спричиненої шкідливим програмним забезпеченням, вилученням даних та іншими зловмисними діями. Існує багато стандартів для форматів даних мережевого трафіку, включаючи NetFlow, sFlow та IPFIX.
Відкрита інформація	
Інформація про нові вразливості та експлойти	Відстеження нових вразливостей та експлойтів може запобігти виникненню деяких інцидентів і допомогти у виявленні та аналізі нових атак. Національна база даних вразливостей (NVD) містить інформацію про вразливості.[32] Такі організації, як US-CERT[33] та CERT®/CC періодично надають інформацію про оновлення загроз на брифінгах, у вебпублікаціях і списках розсилання.
Люди	
Люди з організації	Користувачі, адміністратори систем, адміністратори мережі, персонал служби безпеки та інші особи з організації можуть повідомляти про ознаки інцидентів. Усі такі звіти необхідно перевіряти. Один із підходів полягає у тому, щоб запитати людей, які надають таку інформацію, наскільки вони впевнені в її достовірності. Записи щодо цього оцінювання разом із наданою інформацією можуть значно допомогти під час аналізу інцидентів, особливо якщо виявлено суперечливі дані.
Люди з інших організацій	До повідомлень чи звітів про інциденти, які надходять ззовні, слід поставитися серйозно. Наприклад з організацією може зв'язатися сторона, яка стверджує, що система в організації здійснює атаку на її системи. Зовнішні користувачі також можуть повідомляти про інші індикатори, наприклад неробочу вебсторінку або недоступну службу. Інші команди реагування на інциденти також можуть повідомляти про інциденти. Важливо, щоб були механізми, за допомогою яких зовнішні сторони зможуть повідомляти чи звітувати про індикатори, а відповідно навчений персонал ретельно ці механізми контролював. Цей процес може бути настільки ж простим, як налаштування номера телефону та адреси електронної пошти на автоматичне пересилання повідомлень до служби підтримки.

[31] Див. NIST SP 800-94, Керівні настанови *щодо систем виявлення та запобігання атакам/вторгненням,* для отримання додаткової інформації щодо продуктів IDPS. Його можна знайти за посиланням: .http://csrc.nist.gov/publications/PubsSPs.html#800-94

3.2.4 Аналіз інциденту

Якби кожен прекурсор або індикатор був гарантовано точним, то виявляти й аналізувати інциденти було б легко. На жаль, це не так. Наприклад індикатори, надані користувачем, такі як скарга на недоступність сервера, часто є недостовірними. Системи виявлення вторгнень можуть видавати помилки першого роду (хибно позитивні) – недостовірні індикатори. Ці приклади демонструють, що саме робить виявлення та аналіз інцидентів настільки складним: в ідеалі кожен індикатор слід спочатку оцінити, щоб визначити, чи він аргументований. Ситуацію погіршує той факт, що загальна кількість індикаторів може становити тисячі чи мільйони на день. Вибрати з усіх індикаторів аргументовані та за ними знайти реальні інциденти, пов'язані з безпекою, які насправді відбулися, може бути непростим завданням.

Навіть якщо індикатор точний, це не обов'язково означає, що інцидент дійсно стався. Деякі індикатори, такі як збій сервера або модифікація критичних файлів, можуть статися з кількох причин, окрім інциденту, пов'язаного з безпекою, включаючи людський фактор. Однак, враховуючи наявність індикаторів, цілком обґрунтовано можна підозрювати, що інцидент може статися, і діяти відповідно. Іноді під час визначення того, чи конкретна подія насправді є інцидентом, слід просто керуватися розсудливістю. Для прийняття рішення може знадобитися співпрацювати з іншим технічним персоналом та фахівцями з інформаційної безпеки. У багатьох випадках ситуацією слід управляти та все одно вирішувати її, незалежно від того, чи вона пов'язана з безпекою, чи ні. Наприклад якщо в організації зникає підключення до інтернету кожні 12 годин і ніхто не знає, з яких причини, працівники захочуть вирішити проблему з однаковою швидкістю і використовуватимуть однакові ресурси для діагностики проблеми, незалежно від причин її виникнення.

Деякі інциденти легко виявити, наприклад явно неробочу вебсторінку. Однак багато інцидентів не пов'язані з такою явною «симптоматикою». Невеличкі ознаки, такі як одна зміна в одному файлі конфігурації системи, можуть бути єдиними ознаками того, що стався інцидент. Під час управління інцидентами виявлення може бути найскладнішим завданням. Фахівці з управління інцидентами відповідають за аналіз неоднозначних, суперечливих і неповних ознак, щоб визначити, що саме сталося. Незважаючи на те, що існують технічні рішення, які можуть полегшити процес виявлення, найкращий спосіб – сформувати команду високодосвідчених і висококваліфікованих працівників, які зможуть ефективно та результативно аналізувати прекурсори та індикатори та вживати відповідних заходів. Без добре підготовленого та кваліфікованого персоналу виявлення та аналіз інцидентів проводитимуться неефективно, і ставатимуться помилки, які надто дорого коштують.

Команда реагування на інцидент повинна працювати швидко, щоб проаналізувати та підтвердити кожен інцидент, дотримуючись заздалегідь визначеного процесу та документуючи кожен зроблений крок. Коли команда вважає, що стався інцидент, вона має швидко виконати початковий аналіз, щоб визначити масштабність інциденту, наприклад, які мережі, системи чи застосунки постраждали; хто або що стало причиною інциденту; і як саме відбувається інцидент (наприклад, які інструменти або методи атаки використовуються, якими вразливими місцями скористалися). Початковий аналіз повинен надати команді достатньо інформації, щоб визначити пріоритети наступних заходів, таких як стримування (локалізація) інциденту та поглиблений аналіз наслідків інциденту.

[32] http://nvd.nist.gov/
[33] http://www.us-cert.gov/cas/signup.html

Виконання початкового аналізу та перевірки є складним. Нижче наведено рекомендації щодо полегшення та ефективнішого аналізу інцидентів:

- **Профілюйте мережі та системи.** *Профілювання* аналізує та вимірює динамічні показники очікуваної активності, щоб можна було легше ідентифікувати зміни у ній. Прикладами профілювання є запуск на хостах програмного забезпечення для перевірки файлів на предмет порушень цілісності, щоб отримати хеш-суми для критичних файлів, а також моніторинг використання пропускної здатності мережі, щоб визначити середній і піковий рівні використання в різні дні та в різний час. На практиці точно виявити інциденти, використовуючи більшість методів профілювання, важко. Організації повинні використовувати профілювання як один із кількох методів виявлення та аналізу.

- **Зрозумійте, як виглядає нормальна робота.** Учасники команди реагування на інциденти мають вивчати мережі, системи та застосунки, щоб добре зрозуміти, як для них виглядає нормальна робота, щоб легше було розпізнати аномалії. Жоден фахівець із управління інцидентами не матиме вичерпних знань про роботу всіх систем у середовищі, але фахівці з управління інцидентами повинні знати, які експерти можуть заповнити прогалини. Одним зі способів отримати ці знання є перегляд записів журналу та сповіщень щодо безпеки. Цей процес може бути нудним та довгим, якщо не використовується фільтрування для стиснення журналів до розумного розміру. Коли фахівці з управління інцидентами вже ознайомились із журналами та сповіщеннями, вони зможуть зосередитися на записах, котрі не мають пояснень, які зазвичай мають більше значення для дослідження. Часте проведення оглядів журналів підтримуватиме знання актуалізованими, а самі аналітики матимуть можливість помічати тенденції та зміни, які відбуваються з часом. Такі огляди також підказують аналітику, наскільки надійними є ті чи інші джерела.

- **Створіть політику зберігання журналів.** Інформація про інцидент може бути записана в кількох місцях, як-от брандмауер, IDPS та журнали застосунків. Створення та впровадження політики зберігання журналів, яка визначає, як довго мають зберігатися дані журналу, може виявитись надзвичайно корисним для аналізу, оскільки старі записи журналу можуть відображати розвідувальну активність або попередні випадки схожих атак. Іншою причиною зберігання журналів є те, що інциденти можуть бути виявлені лише через кілька днів, тижнів чи навіть місяців. Тривалість зберігання даних журналу залежить від кількох чинників, зокрема від політики зберігання даних організації та обсягу даних. Для отримання додаткових рекомендацій щодо ведення журналів див. NIST SP 800-92, *Керівні настанови щодо управління журналами, пов'язаними з комп'ютерною безпекою*.[34]

- **Співставляйте події між собою.** Докази інциденту можуть бути записані в кілька журналів, кожен із яких містить різні типи даних – в журналі брандмауера (фаєрвола) може міститися IP-адреса відправника, котру використовували, тоді як у журналі застосунку може міститися ім'я користувача. Мережева IDPS може виявити, що атаку було запущено щодо певного хоста, але вона може не знати, чи була атака успішною. Аналітику може знадобитися уважно дослідити журнали хоста, щоб визначити цю інформацію. Кореляція подій між багатьма джерелами індикаторів може виявитися неоціненною для перевірки того, чи відбувся конкретний інцидент.

[34] http://csrc.nist.gov/publications/PubsSPs.html#800-92

- **Стежте за тим, щоб усі годинники хоста були синхронізовані.** Такі протоколи, як Мережевий протокол часу (NTP), синхронізують годинники між хостами.[35] Кореляція подій стане складнішою, якщо пристрої, котрі повідомляють про події, мають неузгоджені налаштування годинників. З погляду доказів, краще мати послідовні часові позначки в журналах, наприклад мати три журнали, які показують, що атака сталася о 00:07:01 год., а не журнали, в яких зазначено, що атака сталася о 00:07:01 год., 00:10:35 год. та 23:07:06 год.

- **Підтримуйте в актуалізованому стані та використовуйте інформаційну базу знань.** База знань повинна містити інформацію, котра необхідна фахівцям з управління інцидентами для швидкого пошуку даних під час аналізу інцидентів. Незважаючи на те, що можна створити базу знань зі складною структурою, ефективним може бути й простий підхід. Текстові документи, електронні таблиці та порівняно прості бази даних забезпечують ефективні, гнучкі та зручні для пошуку механізми для обміну даними між учасниками команди. База знань також повинна містити різноманітну інформацію, включаючи роз'яснення щодо значущості й достовірності прекурсорів та індикаторів, таких як сповіщення IDPS, записи журналу операційної системи та коди помилок застосунку.

- **Використовуйте для проведення дослідження пошукові системи в інтернеті.** Пошукові системи в інтернеті можуть допомогти аналітикам знайти інформацію про нетипову діяльність. Наприклад аналітик може побачити деякі нетипові спроби підключення, спрямовані на порт TCP 22912. Пошук за ключовими словами «TCP», «порт» і «22912» може видати деякі результати, які містять журнали з подібною активністю або навіть пояснення щодо значення номера порту. Слід мати на увазі, що для дослідження потрібно використовувати окремі робочі станції, щоб мінімізувати ризик від проведення таких пошуків для організації.

- **Запустіть аналізатори трафіку (сніфери) для збору додаткових даних.** Інколи індикатори не фіксують достатню кількість детальних даних, щоб дати змогу фахівцю з управління інцидентами зрозуміти, що відбувається. Якщо інцидент відбувається в мережі, найшвидшим способом збору необхідних даних може бути перехоплення мережевого трафіку сніфером. Налаштування сніфера для відстеження трафіку, який відповідає заданим критеріям, має підтримувати необхідний об'єм даних і мінімізувати ненавмисне захоплення іншої інформації. Через занепокоєння питаннями конфіденційності деякі організації можуть вимагати, щоб фахівці з управління інцидентами подавали запити й отримували дозволи перед використанням сніферів.

- **Фільтруйте дані.** Насправді часу дійсно недостатньо, щоб переглянути і проаналізувати всі індикатори; як мінімум, слід розслідувати найбільш підозрілу активність. Однією з ефективних стратегій є фільтрування, коли виключаються категорії індикаторів, котрі виглядають незначними. Інша стратегія фільтрування полягає в тому, щоб показати лише ті категорії індикаторів, котрі є найбільш значущими; однак такий підхід несе значний ризик, оскільки нова та невідома зловмисна активність може не підпадати під одну з відібраних категорій індикаторів.

- **Звертайтеся по допомогу до інших.** Інколи команда не може повноцінно визначити причину та характер інциденту. Якщо команді бракує необхідної інформації для локалізації та ліквідації інциденту, їй слід проконсультуватись із внутрішніми ресурсами (наприклад, працівниками, які займаються питаннями інформаційної безпеки) і зовнішніми ресурсами (наприклад, US-CERT, іншими CSIRT, підрядниками, які мають досвід реагування на інциденти). Важливо точно визначити причину кожного інциденту, щоб його можна було повністю локалізувати і пом'якшити вразливості, котрими скористалися, з метою запобігання подібним інцидентам.

3.2.5 Документація щодо інциденту

Команда реагування на інцидент, яка підозрює, що стався інцидент, повинна негайно почати документувати всі факти, що стосуються інциденту.[36] Ефективним і простим засобом для цього є журнал,[37] але з цією метою також можуть підійти й ноутбуки, обладнання для звукозапису, а також цифрові камери.[38] Документування системних подій, розмов та змін у файлах, виявлених під час спостережень, може привести до ефективнішого та систематичнішого вирішення проблеми із нижчим ризиком припуститися помилок. Кожен крок, зроблений із моменту виявлення інциденту до моменту його остаточного вирішення, має бути задокументований і позначений часовою міткою. Кожен документ, що стосується інциденту, повинен бути датований і підписаний особами, які займаються управлінням інцидентом. Інформація такого характеру також може бути використана як доказ у суді, якщо є судове провадження. За можливості, фахівці з управління інцидентами повинні працювати в командах принаймні з двох осіб: одна людина може записувати і журналювати події, а інша людина виконує технічні завдання. У пункті 3.3.2 представлено більше інформації про докази.[39]

Команда реагування на інциденти повинна вести облік щодо стану інцидентів, а також щодо іншої відповідної інформації.[40] Використання застосунку або бази даних, наприклад системи відстеження проблем, допомагає упевнитись, що інцидентами належно управляють і вчасно їх вирішують. Система відстеження проблем повинна містити інформацію про:

- Поточний стан справ щодо інциденту (новий, триває, передано на розслідування, вирішений тощо)
- Коротку довідку щодо інциденту
- Індикатори, пов’язані з інцидентом
- Інші інциденти, пов’язані із цим інцидентом
- Дії, яких було вжито всіма особами, які залучені до управління цим інцидентом
- Рух речових доказів, якщо така інформація є
- Оцінювання наслідків, пов’язаних із інцидентом
- Контактна інформація інших причетних сторін (наприклад, власників системи, адміністраторів системи)
- Перелік доказів, зібраних під час розслідування інциденту
- Коментарі фахівців з управління інцидентами
- Подальші кроки, які необхідно буде зробити (наприклад, перебудувати хост, оновити застосунок).[41]

---

[35] Більше інформації щодо NTP можна знайти за посиланням .http://www.ntp.org/

[36] Фахівці з управління інцидентами повинні документувати лише факти щодо інциденту, а не особисті думки чи висновки. Суб'єктивні матеріали слід викладати у звітах про інциденти, а не представляти як докази.

[37] Якщо використовується журнал, бажано, щоб журнал був прошитий, а фахівці з управління інцидентами пронумерували сторінки, писали чорнилом, і тримали журнал цілісним (це означає, що не слід виривати з нього жодних сторінок).

[38] Зважте на прийнятність доказів, зібраних разом із пристроєм, перед тим, як їх використовувати. Наприклад будь-які пристрої, які є потенційними джерелами доказів, не повинні використовуватися для документування чи запису інших доказів.

[39] NIST SP 800-86, *Керівні настанови щодо інтегрування методів криміналістики до реагування на інциденти,* надають детальну інформацію про створення потенціалу в галузі криміналістики, включаючи розроблення політики та порядку.

[40] У Додатку B міститься запропонований список елементів даних, які потрібно збирати під час повідомлення/звітування про інциденти. Водночас, у документі CERT®/CC *Практичні досягнення Команд реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT)* міститься кілька зразків форм звітності щодо інцидентів. Документ можна знайти за посиланням: .http://www.cert.org/archive/pdf/03tr001.pdf

[41] Транс'європейська науково-освітня мережева асоціація (TERENA) розробила RFC 3067, *Опис інцидентних об'єктів та вимоги до формату обміну TERENA* (http://www.ietf.org/rfc/rfc3067.txt). Документ містить рекомендації щодо того, яку інформацію слід збирати для кожного інциденту. Розширена робоча група щодо управління індидентами (inch) IETF () http://www.cert.org/ietf/inch/inch.htmlстворила документ RFC, в якому детально викладено дані щодо роботи TERENA – RFC 5070, *Опис інцидентних об'єктів та вимоги до формату обміну* (http://www.ietf.org/rfc/rfc5070.txt).

Команда реагування на інциденти має захищати дані про інцидент і обмежувати доступ до них, оскільки досить часто вони містять конфіденційну інформацію, наприклад дані про вразливості, котрими скористалися, нещодавні злами та порушення у сфері безпеки та про користувачів, які, можливо, вчинили невідповідні дії. Наприклад доступ до бази даних інцидентів повинен бути лише в уповноваженого персоналу. Комунікації щодо інцидентів (наприклад, електронні листи) і документи повинні бути зашифровані або захищені в інший спосіб, щоб лише уповноважений персонал міг їх прочитати.

3.2.6 Пріоритезація інцидентів

Пріоритезація процесу управління окремими інцидентами є, мабуть, найважливішим аспектом прийняття рішень у процесі управління інцидентами. Інциденти не можна розглядати за принципом «хто перший прийшов – той перший обслуговується» через обмеженість ресурсів. Замість цього, управління інцидентами слід пріоритезувати на основі відповідних чинників, таких як:

- **Функціональні наслідки інциденту.** Інциденти, ціллю яких є IT-системи, зазвичай впливають на бізнес-функціональність, яку надають ці системи, що призводить до певних негативних наслідків для користувачів цих систем. Фахівці з управління інцидентами повинні зважити, як цей інцидент вплине на поточну функціональність уражених систем. Фахівці з управління інцидентами повинні враховувати не тільки поточні функціональні наслідки інциденту, але й імовірні майбутні функціональні наслідки інциденту, якщо його не буде негайно стримано (локалізовано).

- **Інформаційні наслідки інциденту.** Інциденти можуть вплинути на конфіденційність, цілісність і доступність інформації організації. Наприклад зловмисний агент може передати конфіденційну інформацію. Фахівці з управління інцидентами повинні зважити, як ця передача інформації вплине на загальну місію організації. Інцидент, що призводить до передачі конфіденційної інформації, також може вплинути й на інші організації, якщо будь-які дані стосуються організації-партнера.

- **Можливість відновлення після інциденту.** Масштаб інциденту і тип ресурсів, на які він впливає, визначать кількість часу та ресурсів, які необхідно витратити на відновлення після цього інциденту. У деяких випадках відновитися після інциденту неможливо (наприклад, якщо була порушена конфіденційність таємної, службової чи конфіденційної інформації), і в такому випадку немає сенсу витрачати обмежені ресурси на подовжений цикл управління інцидентами, якщо ці зусилля не будуть спрямовані на забезпечення того, щоб подібного випадку не сталося в майбутньому. В інших випадках для управління інцидентом може знадобитися набагато більше ресурсів ніж ті, що є в організації. Фахівці з управління інцидентами мають враховувати зусилля, необхідні для фактичного відновлення після інциденту, і ретельно продумувати, наскільки ці зусилля будуть варті мети, задля якої вони застосовуються, та як зусилля з відновлення співвідносяться з будь-якими вимогами з управління інцидентами.

Поєднання функціональних наслідків для системи організації та наслідків для інформації організації визначає загальний вплив інциденту на бізнес – наприклад атака на відмову в обслуговуванні, спрямована на публічний вебсервер, може тимчасово зменшити функціональні можливості користувачів, які намагаються отримати доступ до сервера, оскільки несанкціонований доступ на рівні суперкористувача, тобто рута, до публічного вебсервера може призвести до передачі інформації, що дає змогу ідентифікувати особу (PII), а це може мати тривалі наслідки для репутації організації.

Можливість відновлення після інциденту визначає й можливе реагування, якого може вжити команда під час управління інцидентами. Інцидент із високими функціональними наслідками і низькими зусиллями для відновлення є ідеальним «кандидатом» для негайного вжиття дій від команди. Водночас, для деяких інцидентів може не бути легких шляхів відновлення, і, можливо, реагування на них має бути на більш стратегічному рівні – наприклад для інциденту, який призводить до передачі зловмисником гігабайтів конфіденційних даних та їх оприлюднення, немає легкого шляху відновлення, оскільки витік даних вже стався. У цьому випадку команда може передати частину відповідальності за управління інцидентом з передачею даних команді більш стратегічного рівня, яка розробляє стратегію запобігання майбутнім порушенням і створює план роз'яснювальної роботи для оповіщення тих осіб або організацій, чиї дані було передано. Команда повинна пріоритезувати реагування на кожен інцидент на основі оцінювання наслідків для бізнесу, спричинених інцидентом, та попереднього оцінювання зусиль, необхідних для відновлення після інциденту.

Завдяки своїй поінформованості про ситуацію організація може набагато краще кількісно оцінити наслідки власних інцидентів. В таблиці 3-2 надано приклади категорій функціональних наслідків, які організація може використовувати для оцінювання власних інцидентів. Оцінювання інцидентів може допомогти у пріоритезації обмежених ресурсів.

Таблиця 3-2. Категорії функціональних наслідків

Категорія	Визначення
Жодних	Не впливає на здатність організації надавати усі послуги всім користувачам
Низькі	Мінімальний вплив; організація все ще може надавати всі критично важливі послуги всім користувачам, але втратила ефективність
Середні	Організація втратила здатність надавати критично важливі послуги певній групі користувачів системи
Високі	Організація більше не може надавати деякі критично важливі послуги жодній категорії користувачів

У таблиці 3-3 наведено приклади можливих категорій інформаційних наслідків, які описують масштабність порушень конфіденційності, котрі сталися під час інциденту. У цій таблиці, за винятком пункту «Жодних наслідків», категорії не є взаємовиключними, і організація може вибрати більше однієї.

Таблиця 3-3. Категорії інформаційних наслідків

Категорія	Визначення
Жодних	Не сталося жодної передачі, зміни, видалення чи інших варіантів порушення конфіденційності інформації
Витік персональних даних	Було отримано доступ або передано конфіденційну інформацію, що дає змогу ідентифікувати особу (PII) платників податків, працівників, бенефіціарів тощо.
Витік службової інформації	Було отримано доступ або передано несекретну службову інформацію, наприклад інформацію про захищену критичну інфраструктуру (PCII)
Втрата цілісності	Конфіденційну або службову інформацію було змінено або видалено

В таблиці 3-4 представлено приклади категорій зусиль для відновлення, які відображають рівень і тип ресурсів, необхідних для відновлення після інциденту.

Таблиця 3-4. Категорії зусиль для забезпечення можливостей відновлення

Категорія	Визначення
Звичайні	Час, необхідний для відновлення, можна передбачити з наявними ресурсами
Доповнені	Час, необхідний для відновлення, можна передбачити за наявності додаткових ресурсів
Розширені	Час, необхідний для відновлення, неможливо передбачити; необхідні додаткові ресурси та стороння допомога
Можливості відновлення відсутні	Відновлення після інциденту неможливе (наприклад, було передано та опубліковано конфіденційні дані), треба розпочати розслідування

Організації також повинні встановити процес передавання на вищій рівень для тих випадків, коли команда не здійснює реагування на інцидент у визначений час. Це може статися з багатьох причин: наприклад мобільні телефони можуть вийти з ладу або в людей можуть виникнути екстрені ситуації особистого характеру. У процесі передавання на вищій рівень має бути зазначено, скільки часу особа має чекати на відповідь і що робити, якщо відповіді не буде. Як правило, першим кроком є дублювання до початкової контактної особи. Після нетривалого очікування (можливо, 15 хвилин) абонент повинен передати інцидент на вищий рівень, наприклад менеджеру команди реагування на інцидент. Якщо ця особа не реагує протягом певного часу, інцидент слід знову перевести на більш високий рівень керівництва. Цей процес слід повторювати, поки хтось не відповість.

3.2.7 Повідомлення про інцидент

Коли інцидент аналізують та пріоритезують, команда реагування на інцидент повинна повідомити відповідних осіб, щоб усі, кому слід долучитися, виконували передбачені функції. Політика реагування на інциденти має передбачати положення, що стосуються звітування про інциденти – як мінімум, про що необхідно повідомляти, кому саме та в які строки (наприклад, первинне повідомлення, регулярні оновлення статусу). Точні вимоги до звітності/інформування відрізняються залежно від організації, але сторони, яким зазвичай повідомляють про інцидент, включають:

- Начальника інформаційного управління, директора з інформаційних технологій тощо (CIO)
- Керівника служби інформаційної безпеки
- Місцевого фахівця з інформаційної безпеки
- Інші команди реагування на інциденти в організації
- Зовнішні команди реагування на інциденти (за потреби)
- Власника системи
- Відділ кадрів / по роботі з персоналом (для випадків, що сталися з працівниками, наприклад переслідування електронною поштою)
- Служба зі зв’язків із громадськістю (для інцидентів, які можуть викликати розголос)
- Юридичний відділ (для інцидентів із потенційними правовими наслідками)
- US-CERT (в обов’язковому порядку для федеральних органів, установ та систем, котрі функціонують від імені федерального уряду; див. пункт 2.3.4.3)

- Органи правопорядку (за потреби)

Під час управління інцидентами команді може знадобитися повідомити певні сторони щодо оновлення статусу, в деяких випадках навіть організацію загалом. Команда має спланувати і підготувати кілька методів комунікації, включаючи методи з позасмуговим підключенням (наприклад, особисте спілкування, паперові документи), і вибрати відповідні методи для конкретного інциденту. Можливі методи комунікації включають:

- Електронну пошту
- Вебсайт (внутрішній, зовнішній або портал)
- Телефонні дзвінки
- Особисте спілкування (наприклад, щоденні брифінги)
- Привітання голосової скриньки (наприклад, налаштуйте окрему голосову скриньку для оновлень щодо інцидентів та оновлюйте повідомлення привітання, щоб відображати поточний статус інциденту; використовуйте привітання голосової скриньки служби підтримки)
- Паперові документи (наприклад, розклейте оголошення на дошках оголошень і дверях, роздайте оголошення на всіх входах).

3.3 Стримування, ліквідація наслідків та відновлення

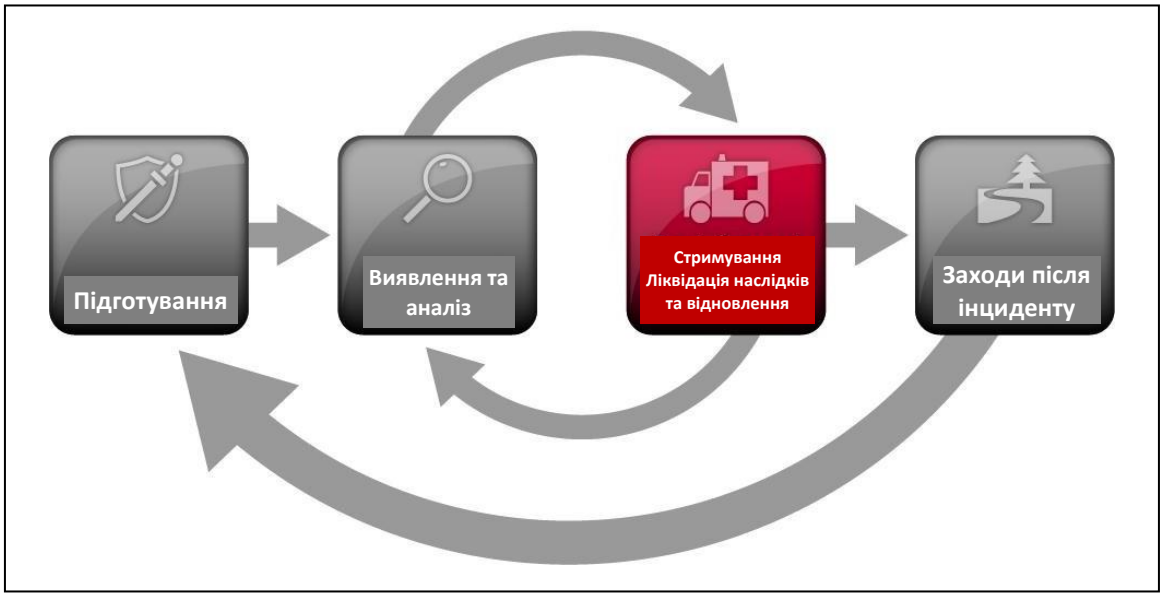

Рисунок 3-3. Життєвий цикл реагування на інциденти (стримування, ліквідація наслідків та відновлення)

3.3.1 Вибір стратегії стримування

Стримування (локалізація) має велике значення до того, як інцидент призведе до перевантаження ресурсів або збільшення збитків. У більшості інцидентів стримування є необхідним, тому важливо це враховувати на початку кожного інциденту. Стримування (локалізація) дає час для розроблення цілеспрямованої стратегії відновлення. Невід'ємною частиною стримування (локалізації) є прийняття рішень (наприклад, вимкнути систему, відключити її від мережі, вимкнути певні функції).

Подібні рішення набагато легше приймати, якщо є заздалегідь визначені стратегії та порядок стримування (локалізації) інциденту. Організаціям необхідно визначити прийнятні ризики під час роботи з інцидентами і розробити відповідні стратегії.

Стратегії стримування (локалізації) відрізняються залежно від типу інциденту. Наприклад стратегія стримування (локалізації) атаки із зараженням шкідливим програмним забезпеченням, надісланим електронною поштою, значно відрізняється від стратегії стримування мережевої DDoS-атаки. Організаціям необхідно створити окремі стратегії стримування (локалізації) для всіх типів серйозних інцидентів із чітко задокументованими критеріями, які сприятимуть прийняттю рішень. Критерії для визначення відповідної стратегії включають:

- Потенційне пошкодження та крадіжку ресурсів
- Необхідність збереження доказів
- Доступність послуг (наприклад, підключення до мережі, надання послуг стороннім особам / третім сторонам)
- Час і ресурси, необхідні для реалізації стратегії
- Ефективність стратегії (наприклад, часткове стримування, повне стримування)
- Тривалість обраного рішення (наприклад, екстрений вихід із положення, який слід припинити використовувати за чотири години, тимчасовий вихід із положення, який слід припинити використовувати за два тижні, постійне рішення).

У певних випадках деякі організації перенаправляють зловмисника в «пісочницю» (форма стримування), щоб вони могли контролювати активність зловмисника, як правило, для збору додаткових доказів. Команді реагування на інциденти слід обговорити цю стратегію зі своїм юридичним відділом, щоб визначити, можливо це, чи ні. Не слід використовувати варіанти моніторингу активності зловмисника, окрім «пісочниці»: якщо організація знає, що систему було зламано, і дозволяє порушенню конфіденційності продовжуватися, вона може нести відповідальність у випадку, якщо зловмисник використає зламану систему для атаки на інші системи. Стратегія відкладеного стримування (локалізації) небезпечна, оскільки зловмисник може посилити несанкціонований доступ або порушити інші системи.

Інша потенційна проблема щодо стримування (локалізації) полягає в тому, що деякі атаки, в разі їх стримування, можуть завдати додаткової шкоди. Наприклад зламаний хост може запустити шкідливий процес, котрий періодично направляє пінг-запит до іншого хоста. Коли фахівець із управління інцидентами намагається стримати (локалізувати) інцидент, від’єднавши зламаний хост від мережі, наступні пінг-запити припинять виконуватися. У результаті збою шкідливий процес може перезаписати або зашифрувати всі дані на жорсткому диску хоста. Фахівцям з управління інцидентами не слід робити висновок, що лише через те, що хост був відключений від мережі, вони попередили подальше пошкодження хоста.

3.3.2 Збір доказів та управління ними

Незважаючи на те, що основною причиною збору доказів під час інциденту є розв’язання інциденту, це також може знадобитися для судового провадження.[42] У таких випадках важливо чітко задокументувати, як саме було збережено всі докази, включаючи системи, котрі зламали.[43] Докази необхідно збирати відповідно до порядку, що відповідає всім чинним нормативно-правовим актам, які були розроблено в результаті попередніх обговорень із працівниками юридичного відділу та відповідними органами правопорядку, щоб будь-які докази могли бути визнані прийнятними для суду.[44]

Крім того, має завжди вестися облік доказів: щоразу, коли докази передаються від особи до особи, у бланках для відстеження руху речових доказів має бути детально описане приймання-передача та мають бути підписи кожної сторони. Для всіх доказів необхідно вести детальний журнал, включаючи таке:

- Ідентифікаційна інформація (наприклад, місцезнаходження, серійний номер, номер моделі, ім'я хоста, MAC-адреси (управління доступом до посередників) та IP-адреси комп'ютера)
- Ім’я, посада та номер телефону кожної особи, яка була залучена до збору чи управління доказами під час розслідування
- Час і дата (включаючи часовий пояс) кожного випадку управління доказами
- Місця, де зберігалися докази.

Збір доказів з обчислювальних ресурсів створює певні виклики. Як правило, бажано отримувати докази від системи, котра представляє інтерес, як тільки є підозра, що міг статися інцидент. Багато інцидентів викликають динамічний ланцюг подій. Початковий «знімок» системи може принести більше користі для визначення проблеми та її джерела, ніж більшість інших дій, котрі можна виконати на цьому етапі. З погляду доказів, набагато краще отримати «знімок» системи як є, ніж робити це після того, як фахівці з управління інцидентами, адміністратори системи та інші ненавмисно змінили стан пристрою під час проведення розслідування. Користувачів та адміністраторів системи слід ознайомити із кроками, які їм необхідно вжити для збереження доказів. Для отримання детальної інформації щодо порядку зберігання доказів, див. NIST SP 800-86, *Керівні настанови щодо інтегрування методів криміналістики до реагування на інциденти*.

3.3.3 Визначення хостів, що атакують

Під час управління інцидентами власникам системи та іншим інколи хочеться або їм необхідно ідентифікувати хост чи хости, що атакують. Незважаючи на те, що ця інформація може бути важливою, фахівцям з управління інцидентами зазвичай потрібно зосередитися на стримуванні (локалізації), ліквідації наслідків та відновленні. Виявлення хоста, що атакує, може бути трудомістким і безперспективним процесом, який може перешкодити команді досягти своєї основної мети – мінімізувати наслідки для бізнесу. Пункти, наведені нижче, описують дії, які найчастіше виконуються для визначення хоста, що атакує:

- **Перевірка IP-адреси хоста, що атакує.** Нові фахівці з управління інцидентами часто зосереджуються на IP-адресі хоста, що атакує. Фахівець із управління інцидентами може спробувати пересвідчитись, чи адреса не була підроблена, перевіривши підключення до неї. Однак цей варіант перевірки просто вказує, що хост за цією адресою відповідає на запити або не відповідає. Якщо відповідь не отримана, тобто хост не відправив відповідь на запит, це не означає, що адреса не справжня – наприклад хост може бути налаштований на ігнорування пінг-запитів і запитів від програм визначення режимів трасування. Крім того, зловмисник міг отримати динамічну адресу, яка вже була перепризначена для когось іншого.

[42] NIST SP 800-86, *Керівні настанови щодо інтегрування методів криміналістики до реагування на інциденти* надають детальну інформацію про створення потенціалу в галузі криміналістики. Цей документ зосереджений на методах криміналістики для ПК, але значну частину матеріалів також можна застосовувати й до інших систем. Ознайомитись із документом можна за посиланням: .http://csrc.nist.gov/publications/PubsSPs.html#800-86

[43] Зазвичай збір доказів та управління ними не проводиться для кожного інциденту, який трапляється – наприклад більшість інцидентів зі зловмисним програмним забезпеченням не потребують збору доказів. У багатьох організаціях для більшості інцидентів не потрібно використовувати методи цифрової криміналістики.

[44] Документ *Пошук та вилучення комп’ютерів і отримання електронних доказів в рамках розслідувань у кримінальних справах*, виданий Відділом комп'ютерної злочинності та злочинності у сфері інтелектуальної власності (CCIPS) Міністерства юстиції США, надає правові роз’яснення щодо збору доказів. Документ можна знайти за посиланням: .http://www.cybercrime.gov/ssmanual/index.html

- **Вивчення хоста, що атакує, за допомогою пошукових систем.** Виконання пошуку в інтернеті з використанням очевидної IP-адреси відправника, з якої здійснювалась атака, може привести до отримання додаткової інформації про атаку, наприклад повідомлення зі списку розсилки щодо подібної атаки.

- **Використання баз даних інцидентів.** Кілька груп збирають та об'єднують дані про інциденти від різних організацій у бази даних інцидентів. Цей обмін інформацією може відбуватися в різних формах, наприклад за допомогою трекерів та «чорних списків», що оновлюються в режимі реального часу. Організація також може перевірити власну базу знань або систему відстеження проблем на предмет схожої активності.

- **Моніторинг можливих каналів комунікацій зловмисників.** Фахівці з управління інцидентами можуть контролювати канали комунікації, котрі найімовірніше використовуватиме хост, що атакує. Наприклад багато ботів використовують IRC як основний засіб комунікації. Крім того, зловмисники можуть активно спілкуватися через деякі IRC-канали, щоб похвалитися своїми компроментаціями та обмінюватися інформацією. Однак фахівцям з управління інцидентами необхідно розглядати будь-яку подібну інформацію, котру вони отримали, лише як потенційну версію чи напрям розслідування, а не як факт.

3.3.4 Ліквідація наслідків та відновлення

Після того, як інцидент було стримано (локалізовано), може знадобитися ліквідація його наслідків, щоб усунути складові інциденту, наприклад видалити зловмисне програмне забезпечення та заблокувати зламані облікові записи користувачів, а також виявити і пом'якшити наслідки всіх вразливостей, котрими скористалися. Під час ліквідації наслідків важливо визначити усі хости в організації, що постраждали, щоб можна було усунути відповідні вразливості. У деяких випадках ліквідація наслідків або не потрібна, або виконується під час відновлення.

Під час відновлення адміністратори відновлюють нормальну роботу систем, підтверджують, що системи функціонують нормально, і (якщо це потрібно) усувають вразливості, щоб запобігти подібним інцидентам. Відновлення може включати такі дії, як відновлення систем із чистих резервних копій, відновлення системи з нуля, заміну зламаних файлів «чистими» версіями, встановлення патчів, зміну паролів та посилення периметру безпеки мережі (наприклад, набори правил брандмауера, списки управління доступом до граничного маршрутизатора). Частиною процесу відновлення часто є вищі рівні моніторингу мережі або вищі рівні журналювання в системі. Після однієї успішної атаки той самий ресурс часто атакують знову, або аналогічно атакують інші ресурси в організації.

Ліквідацію наслідків та відновлення слід проводити поетапно, щоб у пріоритеті були кроки з відновлення. У разі масштабних інцидентів відновлення може зайняти місяці. Метою ранніх етапів має бути підвищення загального рівня безпеки за допомогою порівняно швидких (від кількох днів до тижнів), але значущих змін для запобігання майбутнім інцидентам. Подальші етапи повинні бути зосереджені на довгострокових змінах (наприклад, змінах інфраструктури) та поточній роботі для забезпечення максимального рівня безпеки підприємства.

У зв'язку з тим, що заходи з ліквідації наслідків та відновлення зазвичай індивідуально підібрані для кожної ОС або застосунку, детальні рекомендації та поради щодо них не входять до тематики цього документа.

3.4 Заходи після інциденту

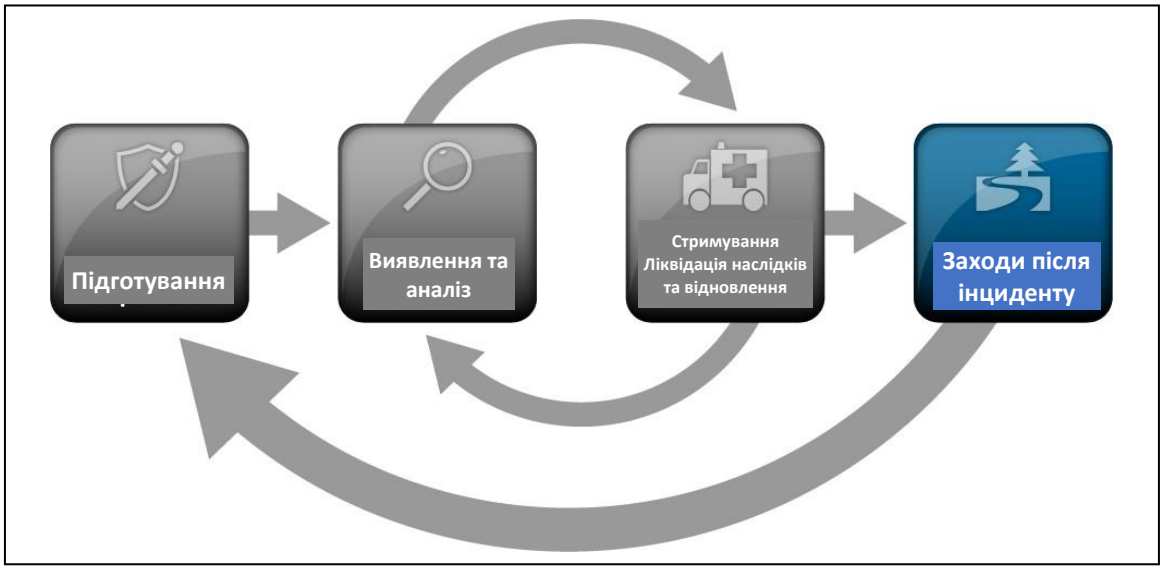

Рисунок 3-4. Життєвий цикл реагування на інциденти (заходи після інциденту)

3.4.1 Засвоєний досвід

Навчання та вдосконалення – це одна з найважливіших частин реагування на інциденти, про яку, при цьому, також найчастіше забувають. Кожна команда реагування на інциденти повинна розвиватися, щоб її кваліфікація відображала нові загрози, вдосконалені технології та засвоєний досвід. Проведення зустрічі щодо «засвоєного досвіду» з усіма залученими сторонами після серйозного інциденту та, за бажанням, періодично після менш масштабних інцидентів, якщо ресурси це дозволяють, може бути надзвичайно корисним для вдосконалення засобів безпеки та й, власне, процесу управління інцидентами. На одній подібній зустрічі можна розглянути кілька інцидентів. Ця зустріч дає можливість розставити всі крапки над «і» щодо інциденту, переглянувши те, що сталося, що було зроблено для того, щоб втрутитись у ситуацію, та наскільки добре спрацювало це втручання. Зустріч має відбутися протягом кількох днів після завершення інциденту. Запитання, на які потрібно дати відповіді під час зустрічі, включають:

- Що саме сталося, в який день та о котрій годині?
- Наскільки добре впоралися працівники та керівництво під час боротьби з інцидентом? Чи всі дотримувалися задокументованого порядку? Він відповідав ситуації?
- Яку інформацію необхідно було отримати раніше?
- Чи було вжито якихось кроків або заходів, котрі, можливо, загальмували процес відновлення?
- Що персонал та керівництво робитимуть інакше, коли наступного разу станеться подібний інцидент?
- Як можна було покращити обмін інформацією з іншими організаціями?
- Які коригувальні заходи можуть запобігти подібним інцидентам у майбутньому?
- На які прекурсори чи індикатори слід звертати увагу в майбутньому, щоб виявити подібні випадки?

- Які додаткові інструменти чи ресурси необхідні для виявлення, аналізу та пом'якшення наслідків майбутніх інцидентів?

Невеликі інциденти не потребують проведення глибокого аналізу після них, за винятком тих інцидентів, що здійснюються за допомогою нових методів атак, котрі викликають значне занепокоєння та інтерес. Після того, як відбуваються серйозні атаки, зазвичай варто проводити зустрічі для обговорення та аналізу причин, які об'єднують команди й організації, щоб забезпечити механізм обміну інформацією. Під час проведення таких зустрічей головне завдання полягає у залученні потрібних людей. Важливо не тільки запросити тих людей, які були причетні до інциденту, котрий аналізується, а й продумати, кого слід запросити з метою сприяння подальшій співпраці.

Успіх таких зустрічей також залежить від порядку денного. Опитування учасників щодо очікувань та потреб (включаючи запропоновані для висвітлення теми) перед зустріччю підвищує ймовірність того, що потреби учасників можна буде задовольнити. Крім того, встановлення регламенту до або на початку зустрічі може звести до мінімуму плутанину та розбрат. Якщо у вас буде один або кілька модераторів, які володіють навичками фасилітації групи, це може забезпечити високу віддачу. Насамкінець, також важливо задокументувати основні моменти щодо досягнутих домовленостей та запланованих заходів і повідомити про них сторонам, які не змогли бути присутніми на зустрічі.

Зустрічі щодо засвоєного досвіду також дають інші переваги. Звіти з цих зустрічей – це гарні навчальні матеріали для нових учасників команди, за допомогою яких їм можна показати, як більш досвідчені учасники команди реагують на інциденти. Ще однією важливою частиною процесу опрацювання засвоєного досвіду є оновлення політики та порядку реагування на інциденти. Аналіз причин усього, що відбулося, і того, як управляли інцидентом, часто виявляє, що десь було пропущено крок або допущено неточність у затвердженому порядку, що дає поштовх для змін. Через зміну характеру інформаційних технологій та зміни в персоналі, команда реагування на інциденти повинна переглядати всю документацію, пов'язану з інцидентами, та порядок управління інцидентами через визначені проміжки часу.

Іншим важливим заходом після інциденту є створення звіту про подальші дії для кожного інциденту, який може бути дуже цінним для використання в майбутньому. У звіті міститься довідкова інформація, яку можна буде використати для допомоги під час управління подібними інцидентами. З правових міркувань важливо створити формальну хронологію подій (включаючи позначену часовою міткою інформацію, таку як дані журналів систем), так само як і провести попереднє оцінювання суми збитків, завданих інцидентом, у грошовому виразі. Це оцінювання в подальшому може стати основою для провадження, що ведуть такі структури, як Генеральна прокуратура США. Звіт про подальші дії слід зберігати протягом періоду, визначеного політикою щодо зберігання записів.[45]

3.4.2 Використання даних, зібраних про інцидент

Завдяки опрацюванню засвоєного досвіду має виникнути набір об'єктивних та суб'єктивних даних щодо кожного інциденту. З часом зібрані дані про інциденти стануть корисними в кількох аспектах. Дані, зокрема загальна кількість годин роботи і витрати на ліквідацію наслідків, можуть бути використані для обґрунтування додаткового фінансування команди реагування на інцидент. Вивчення характеристик інцидентів може вказати на слабкості та загрози безпеки у системі, а також на зміни тенденцій у сфері інцидентів. Ці дані можна використати в процесі оцінювання ризику, що в кінцевому підсумку приведе до вибору та запровадження додаткових інструментів контролю. Ще один варіант використання даних із користю – це вимірювання успіху команди реагування на інциденти.

Якщо дані про інцидент належно збирають і зберігають, вони повинні забезпечувати кілька показників вимірювання успіху (або принаймні вжитих заходів) команди реагування на інцидент.

Дані про інциденти також можна збирати, щоб визначити, чи спричиняє зміна потенціалу реагування на інциденти відповідні зміни в роботі команди (наприклад, підвищення ефективності, зниження витрат). Більше того, організаціям, котрі зобов'язані повідомляти чи звітувати про інциденти, необхідно буде збирати необхідні дані, щоб відповідати поставленим вимогам. Додаткову інформацію щодо обміну даними про інциденти з іншими організаціями див. у Розділі 4.

Організації мають зосередитися на зборі даних, які можна використати для дій, а не на зборі даних просто тому, що ці дані є. Наприклад підрахунок кількості сканувань портів із прекурсорами, котрі відбуваються щотижня, і створення діаграми наприкінці року, яка показує збільшення кількості сканувань портів на вісім відсотків, не дуже корисно і може бути трудомістким процесом. Абсолютні цифри не інформативні – важливо зрозуміти, яку вони становлять загрозу для бізнес-процесів організації. Організації мають вирішити, які дані про інциденти збирати на основі вимог до звітності та очікуваної ефективності інвестицій (наприклад, виявлення нової загрози та пом'якшення наслідків вразливостей, пов'язаних із нею, перш ніж ними скористаються). Можливі показники для даних, пов'язаних із інцидентами, включають:

- **Кількість інцидентів, котрими управляли.**[46] Управління більшою кількістю інцидентів не обов'язково краще – наприклад кількість інцидентів, котрі були в обробці та управлінні, може зменшитися в результаті кращого контролю безпеки мережі та хоста, а не через недбалість команди реагування на інциденти. Кількість інцидентів, котрі були в обробці та управлінні, найкраще сприймати як міру відносного обсягу роботи, яку мала виконати команда реагування на інциденти, а не як показник якості роботи команди, якщо вона не розглядається в контексті інших заходів, які разом дають показник якості роботи. Набагато ефективніше проводити окремі підрахунки щодо інцидентів для кожної категорії інцидентів. Для надання додаткової інформації також можна використовувати підкатегорії. Наприклад усе більша кількість інцидентів, здійснених інсайдерами (внутрішніми зловмисниками), може призвести до посилення положень політики щодо проведення перевірки анкетних даних персоналу та неправомірного використання обчислювальних ресурсів, а також посилення контролю рівня безпеки у внутрішніх мережах (наприклад, встановлення програмного забезпечення для виявлення вторгнень у більшій кількості внутрішніх мереж і хостів).

---

45 Порядок ведення загальної документації (GRS) 24, *Операційна та управлінська документація щодо інформаційних технологій*, зазначає, що «записи про управління інцидентами, пов'язаними з комп'ютерною безпекою, звітність і документи щодо подальшої діяльності» слід знищити «через 3 роки після того, як буде завершено всі необхідні подальші заходи». GRS 24 можна знайти на сайті Національного управління архівів та документації за посиланням: .http://www.archives.gov/records-mgmt/grs/grs24.html

46 Такі показники, як кількість інцидентів, котрими управляли, як правило, не мають значення при порівнянні кількох організацій, оскільки кожна організація, ймовірно, по-різному визначила основні терміни. Зокрема, більшість організацій визначають «інцидент» з погляду власної політики та практики, і те, що одна організація вважає одним інцидентом, інші можуть вважати кількома інцидентами. Більш конкретні показники, такі як кількість сканувань портів, також не мають значення в рамках порівняння організацій. Наприклад малоймовірно, що інші системи безпеки, такі як детектори (датчики) виявлення вторгнень у мережу, будуть використовувати такі самі критерії для маркування активності, як для сканування порту.

- **Час на один інцидент.** Для кожного інциденту час можна виміряти кількома способами:
  - Загальний об’єм трудовитрат на роботу над інцидентом
  - Час, що минув від моменту початку інциденту до моменту його виявлення, до первинного оцінення наслідків та до кожного етапу процесу управління інцидентом (наприклад, стримування/локалізації, відновлення)
  - Скільки часу знадобилося команді реагування на інцидент, щоб відреагувати на первинне повідомлення про інцидент
  - Скільки часу знадобилося, щоб повідомити про інцидент керівництву та, якщо необхідно, відповідним зовнішнім організаціям (наприклад, US-CERT).
- **Об'єктивне оцінювання кожного інциденту.** Процес реагування на інцидент, який було вирішено, можна проаналізувати, щоб визначити, наскільки ефективним він був. Нижче наведено приклади проведення об’єктивного оцінювання інциденту:
  - Перегляд журналів, форм, звітів та іншої документації про інциденти на предмет дотримання встановлених політик і порядку реагування на інциденти
  - Визначення того, які прекурсори та індикатори інциденту було задокументовано, щоб визначити, наскільки ефективно інцидент було зафіксовано в журналах та ідентифіковано
  - Визначення того, чи викликав інцидент пошкодження до того, як його було виявлено
  - Визначення того, чи була виявлена фактична причина інциденту, а також визначення вектору атаки, вразливостей, котрими скористалися, та характеристик систем, мереж і програм, що стали ціллю або зазнали шкоди.
  - Визначення того, чи є інцидент повторенням попереднього інциденту
  - Розрахунок приблизних збитків у грошовому вираженні (наприклад, інформація та критичні бізнес-процеси, на яких негативно позначився інцидент)
  - Вимірювання різниці між первинним і остаточним оціненням наслідків (див. пункт 3.2.6)
  - Визначення того, які заходи могли б запобігти інциденту, якщо це було можливо.
- **Суб'єктивне оцінювання кожного інциденту.** Учасників команди реагування на інциденти можуть попросити оцінити свою власну роботу, а також роботу інших учасників команди та всієї команди загалом. Ще одним цінним джерелом інформації є власник ресурсу, на який було здійснено атаку, щоб визначити, чи вважає власник інциденту, що інцидентом ефективно управляли, і чи результат був задовільним.

Окрім використання цих показників для вимірювання успіху команди, організації можуть вирішити, що періодичні перевірки своїх програм реагування на інциденти можуть бути корисним. Аудити безпеки можуть виявити проблеми та недоліки, які потім можна буде виправити. Як мінімум, аудит безпеки для реагування на інцидент має оцінити, чи відповідають зазначені далі аспекти чинному законодавству, політикам і загальноприйнятим практикам:

- Політика, плани та порядок реагування на інциденти
- Інструменти і ресурси

- Модель і структура команди
- Тренінги та навчання осіб, які займаються управлінням інцидентами
- Документація та звіти про інциденти
- Показники вимірювання успіху, про які йшлося раніше в цьому пункті.

3.4.3 Зберігання доказів

Організаціям слід впровадити політику щодо того, як довго слід зберігати докази щодо інциденту. Більшість організацій приймають рішення зберігати всі докази протягом місяців або років після закінчення інциденту. Під час створення політики слід враховувати зазначені чинники:

- **Притягнення до відповідальності** Якщо зловмисник може бути притягнутий до відповідальності, треба буде зберігати докази до завершення всіх юридичних дій. У деяких випадках це може зайняти кілька років. Крім того, докази, які в цей момент здаються незначними, в майбутньому можуть стати більш важливими. Наприклад якщо зловмисник може скористатися знаннями, зібраними під час однієї атаки, щоб пізніше здійснити більш серйозну атаку, то докази з першої атаки можуть бути визначальними для пояснення того, як було здійснено другу атаку.
- **Зберігання даних.** У більшості організацій є політика зберігання даних, яка визначає, як довго можуть зберігатися певні типи даних. Наприклад організація може визначити, що повідомлення електронної пошти мають зберігатися лише 180 днів. Якщо образ диска містить тисячі листів електронної пошти, організація може не захотіти, щоб образ зберігався більше 180 днів, за винятком випадків, коли це дійсно необхідно. Як зазначалося в пункті 3.4.2, Загальний графік записів (GRS) 24 визначає, що записи про інциденти слід зберігати не менше трьох років.
- **Витрати.** Оригінальне апаратне забезпечення (наприклад, жорсткі диски, зламані системи), котре зберігається як доказ, а також жорсткі диски та знімні носії, що використовуються для зберігання образів дисків, як правило, коштують недорого, якщо зважати на ціну зберігання одиниці обладнання. Утім, якщо організація зберігає багато таких одиниць обладнання роками, витрати можуть бути значними. Організації також слід зберігати цілком працездатні комп'ютери, які можуть використовувати обладнання та носії, що зберігаються.

3.5 Контрольний список з управління інцидентами

Контрольний список, наведений у таблиці 3-5, містить основні кроки, котрі необхідно виконати під час управління інцидентом. Майте на увазі, що фактичні кроки можуть відрізнятися залежно від типу інциденту і характеру окремих інцидентів. Наприклад якщо фахівець з управління інцидентами точно знає, що сталося на основі аналізу індикаторів (Крок 1.1), може не знадобитися виконувати Кроки 1.2 або 1.3, щоб продовжувати вивчати активність. Контрольний список містить вказівки для фахівців з управління інцидентами щодо основних кроків, які слід виконати. Він не диктує точну послідовність кроків, яких слід завжди дотримуватися.

Таблиця 3-5. Контрольний список з управління інцидентами

	Дія	Завершено
	Виявлення та аналіз	
1.	Визначте, чи інцидент насправді стався	
1,1:	Проаналізуйте прекурсори та індикатори	
1.2	Шукайте інформацію, що корелюється	
1.3	Проведіть дослідження (наприклад, пошукові системи, база знань)	
1.4	Як тільки фахівець з управління інцидентами вважає, що інцидент стався, почніть документувати розслідування та збирати докази	
2.	Пріоритезуйте управління інцидентом на основі відповідних чинників (функціональні наслідки, інформаційні наслідки інциденту, зусилля, які необхідно докласти для відновлення після інциденту)	
3.	Повідомте/прозвітуйте про інцидент відповідному внутрішньорганізаційному персоналу та зовнішнім організаціям	
	Стримування, ліквідація наслідків та відновлення	
4.	Отримайте, зберігайте, убезпечьте і задокументуйте докази	
5.	Стримайте (локалізуйте) інцидент	
6.	Ліквідуйте інцидент	
6.1	Виявіть і пом’якшіть наслідки всіх вразливостей, котрими скористалися	
6.2	Видаліть зловмисне програмне забезпечення, невідповідні матеріали та інші складові	
6.3	Якщо буде виявлено більше хостів, що постраждали (наприклад, нові зараження зловмисним ПЗ), повторіть кроки з виявлення та аналізу (1.1, 1.2), щоб ідентифікувати усі інші хости, що постраждали, а потім стримуйте (5) і ліквідуйте (6) інцидент для них	
7.	Відновіться після інциденту	
7.1	Поверніть системи, що постраждали, до стану готовності до роботи	
7.2	Підтвердіть, що системи, що постраждали, функціонують нормально	
7.3	Якщо потрібно, запровадьте додатковий моніторинг для пошуку майбутньої схожої активності	
	Заходи після інциденту	
8.	Створіть звіт про подальші дії	
9.	Проведіть зустріч щодо засвоєного досвіду (обов'язковий крок для серйозних інцидентів, в іншому випадку необов'язковий)	

3.6 Рекомендації

Основні рекомендації щодо управління інцидентами, представлені в цьому пункті, наведено нижче.

- **Отримайте інструменти і ресурси, які можуть бути корисними під час управління інцидентами.** Команда зможе ефективніше управляти інцидентами, якщо в неї вже є різні інструменти і ресурси. Наприклад: списки контактів, програмне забезпечення для шифрування, діаграми мережі, пристрої резервного копіювання, цифрове криміналістичне програмне забезпечення та переліки портів.

- **Запобігайте виникненню інцидентів шляхом забезпечення достатнього рівня безпеки мереж, систем і застосунків.** Запобігання інцидентам, їх попередження корисні для організації, а також зменшують навантаження на команду реагування на інциденти. Проведення періодичного оцінювання ризиків і зменшення виявлених ризиків до прийнятного рівня є ефективними інструментами для зменшення кількості інцидентів. Обізнаність користувачів, IT-персоналу та керівництва щодо політики та порядку у сфері безпеки також має величезне значення.

- **Ідентифікуйте прекурсори та індикатори за допомогою сповіщень, згенерованих кількома типами програмного забезпечення, що сприяє безпеці.** Системи виявлення та запобігання атакам/вторгненням, антивірусне програмне забезпечення та програмне забезпечення для перевірки файлів на предмет порушень цілісності дуже цінні для виявлення ознак інцидентів. Кожен тип програмного забезпечення може виявляти інциденти, котрі інші типи програмного забезпечення не можуть, тому наполегливо рекомендується використовувати кілька типів програмного забезпечення, яке сприяє комп'ютерній безпеці. Моніторингові сервіси від третіх сторін також можуть бути корисними.

- **Створіть механізми, за допомогою яких сторонні особи / треті сторони зможуть повідомляти про інциденти.** Сторонні особи / треті сторони можуть захотіти повідомити організацію про інциденти, наприклад вони можуть вважати, що один із користувачів організації атакує їх. Організаціям необхідно оприлюднювати номер телефону та адресу електронної пошти, щоб сторонні особи / треті сторони могли використати їх для інформування про такі інциденти.

- **Вимагайте базового рівня журналювання та аудиту безпеки для всіх систем, а також більш високого базового рівня для всіх критично важливих систем.** Журнали операційних систем, служб і застосунків також мають неабияке значення під час аналізу інцидентів, особливо якщо ввімкнено аудит безпеки. У журналах можна побачити додаткову інформацію, зокрема, до яких облікових записів було отримано доступ і які саме дії були виконано.

- **Профілюйте мережі та системи.** *Профілювання* аналізує та вимірює динамічні показники очікуваного рівня активності, щоб можна було легше ідентифікувати зміни у закономірностях. Якщо процес профілювання автоматизовано, відхилення від очікуваних рівнів активності можна швидко виявити і повідомити адміністраторам, що приведе до швидшого виявлення інцидентів та функціональних проблем.

- **Зрозумійте, як виглядає нормальна робота для мереж, систем та застосунків** Учасники команди, які розуміють, як виглядає нормальна робота, мають легше розпізнавати аномалії у роботі. Найкращий спосіб здобути такі знання – це переглянути записи журналів та сповіщення щодо безпеки; фахівцям з управління інцидентами необхідно ознайомитися з типовими даними і тоді вони зможуть вивчати нетипові записи, щоб здобути більше знань.

- **Створіть політику зберігання журналів.** Інформація про інцидент може бути записана в кількох місцях. Створення та впровадження політики зберігання журналів, яка визначає, як довго мають зберігатися дані журналу, може виявитися надзвичайно корисним для аналізу, оскільки старі записи журналу можуть відображати розвідувальну активність або попередні випадки схожих атак.

- **Співставляйте події між собою.** Докази інциденту можуть бути записані в кількох журналах. Кореляція подій між багатьма джерелами може виявитись неоціненною під час збору всієї наявної інформації щодо інциденту та перевірки того, чи інцидент насправді відбувся.

- **Стежте за тим, щоб усі годинники хоста були синхронізовані.** Кореляція подій стане складнішою, якщо пристрої, котрі повідомляють про події, мають неузгоджені налаштування годинників. З погляду доказової бази, розбіжності у даних годинників також можуть викликати проблеми.

- **Підтримуйте в актуалізованому стані та використовуйте інформаційну базу знань.** Під час аналізу інцидентів фахівцям з управління інцидентами необхідно швидко отримувати довідкову інформацію; наявність централізованої бази знань – це гарантія несуперечливого джерела інформації, яке можна підтримувати в актуалізованому стані. База знань повинна включати загальну інформацію, таку як дані про прекурсори та індикатори попередніх інцидентів.

- **Почніть документувати всю інформацію, як тільки у команди виникла підозра, що стався інцидент** Кожен крок, зроблений з моменту виявлення інциденту до моменту його остаточного вирішення, має бути задокументований і позначений часовою міткою. Інформація такого характеру також може бути використана як доказ у суді, якщо є судове провадження. Документування всіх виконаних кроків також може привести до ефективнішого та систематичнішого вирішення проблеми із нижчим ризиком припуститися помилок.

- **Захистіть дані про інциденти.** Досить часто вони містять конфіденційну інформацію, наприклад дані про вразливості, нещодавні злами та порушення у сфері безпеки та про користувачів, які, можливо, вчинили невідповідні дії. Команді слід забезпечити належне обмеження доступу до даних про інциденти, як логічно, так і фізично.

- **Пріоритезуйте управління інцидентом на основі відповідних чинників.** Інциденти не можна розглядати за принципом «хто перший прийшов – той перший обслуговується» через обмеженість ресурсів. Натомість, організаціям необхідно створити письмові рекомендації щодо того, як швидко команда повинна реагувати на інцидент і які дії слід виконати, зважаючи на відповідні чинники, такі як функціональні та інформаційні наслідки інциденту, а також імовірність відновлення після інциденту. Це заощаджує час для фахівців з управління інцидентами та надає обґрунтування для дій керівництва та власників системи. Організації також повинні встановити процес передавання на вищій рівень для тих випадків, коли команда не здійснює реагування на інцидент у визначений час.

- **Включіть положення, що стосуються звітування про інциденти, до політики реагування на інциденти організації.** Організації мають вказати, про які інциденти необхідно повідомляти / звітувати, коли це треба робити і кого слід інформувати. Сторони, котрих найчастіше інформують чи яким найчастіше звітують, включають CIO, керівника служби інформаційної безпеки, місцевого фахівця з інформаційної безпеки, інші команди реагування на інциденти в організації та власників систем.

- **Створіть стратегії та порядок стримування (локалізації) інцидентів.** Важливо швидко та ефективно стримувати (локалізувати) інциденти, щоб обмежити їхні наслідки для бізнесу. Організаціям необхідно визначити прийнятні ризики під час стримування (локалізації) інцидентів і розробити відповідні стратегії та порядок. Стратегії стримування (локалізації) повинні відрізнятися залежно від типу інциденту.

- **Дотримуйтеся встановленого порядку для збору доказів та управління ними.** Команді слід чітко задокументувати, як було збережено всі докази. Завжди має вестися облік доказів. Команді необхідно зустрітися з працівниками юридичного відділу та органами правопорядку, щоб обговорити питання управління доказами, а потім розробити порядок на основі цих обговорень.

- **Збережіть мінливі дані із систем як докази.** Це включає поточний статус мережевих підключень, процесів, сеансів входу, відкритих файлів, конфігурацій мережевого інтерфейсу та вмісту пам'яті. Виконання ретельно підібраних команд із надійних носіїв може допомогти зібрати необхідну інформацію, не пошкоджуючи докази із системи.

- **Зробіть «знімки» системи за допомогою повних криміналістичних образів дисків, а не просто резервних копій файлової системи.** Образи дисків слід записувати на очищені носії із захистом від запису або одноразовим записом. Для цілей розслідування та для доказової бази цей процес кращий ніж резервне копіювання файлової системи. Створення образу також цінне тим, що аналізувати образи набагато безпечніше, ніж аналізувати оригінальну систему, оскільки процес аналізу може ненавмисно змінити оригінал.

- **Проводьте наради/зустрічі щодо засвоєного досвіду після серйозних інцидентів.** Зустрічі щодо засвоєного досвіду надзвичайно корисні для вдосконалення засобів безпеки та й, власне, процесу управління інцидентами.

4. Координація та обмін інформацією

Зважаючи на природу сучасних загроз і атак спільна робота організацій під час реагування на інциденти стає більш важливою, ніж будь-коли раніше. Організаціям слід забезпечити ефективну координацію частини своєї діяльності з реагування на інциденти із відповідними партнерами. Найважливішим аспектом координації реагування на інциденти є обмін інформацією, коли різні організації обмінюються одна з одною інформацією про загрози, атаки та вразливості, щоб знання кожної організації також приносили користь іншій. Обмін інформацією про інциденти часто є взаємовигідним, оскільки одні й ті самі загрози й атаки часто впливають на кілька організацій одночасно.

Як вже було зазначено в Розділі 2, координація та обмін інформацією з партнерськими організаціями може посилити здатність організації ефективно реагувати на IT-інциденти. Наприклад якщо організація виявляє певну активність чи тенденції роботи у своїй мережі, які видаються підозрілими, і надсилає інформацію про подію кільком надійним партнерам, хтось інший у цій мережі можливо вже бачив подібну підозрілу активність та зможе надати додаткові деталі про неї, включаючи сигнатури, інші індикатори, які потрібно шукати, або запропонує дії з її усунення. Співпраця з надійним партнером може допомогти організації реагувати на інцидент швидше та ефективніше, ніж у випадку організації, що працює ізольовано.

Зазначене підвищення ефективності стандартних методів реагування на інциденти є не єдиним стимулом для міжорганізаційної координації та обміну інформацією. Іншим стимулом для обміну інформацією є здатність реагувати на інциденти за допомогою методів, котрі можуть бути недоступні організації, що працює самотужки, особливо якщо ця організація мала або середня. Наприклад у невеликій організації, яка знаходить особливо складний варіант зловмисного програмного забезпечення у своїй мережі, може не бути внутрішніх ресурсів для повного аналізу шкідливого програмного забезпечення та визначення його наслідків для системи. У цьому випадку організація може скористатися надійною мережею обміну інформацією, щоб ефективно передати аналіз цього зловмисного програмного забезпечення ресурсам сторонніх компаній, які мають відповідні технічні можливості для виконання аналізу шкідливого програмного забезпечення.

У цьому розділі видання мова піде про координацію та обмін інформацією. У пункті 4.1 представлено загальний огляд координації реагування на інциденти, цей пункт також зосереджений на необхідності міжорганізаційної координації для доповнення процесів реагування на інциденти організації. У пункті 4.2 розглянуто методи обміну інформацією між організаціями, а в пункті 4.3 розглянуто, як встановити обмеження щодо того, яка саме інформація підлягає обміну з іншими організаціями, а яка – ні.

4.1 Координація

Як зазначалося в пункті 2.3.4, організації може знадобитися взаємодіяти з кількома типами зовнішніх організацій під час проведення заходів з реагування на інциденти. Серед таких організацій є інші команди реагування на інциденти, органи правопорядку, інтернет-провайдери, а також виборці та клієнти/споживачі. Команді реагування на інциденти організації необхідно спланувати свою координацію щодо інцидентів з цими сторонами до того, як інциденти виникнуть, щоб переконатися, що всі сторони знають, які функції вони мають виконувати, і що встановлено ефективні способи комунікації між сторонами. На рис. 4-1 представлено приклад того, як організація може здійснювати координацію на кожному етапі життєвого циклу реагування на інцидент, підкреслюючи, що координація дуже важлива протягом усього життєвого циклу.

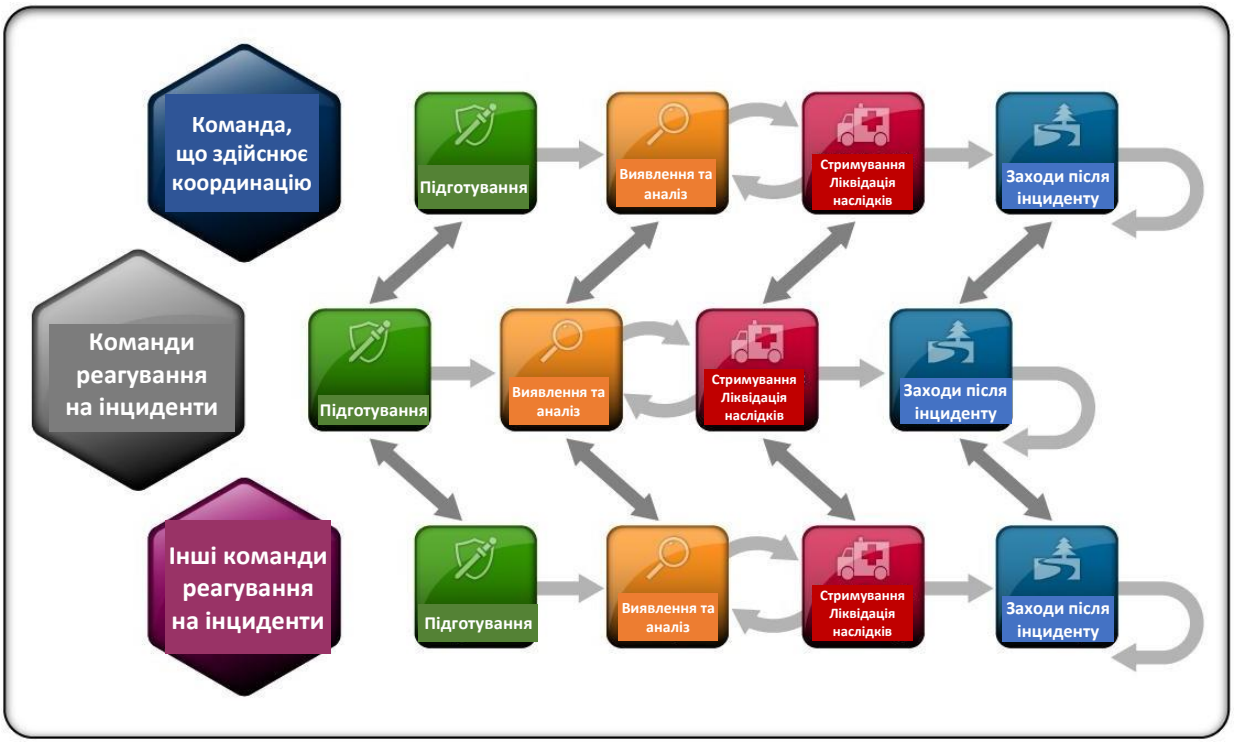

Рисунок 4-1. Координація реагування на інциденти

4.1.1 Співпраця в рамках координації дій

В межах організації команда реагування на інциденти може брати участь у різних типах координаційних заходів, залежно від типу організації, з якою здійснюється координація. Зокрема, учасники команди, відповідальні за технічні деталі реагування на інциденти, можуть координувати свої дії з колегами з партнерських організацій, які займаються оперативною діяльністю, щоб поділитися стратегіями пом'якшення наслідків атаки, яка охоплює кілька організацій. Водночас, під час того самого інциденту менеджер команди реагування на інцидент може координувати роботу з ISAC, щоб виконати необхідні вимоги щодо звітування і звернутися за порадою та додатковими ресурсами для успішного реагування на інцидент. В таблиці 4-1 представлено декілька прикладів співпраці в рамках координації дій, які можуть існувати, якщо організація співпрацює із зовнішніми організаціями.

Таблиця 4-1. Співпраця в рамках координації дій

Категорія	Визначення	Якою інформацією обмінюються
Команда-до-команди	Взаємини на рівні команда-до-команди існують, коли технічні команди, служби та спеціалісти, що забезпечують реагування на інциденти в різних організаціях, співпрацюють зі своїми колегами протягом будь-якого етапу життєвого циклу управління інцидентами. Організації, які беруть участь у цьому типі взаємин, зазвичай є колегами, посади яких знаходяться на одному рівні, без будь-яких повноважень один до одного; вони просто приймають рішення ділитися інформацією, об'єднувати ресурси та повторно використовувати знання для вирішення проблем, спільних для обох команд.	Інформація, котрою найчастіше діляться у взаєминах типу команда-до-команди, є тактичною і технічною (наприклад, технічні індикатори компрометації / несанкціонованого доступу, пропозиції щодо дій з усунення проблеми), але може також включати інші типи інформації (плани, порядок, засвоєний досвід), якщо такий обмін інформацією проводиться як частина етапу Підготування.
Команда-до-команди, що здійснює координацію	Взаємини на рівні команда-до-команди, що здійснює координацію, існують між командою реагування на інциденти організації та окремою організацією, яка діє як центральний пункт для скоординованого реагування на інциденти та управління, як-от US-CERT або ISAC. Цей тип взаємин може включати певну міру обов'язкової звітності від організацій-учасниць координаційному органу, а також очікування, що команда, яка здійснює координацію, поширюватиме своєчасну та корисну інформацію серед організацій-учасниць.	Команди та координаційні підрозділи часто обмінюються тактичною, технічною інформацією, а також інформацією про загрози, вразливості та ризики для спільноти, яку обслуговує команда, що здійснює координацію. Команді, що здійснює координацію, також може знадобитися конкретна інформація про наслідки інцидентів, щоб допомогти прийняти рішення про те, на що саме слід зосередити свої ресурси та увагу.
Команда, що здійснює координацію-до-команди, що здійснює координацію	Взаємини між кількома командами, що здійснюють координацію, такими як US-CERT та ISAC, існують для обміну інформацією, що стосується наскрізних інцидентів, котрі можуть вплинути на декілька спільнот чи громад. Команди, що здійснюють координацію, діють від імені відповідних організацій-учасниць спільноти, щоб обмінюватись інформацією про природу і масштаби наскрізних інцидентів та стратегії пом'якшення наслідків, які можна неодноразово використовувати, щоб допомагати у реагуванні в рамках взаємодії між спільнотами.	Тип інформації, якою обмінюються команди, що здійснюють координацію, зі своїми колегами, часто включає періодичні підсумки під час операцій, у яких підтримується «стабільний стан», що перемежовуються обміном тактичними, технічними деталями, планами реагування та інформацією про наслідки або оцінюванням ризиків під час скоординованої діяльності з реагування на інциденти.

Організаціям може видатися, що побудувати взаємини, необхідні для координації, складно. Для того, щоб почати розбудовувати таку спільноту, непогано було б спочатку розглянути галузь, до якої належить організація, і географічний регіон, де працює організація. Команда реагування на інциденти організації може спробувати налагодити відносини з іншими командами (на рівні команда-до-команди) у власній галузі та регіоні або приєднатися до наявних органів у галузі, де вже є сприяння обміну інформацією. Іншим міркуванням для побудови взаємин є те, що одні типи відносин є обов'язковим, а інші – добровільними; наприклад відносини команда-до-команди, що здійснює координацію, часто є обов'язковими, тоді як відносини на рівні команда-до-команди, як правило, є добровільними. Організації розбудовують такі добровільні відносини, оскільки вони відповідають взаємним інтересам організацій.

Обов’язкові відносини, зазвичай, визначені регуляторними органами у галузі або іншими відомствами.

4.1.2 Договори щодо обміну даними та вимоги до звітності

До того, як організації, котрі намагаються ділитися інформацією із зовнішніми організаціями, почнуть будь-яку координацію, їм слід проконсультуватися зі своїм юридичним відділом. Можливо, до початку обговорень необхідно укласти договори, контракти чи інші угоди. Прикладом є угода про нерозголошення інформації (NDA) для захисту від розкриття найбільш конфіденційної інформації організації. Організаціям також слід звернути увагу на будь-які чинні вимоги до звітності, наприклад у контексті обміну інформацією про інциденти з ISAC або звітування про інциденти до CIRT вищого рівня.

4.2 Технології обміну інформацією

Обмін інформацією – це визначальний елемент для забезпечення координації між організаціями. Навіть у малих організацій має бути можливість обмінюватись інформацією щодо інцидентів із колегами та партнерами, щоб ефективно боротися з багатьма інцидентами. Організаціям слід здійснювати подібний обмін інформацією протягом життєвого циклу реагування на інцидент, а не чекати, поки інцидент буде повністю вирішено, перш ніж ділитися детальними даними щодо нього з іншими. У пункті 4.3 розглянуто типи інформації про інциденти, якою організації можуть хотіти або не хотіти ділитися з іншими.

Загалом, у цьому пункті йдеться про технології обміну інформацією. У пункті 4.2.1 розглянуто спеціальні технології, а в пункті 4.2.2 – частково автоматизовані технології. Врешті решт, у пункті 4.2.3 обговорюються міркування безпеки, пов’язані з обміном інформацією.

4.2.1 Спеціальні

Здебільшого обмін інформацією про інциденти традиційно відбувався за допомогою спеціальних, тобто ситуативних, технологій обміну інформацією, таких як електронна пошта, клієнтські сервіси миттєвих повідомлень і телефон. Спеціальні (ситуативні) технології обміну інформацією зазвичай залежать від зв’язків окремого працівника організації з працівниками команд реагування на інциденти партнерських організацій. Працівник використовує ці зв’язки, щоб вручну ділитися інформацією з колегами та координувати разом із ними розроблення стратегій реагування на інцидент. Залежно від розміру організації, зазначені спеціальні (ситуативні) технології можуть бути найбільш економічно ефективним способом обміну інформацією з партнерськими організаціями.
Утім, через неформальний характер спеціального (ситуативного) обміну інформацією не можна гарантувати, що процеси обміну інформацією працюватимуть завжди. Наприклад якщо з команди реагування на інциденти звільняється працівник із налагодженими зв’язками, ця команда може тимчасово втратити більшість каналів обміну інформацією, на які вона покладається для ефективної координації із зовнішніми організаціями.

Спеціальні (ситуативні) технології обміну інформацією також значною мірою не стандартизовані з погляду того, яка інформація передається і як відбуваються ці комунікації. Через відсутність стандартизації такі технології, як правило, вимагають ручного втручання і є більш ресурсомісткими для обробки, ніж інші, частково автоматизовані технології. За можливості організації необхідно намагатися формалізувати свої стратегії обміну інформацією за допомогою офіційних договорів з партнерськими організаціями і технічних механізмів, які допоможуть частково автоматизувати обмін інформацією.

4.2.2 Частково автоматизовані

Організаціям необхідно намагатися автоматизувати якомога більшу частину процесу обміну інформацією, щоб зробити міжорганізаційну координацію результативною та економічно ефективною. Повністю автоматизувати обмін всією інформацією про інциденти насправді неможливо, це також не бажано з міркувань безпеки та довіри. Організації мають намагатися досягти балансу між автоматизованим обміном інформацією та процесами, орієнтованими на людину, для управління інформаційним потоком.

Під час розроблення автоматизованих рішень для обміну інформацією організаціям слід спочатку розглянути, які типи інформації вони будуть передавати партнерам. Організація може захотіти створити офіційний словник бази даних, де будуть перераховані всі юридичні особи і зв'язки між юридичними особами, з якими вони хочуть ділитися інформацією. Щойно організація усвідомить, якими типами інформації вона буде ділитися, необхідно побудувати офіційні моделі із машинною обробкою для отримання цієї інформації. Там, де це можливо, організація має використовувати наявні стандарти обміну даними для представлення інформації, якою їм потрібно ділитися.[47] Організації необхідно співпрацювати зі своїми організаціями-партнерами під час прийняття рішення щодо моделей обміну даними, щоб гарантувати, що обрані стандарти сумісні із системами реагування на інциденти організації-партнера. Обираючи наявні моделі обміну даними, організації можуть віддати перевагу вибору кількох моделей, котрі моделюють різні аспекти області реагування на інцидент, а потім використовувати ці моделі за модульним принципом, передаючи лише ту інформацію, яка потрібна на певному етапі прийняття рішення в життєвому циклі. У Додатку Е наведено неповний перелік наявних стандартів, що визначають моделі обміну даними, котрі стосуються сфери реагування на інцидент.

Додатково до вибору моделей обміну даними для обміну інформацією про інциденти, організація також має співпрацювати зі своїми організаціями-партнерами, щоб узгодити технічні механізми транспортування для забезпечення автоматизованого обміну інформацією. Ці механізми транспортування включають, як мінімум, протокол транспортного рівня для обміну інформацією, модель архітектури для комунікацій з інформаційним ресурсом, а також відповідні порти і доменні імена для доступу до інформаційного ресурсу в конкретній організації. Наприклад група партнерських організацій може вирішити обмінюватися інформацією про інцидент за допомогою підходу до архітектури мережевих протоколів «Передача репрезентативного стану» (Representational State Transfer або REST) для обміну даними IODEF / Міжмережевої оборони у режимі реального часу (Real-Time Inter-Network Defense або RID) через Безпечний протокол передачі гіпертексту (HTTPS) до порту 4590 певного доменного імені в межах DMZ кожної організації.

4.2.3 Міркування щодо безпеки

Є кілька міркувань щодо безпеки, котрі команди реагування на інциденти повинні враховувати при плануванні обміну інформацією. Одне – це здатність визначити, хто та які частини інформації про інциденти може бачити (наприклад, захист конфіденційної інформації). Також може знадобитися провести видалення даних або очищення їх від помилок, щоб прибрати конфіденційні дані з інформації про інцидент, не зачіпаючи інформацію про прекурсори, індикатори та іншу технічну інформацію. Див. пункт 4.3 про обмін детальною інформацією. Команді реагування на інциденти також слід переконатися, що буде вжито необхідних заходів для захисту тієї інформації, якою поділилися з командою інші організації.

В контексті обміну даними існує також багато правових питань. Додаткову інформацію див. у пункті 4.1.2.

4.3 Обмін детальною інформацією

Організаціям слід збалансувати переваги обміну інформацією з недоліками обміну конфіденційною інформацією, в ідеалі ділитися виключно необхідною інформацією з відповідними сторонами. Організації можуть уявляти свою інформацію про інциденти як одне ціле, що складається з двох типів інформації: інформація щодо наслідків для бізнесу і технічна інформація. Інформацією щодо наслідків для бізнесу часто діляться в контексті взаємин команда-до-команди, що здійснює координацію, як це визначено в пункті 4.1.1, тоді як технічною інформацією часто діляться в рамках всіх трьох типів співпраці в рамках координації дій. У цьому пункті розглянуто обидва типи інформації та надано рекомендації щодо здійснення обміну детальною інформацією.

4.3.1 Інформація щодо наслідків для бізнесу

Інформація щодо наслідків для бізнесу включає те, як інцидент впливає на організацію з погляду його наслідків для місії організації, фінансових наслідків тощо. Таку інформацію, принаймні на підсумковому рівні, часто повідомляють команді реагування на інцидент вищого рівня, що здійснює координацію, щоб повідомити попереднє оцінення збитків, завданих інцидентом. Командам реагування, що здійснюють координацію, може знадобитися ця інформація щодо наслідків, щоб приймати рішення про ступінь допомоги, яка має бути надана звітній організації. Команда, що здійснює координацію, також може використовувати цю інформацію для прийняття рішень щодо того, як конкретний інцидент вплине на інші організації у спільноті, яку вона представляє.

Команди, що здійснюють координацію, можуть вимагати від організацій-учасниць звітувати про певну частину інформації щодо наслідків для бізнесу. Наприклад команда, що здійснює координацію, може вимагати від організації-учасниці повідомити інформацію щодо наслідків, використовуючи категорії, визначені в пункті 3.2.6. У цьому випадку для гіпотетичного інциденту організація повідомить, що вона має *середні* функціональні наслідки, *жодних* інформаційних наслідків, і їй буде потрібен *продовжений* час для можливості відновлення. Ця інформація високого рівня сповістить команду, яка здійснює координацію, про те, що організація-учасниця потребує певного рівня додаткових ресурсів для відновлення після інциденту. Потім команда, що здійснює координацію, могла б продовжити додаткове спілкування з організацією-учасницею, щоб визначити, скільки ресурсів потрібно, а також тип ресурсів на основі технічної інформації, наданої про інцидент.

Інформація щодо наслідків для бізнесу корисна лише для звітування організаціям, котрі певною мірою зацікавлені в забезпеченні місії організації, на якій стався інцидент. У багатьох випадках командам реагування на інциденти слід уникати обміну інформацією щодо наслідків для бізнесу із зовнішніми організаціями, якщо немає чіткої цінної пропозиції або офіційних вимог до звітності. Під час обміну інформацією з колегами та організаціями-партнерами, команди реагування на інциденти мають зосередитися на обміні технічною інформацією, як це зазначено в пункті 4.3.2.

[47] Відповідно до Закону США про передачу і вдосконалення національних технологій (NTTAA), «усі федеральні органи, агентства та відомства повинні використовувати технічні стандарти, розроблені або прийняті органами стандартизації на основі добровільного консенсусу». Див. http://standards.gov/nttaa.cfm для додаткових деталей.

4.3.2 Технічна інформація

Існує багато різних типів технічних індикаторів, які означають виникнення інциденту в організації. Ці індикатори з'являються із різноманітної технічної інформації, пов'язаної з інцидентами, такої як імена хостів та IP-адреси хостів, що атакують, зразки зловмисного програмного забезпечення, прекурсори та індикатори подібних інцидентів, а також типи вразливостей, котрими скористалися під час інциденту. Пункт 3.2.2 коротко презентує, як організації повинні збирати та використовувати ці індикатори, щоб допомогти виявити інцидент, який триває. Крім того, у пункті 3.2.3 надано перелік поширених джерел даних індикаторів інцидентів.

Незважаючи на те, що організації отримують переваги від збору власних внутрішніх індикаторів, вони можуть отримати додаткову користь від аналізу індикаторів, отриманих від організацій-партнерів, та обміну внутрішніми індикаторами для зовнішнього аналізу та використання. Якщо організація отримує дані щодо зовнішніх індикаторів, які стосуються інциденту, котрого вона не бачила, вона може використовувати ці дані індикаторів для ідентифікації інциденту, коли він починає відбуватися. Подібно до цього, організація може використовувати дані зовнішніх індикаторів для виявлення поточного інциденту, про який вона не знала через брак внутрішніх ресурсів для отримання даних конкретних індикаторів. Організації також можуть отримати переваги від обміну своїми внутрішніми даними про індикатори із зовнішніми організаціями. Наприклад якщо вони діляться технічною інформацією, що стосується інциденту, який відбувається у них, організація-партнер може відреагувати за допомогою запропонованої стратегії відновлення для управління цим інцидентом.

Організаціям необхідно ділитися якомога більшою кількістю цієї інформації; однак можуть існувати як причини, пов'язані із безпекою, так і міркування щодо відповідальності, через які організація не хоче розкривати деталі про вразливості, котрими скористалися. Зазвичай з іншими безпечно ділитися зовнішніми індикаторами, такі як загальні характеристики атак і дані хостів, що атакують. Організаціям необхідно зважити, якими типами технічної інформації слід або не слід ділитися із різними сторонами, а потім вже намагатися поділитися якомога більшою кількістю відповідної інформації з іншими організаціями.

Дані технічних індикаторів корисні, коли вони допомагають організації ідентифікувати фактичний інцидент. Хоча не всі дані індикаторів, отримані із зовнішніх джерел, будуть стосуватись організації, яка їх отримує. У деяких випадках, ці зовнішні дані будуть генерувати помилки першого роду (хибно позитивні) в мережі організації-отримувача і можуть призвести до витрачання ресурсів на вирішення неіснуючих проблем.

В організаціях, котрі беруть участь в обміні інформацією про інциденти, мають бути працівники із достатньою кваліфікацією, щоб отримувати дані про технічні індикатори від спільнот, що обмінюються інформацією, та поширювати цю інформацію по всьому підприємству, бажано із використанням автоматизованих методів. Організаціям також слід ділитися лише тими індикаторами, щодо яких практично впевнені, що вони свідчать про фактичний інцидент.

4.4 Рекомендації

Основні рекомендації щодо управління інцидентами, представлені в цьому пункті, наведено нижче.

- **Сплануйте координацію щодо інцидентів із зовнішніми сторонами до того, як інциденти виникнуть** Приклади зовнішніх сторін включають інші команди реагування на інциденти, органи правопорядку, інтернет-провайдерів, а також виборців та клієнтів. Таке планування допомагає переконатися, що всі сторони знають, які функції вони мають виконувати, і що встановлено ефективні способи комунікації між сторонами.

- **Проконсультуйтеся зі своїм юридичним відділом до того, як ініціюватимете будь-яку координацію.** Можливо, до початку обговорень необхідно укласти договори, контракти чи інші угоди.

- **Здійснюйте обмін інформацією щодо інцидентів протягом всього життєвого циклу реагування на інциденти.** Обмін інформацією – це головний елемент для забезпечення координації між організаціями. Організаціям не слід чекати, поки інцидент буде повністю вирішено, перш ніж ділитися детальними даними щодо нього з іншими.

- **Намагайтеся автоматизувати якомога більшу частину процесу обміну інформацією.** Це зробить міжорганізаційну координацію результативною та економічно ефективною. Організації мають намагатися досягти балансу між автоматизованим обміном інформацією та процесами, орієнтованими на людину, для управління інформаційним потоком.

- **Збалансуйте переваги обміну інформацією з недоліками обміну конфіденційною інформацією.** В ідеалі організаціям слід ділитися виключно необхідною інформацією з відповідними сторонами. Інформацією щодо наслідків для бізнесу часто діляться в контексті взаємин команда-до-команди, що здійснює координацію, тоді як технічною інформацією часто діляться в усіх трьох типах співпраці в рамках координації дій. Під час обміну інформацією з колегами та організаціями-партнерами, команди реагування на інциденти мають зосередитися на обміні технічною інформацією.

- **Намагайтеся поділитись якомога більшою кількістю відповідної інформації з іншими організаціями.** Організаціям необхідно зважити, якими типами технічної інформації слід або не слід ділитись із різними сторонами. Наприклад з іншими суб'єктами зазвичай безпечно ділитися зовнішніми індикаторами, такими як загальні характеристики атак і дані хостів, що атакують, але можуть існувати як причини, пов’язані з безпекою, так і міркування щодо відповідальності, через які організація не хоче розкривати деталі про вразливості, котрими скористалися.

Додаток A — Сценарії управління інцидентами

Сценарії управління інцидентами забезпечують недорогий та ефективний спосіб розвитку навичок реагування на інциденти та виявлення потенційних проблем, що можуть виникнути під час процесів реагування на інциденти. Команді реагування на інциденти або учасникам команди дають сценарій і перелік відповідних запитань. Після цього команда обговорює кожне запитання та визначає найбільш імовірну відповідь. Мета полягає в тому, щоб визначити, що справді зробила б команда в тій чи іншій ситуації, і порівняти це з політикою, порядком та загальноприйнятими методичними рекомендаціями, щоб виявити розбіжності чи недоліки. Наприклад відповідь на одне запитання може вказувати на те, що реагування буде відкладене, оскільки команді не вистачає певного програмного забезпечення або через те, що інша команда не надає підтримку в неробочий час.

Запитання, що наводяться нижче, можна використовувати практично до будь-якого сценарію. Після кожного запитання наводиться посилання на відповідний(і) пункт(и) документа. Після запитань наведено сценарії, за кожним з яких ідуть додаткові запитання, пов'язані з інцидентами. Організаціям наполегливо рекомендується адаптувати ці запитання та сценарії для використання під час власних тренувань / вправ із реагування на інциденти.[48]

A.1 Підготування запитань до сценарію

1. Чи вважатиме організація цю активність інцидентом? Якщо так, то котру з політик організації порушує ця активність? *(пункт 2.1)*
2. Яких заходів вживають, щоб запобігти подібним інцидентам або обмежити їхні наслідки? *(пункт 3.2.1)*

Виявлення та аналіз:

1. Які прекурсори інциденту, якщо такі є, могла б виявити організація? Чи могли якісь прекурсори змусити організацію вжити заходів до того, як стався інцидент? *(пункти 3.2.2, 3.2.3)*
2. Які індикатори інциденту могла б виявити організація? Які індикатори могли б спонукати когось подумати, що інцидент міг статися? *(пункти 3.2.2, 3.2.3)*
3. Які додаткові інструменти можуть знадобитися для виявлення цього конкретного інциденту? *(пункт 3.2.3)*
4. Як команда реагування на інциденти проаналізує та проведе перевірку для підтвердження цього інциденту? Який персонал буде задіяно у процесах аналізу та перевірки? *(пункт 4.2.3)*
5. Яким людям і групам в організації команда повідомлятиме про інцидент? *(пункт 7.2.3)*
6. Як команда пріоритезує управління цим інцидентом? *(пункт 6.2.3)*

Стримування, ліквідація наслідків та відновлення

1. Якої стратегії слід дотримуватися організації, щоб стримати (локалізувати) інцидент? Чому ця стратегія краща за інші? *(пункт 3.3.1)*
2. Що могло б статися, якби інцидент не стримали (локалізували)? *(пункт 3.3.1)*
3. Які додаткові інструменти можуть знадобитися для реагування на цей конкретний інцидент? *(пункти 3.3.1, 3.3.4)*

4. Який персонал буде задіяно у процесах стримування (локалізації), ліквідації та/або відновлення? *(пункти 3.3.1, 3.3.4)*
5. Які джерела доказів, якщо такі є, організація має отримати? Як саме будуть отримані докази? Де їх будуть зберігати? Протягом якого строку їх слід зберігати? *(пункти 3.2.5, 3.3.2, 3.4.3)*

Заходи після інциденту

1. Хто візьме участь у зустрічі щодо засвоєного досвіду в контексті цього інциденту? *(пункт 3.4.1)*
2. Що можна зробити, щоб подібні інциденти не траплялися в майбутньому? *(пункт 3.2.1)*
3. Що можна зробити для покращення виявлення подібних інцидентів? *(пункт 3.2.1)*

Загальні запитання:

1. Скільки учасників команди реагування на інциденти братимуть участь в управлінні цим інцидентом? *(пункт 3.4.2)*
2. Крім команди реагування на інцидент, які групи в організації будуть задіяні під час управління цим інцидентом? *(пункт 4.4.2)*
3. Яким зовнішнім сторонам команда повідомлятиме/звітуватиме про інцидент? Коли буде складено кожне повідомлення / кожен звіт? Як буде складено кожне повідомлення / кожен звіт? Яку інформацію ви включите до повідомлення/звіту, а яку – ні, і чому? *(пункт 2.3.2)*
4. Які інші комунікації із зовнішніми сторонами можуть відбуватися? *(пункт 2.3.2)*
5. Які інструменти та ресурси використала б команда для управління цим інцидентом? *(пункт 3.1.1)*
6. Які аспекти управління були б іншими, якби інцидент стався в інший день і час (в робочий і в неробочий час)? *(пункт 2.4.2)*
7. Які аспекти управління були б іншими, якби інцидент стався в іншій фізичній локації (на місці в організації чи за межами основної локації організації)? *(пункт 2.4.2)*

[48] Для отримання додаткової інформації щодо тренування, див. NIST SP 800-84, *Керівні настанови щодо програм тестування, навчання та тренування для планів і можливостей IT*, видання можна знайти за посиланням: .http://csrc.nist.gov/publications/PubsSPs.html#800-84

A.2 Сценарії

Сценарій № 1: Атака на відмову в обслуговуванні (DoS) на сервер Системи доменних імен (DNS)

У суботу вдень у зовнішніх користувачів починаються проблеми із доступом до загальнодоступних вебсайтів організації. Протягом наступної години проблема погіршується настільки, що майже кожна спроба доступу стає невдалою. Тим часом працівник організації, який займається питаннями мережі, реагує на сповіщення від граничного маршрутизатора та визначає, що пропускну здатність організації споживає надзвичайно великий обсяг пакетів Протоколу датаграм користувача (UDP), що надходить до та з обох загальнодоступних DNS-серверів організації. Аналіз трафіку показує, що DNS-сервери отримують великі обсяги запитів з однієї зовнішньої IP-адреси. Крім того, всі DNS-запити з цієї адреси надходять з одного порту відправлення.

Нижче наведено додаткові запитання для цього сценарію:

1. До кого слід звернутися організації щодо зовнішньої IP-адреси, про яку йдеться?
2. Припустимо, що після того, як були введені первинні заходи щодо стримування (локалізації), адміністратори мережі виявили, що дев’ять внутрішньоорганізаційних хостів також намагалися надіслати такі самі незвичні запити до DNS-сервера. Як це вплине на управління цим інцидентом?
3. Припустимо, що два з дев’яти внутрішньоорганізаційних хостів від’єдналися від мережі до того, як були ідентифіковані їхні власники системи. Як можна ідентифікувати власників системи?

Сценарій № 2: Зараження «хробаком» і агентом розподіленої атаки на відмову в обслуговуванні (DDoS)

У вівторок вранці опубліковано дані щодо нового «хробака»; він поширюється через знімні носії та може копіювати сам себе, щоб отримати доступ до ресурсів Windows, які знаходяться у спільному використанні. Коли «хробак» заражає хоста, він встановлює агента DDoS.

Організація зазнала масових заражень до того, як через кілька годин після початку поширення «хробака» стали доступними антивірусні сигнатури.

Нижче наведено додаткові запитання для цього сценарію:

1. Як команда реагування на інциденти визначить усі заражені хости?
2. Як організація намагатиметься запобігти проникненню «хробака» до організації перед тим, як будуть випущені антивірусні сигнатури?
3. Як організація намагатиметься запобігти поширенню «хробака» зараженими хостами перед тим, як будуть випущені антивірусні сигнатури?
4. Чи намагатиметься організація встановити патчі (латки) на всі машини та пристрої, де є вразливість? Якщо так, то як саме це буде зроблено?
5. Як змінилося б управління цим інцидентом, якби налаштування заражених хостів, котрі отримали агент DDoS, передбачали атаку на вебсайт іншої організації наступного ранку?
6. Як змінилося б управління цим інцидентом, якби на одному або кількох заражених хостах була б конфіденційна інформація, що дає змогу ідентифікувати особу, яка стосується працівників організації?
7. Як команда реагування на інциденти інформуватиме користувачів організації про стан справ щодо інциденту?

8. Яких додаткових заходів вжила б команда для хостів, які наразі не підключені до мережі (наприклад, співробітники, які зараз у відпустці, працівники, які знаходиться за межами організації та підключаються час від часу)?

Сценарій № 3: Викрадені документи

У понеділок вранці до юридичного відділу організації надійшов дзвінок від Федерального бюро розслідувань (ФБР) щодо підозрілої активності, пов'язаної із системами організації. Пізніше того самого дня агент ФБР зустрічається з керівництвом організації загалом та юридичного відділу зокрема, щоб обговорити цю активність. ФБР проводить розслідування щодо цієї активності, що передбачає опублікування конфіденційних урядових документів, і, згідно з отриманою інформацією, деякі документи належать організації. Агент просить організацію про допомогу, а керівництво просить команду реагування на інциденти допомогти з отриманням необхідних доказів, щоб визначити, справжні документи чи ні, і як міг статися витік цих документів.

Нижче наведено додаткові запитання для цього сценарію:

1. З яких джерел команда реагування на інциденти може збирати докази?
2. Що робитиме команда, щоб розслідування залишалося конфіденційним?
3. Як змінилося б управління цим інцидентом, якби команда визначила внутрішнього хоста, відповідального за витік?
4. Як змінилося б управління цим інцидентом, якби команда виявила руткіт, встановлений на внутрішньому хості, відповідальному за витік?

Сценарій № 4: Зламаний сервер бази даних

У вівторок ввечері адміністратор бази даних проводить технічне обслуговування кількох робочих серверів баз даних. На одному із серверів адміністратор помічає деякі незнайомі та незвичні назви каталогів. Після перегляду переліку файлів каталогу та деяких файлів з нього адміністратор приходить до висновку, що на сервер було здійснено атаку, і викликає на допомогу команду реагування на інциденти. За результатами розслідування команда встановила, що шість тижнів тому зловмисник успішно отримав доступ до сервера на рівні суперкористувача, тобто рута.

Нижче наведено додаткові запитання для цього сценарію:

1. Якими джерелами може скористатися команда, щоб визначити, коли відбувся злам (компрометація / несанкціонований доступ)?
2. Як змінилося б управління цим інцидентом, якби команда виявила, що сервер бази даних запустив аналізатори трафіку (сніфери) і перехопив паролі з мережі?
3. Як змінилося б управління цим інцидентом, якби команда виявила, що на сервері виконується процес, котрий щовечора копіює базу даних, що містить конфіденційну інформацію про клієнтів (включаючи інформацію, що дає змогу ідентифікувати особу), і передає її на зовнішню адресу?
4. Як змінилося б управління цим інцидентом, якби команда виявила руткіт на сервері?

Сценарій № 5: Невідоме вилучення даних

У неділю ввечері один із детекторів (датчиків) виявлення вторгнень у мережу організації сповіщає про аномальну вихідну активність мережі, яка включає передачу великих файлів. Аналітик із виявлення атак/вторгнень переглядає сповіщення; виявляється, що тисячі файлів із розширенням .RAR копіюються з внутрішнього хоста на зовнішній хост, а зовнішній хост знаходиться в іншій країні. Аналітик зв'язується з командою реагування на інцидент, щоб вона могла додатково розслідувати цю активність. Команда не може побачити вміст файлів із розширенням .RAR, оскільки їх вміст зашифровано.

Аналіз внутрішнього хоста, на якому знаходяться файли .RAR, засвідчує ознаки встановлення бота.

Нижче наведено додаткові запитання для цього сценарію:

1. Як команда визначить, що найімовірніше знаходиться у файлах із розширенням .RAR? Які інші команди можуть допомогти команді реагування на інциденти?
2. Якби команда реагування на інциденти визначила, що початковий злам (компрометація / несанкціонований доступ) був здійснений через бездротову мережеву карту на внутрішньоорганізаційному хості, як команда далі розслідуватиме цю активність?
3. Якби команда реагування на інциденти визначила, що внутрішньоорганізаційний хост використовується для передачі конфіденційних файлів з інших хостів на підприємстві, як команда далі розслідуватиме цю активність?

Сценарій № 6: Несанкціонований доступ до документів щодо оплати праці

У середу ввечері до команди, що відповідає за фізичну безпеку організації, надходить дзвінок від спеціалістки з нарахування заробітної плати, яка побачила, як невідома особа вийшла з її офісу, побігла коридором і вийшла з будівлі. Спеціалістка залишила своє робоче місце розблокованим та без нагляду лише на кілька хвилин. У застосунку із нарахування заробітної плати обліковий запис спеціалістки все ще в системі та він знаходиться у головному меню, як і тоді, коли вона залишила своє місце, але спеціалістка помічає, що мишу, схоже, рухали. Команду реагування на інциденти попросили отримати докази, пов’язані з інцидентом, та визначити, які саме дії були виконано.

Нижче наведено додаткові запитання для цього сценарію:

1. Як команда визначить, які саме дії були виконано?
2. Як змінилося б управління цим інцидентом, якби спеціалістка з нарахування заробітної плати впізнала в особі, яка вийшла з її офісу, колишнього працівника відділу нарахування заробітної плати?
3. Як змінилося б управління цим інцидентом, якби у команди були підстави вважати, що ця особа й зараз працює в організації?
4. Як змінилося б управління цим інцидентом, якби команда, що відповідає за фізичну безпеку, визначила, що особа використовувала методи соціальної інженерії, щоб отримати фізичний доступ до будівлі?
5. Як змінилося б управління цим інцидентом, якби журнали за попередній тиждень показували надзвичайно велику кількість невдалих спроб віддаленого входу за допомогою ідентифікатора користувача спеціалістки з нарахування заробітної плати?
6. Як змінилося б управління цим інцидентом, якби команда реагування на інциденти виявила, що двома тижнями раніше на комп’ютері було встановлено програмний продукт (модуль) або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера (так званий keylogger)?

Сценарій № 7: Хост, що зникає

У четвер вдень детектор (датчик) виявлення вторгнень у мережу реєструє активність із пошуку вразливостей, спрямовану на внутрішньоорганізаційні хости, котру генерує внутрішня IP-адреса. Оскільки аналітикині з виявлення атак / вторгнень невідомо про жодну санкціоновану заплановану активність із пошуку вразливостей, вона повідомляє про цю активність команді реагування на інциденти. Коли команда починає аналіз, вона виявляє, що активність зупинено і що більше не існує хоста, який використовує зазначену IP-адресу.

Нижче наведено додаткові запитання для цього сценарію:

1. Які джерела даних можуть містити інформацію про дані хоста, що здійснював пошук вразливостей?
2. Як команда визначить, хто здійснював пошук вразливостей?
3. Як змінилося б управління цим інцидентом, якби пошук вразливостей був спрямований на найкритичніші хости організації?
4. Як змінилося б управління цим інцидентом, якби пошук вразливостей був спрямований на зовнішні хости?
5. Як змінилося б управління цим інцидентом, якби внутрішньоорганізаційна IP-адреса була пов’язана з гостьовою бездротовою мережею організації?
6. Як змінилося б управління цим інцидентом, якби працівники, що відповідають за фізичну безпеку, виявили, що хтось проник на територію за півгодини до початку пошуку вразливостей?

Сценарій № 8: Злам під час віддаленої роботи

У суботу ввечері програмне забезпечення для виявлення атак/вторгнень у мережу записує вхідне з’єднання з IP-адреси, котра знаходиться у «списку спостереження». Аналітик з виявлення атак/вторгнень визначає, що встановлюється з’єднання з VPN-сервером організації, і, відповідно, зв’язується з командою реагування на інциденти. Команда переглядає журнали виявлення атак/вторгнень, брандмауера та VPN-сервера та визначає ідентифікатор користувача, що автентифікувався для сеансу, та ім’я користувача, пов’язане з визначеним ідентифікатором користувача.

Нижче наведено додаткові запитання для цього сценарію:

1. Яким має бути наступний крок команди (наприклад, зателефонувати користувачеві додому, вимкнути ідентифікатор користувача, відключити сеанс VPN)? Чому цей крок слід виконати першим? Який крок слід виконати другим?
2. Як змінилося б управління цим інцидентом, якби зовнішня IP-адреса належала до відкритого проксі?
3. Як змінилося б управління цим інцидентом, якби ідентифікатор використовувався для ініціювання VPN-з’єднань із кількох зовнішніх IP-адрес без відома користувача?
4. Припустимо, що злам комп’ютера визначеного користувача відбувся через гру, котру завантажив член сім’ї та яка містить троянську програму. Як це вплине на аналіз інциденту командою? Як це вплине на збір доказів та управління ними? Що має зробити команда, щоб ліквідувати інцидент із комп’ютера користувача?
5. Припустимо, що користувач встановив антивірусне програмне забезпечення і визначив, що троянська програма включила програмний продукт (модуль) або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера (так званий keylogger). Як це вплине на управління цим інцидентом? Як змінилося б управління цим інцидентом, якби користувач був адміністратором системи? Як змінилося б управління цим інцидентом, якби користувач був високопоставленим керівником в організації?

Сценарій № 9: Анонімна загроза

У четвер вдень до команди, що відповідає за фізичну безпеку організації, надходить дзвінок від IT-менеджерки, яка повідомила, що двоє її співробітників щойно отримали анонімні погрози, які стосуються систем організації. За результатами розслідування команда, що відповідає за фізичну безпеку, вважає, що до загроз слід поставитися серйозно і повідомляє про загрози відповідні внутрішні команди, включаючи команду реагування на інциденти.

Нижче наведено додаткові запитання для цього сценарію:

1. Що команда реагування на інциденти має зробити інакше, якщо таке є, у відповідь на повідомлення про загрози?
2. Який вплив можуть мати заходи з підвищеного рівня фізичної безпеки на те, як команда реагуватиме на інциденти?

Сценарій № 10: Файлообмінні мережі

Організація забороняє користуватися службами файлообмінних мереж. У детекторах (датчиках) виявлення вторгнень у мережу організації увімкнено сигнатури, які можуть виявляти використання кількох популярних служб файлообмінних мереж. У понеділок ввечері аналітик із виявлення атак/вторгнень помічає, що протягом останніх трьох годин з'явилося кілька сповіщень про спільний доступ до файлів і всі вони стосувалися однієї внутрішньоорганізаційної IP-адреси.

1. Які чинники слід використовувати для пріоритезації управління цим інцидентом (наприклад, явний вміст файлів, до яких надається спільний доступ)?
2. Які міркування щодо конфіденційності можуть вплинути на управління цим інцидентом?
3. Як змінилося б управління цим інцидентом, якби комп'ютер, який здійснює обмін файлами, також містив конфіденційну інформацію, що дає змогу ідентифікувати особу?

Сценарій № 11: Невідомі бездротові точки доступу

У понеділок вранці до служби підтримки організації надходять дзвінки від трьох користувачів, що працюють на одному поверсі будівлі, які заявляють, що у них виникли проблеми з бездротовим доступом. Адміністратор мережі, якого просять допомогти у вирішенні проблеми, приносить ноутбук із бездротовим доступом на поверх користувачів. Переглядаючи налаштування бездротової мережі у себе на ноутбуці, він помічає, що є нова точка доступу, яка вказана як доступна. Він разом з учасниками свої команди перевіряє та визначає, що ця точка доступу не була створена його командою, тож, швидше за все, це шахрайська точка доступу, створена без дозволу.

1. Яким має бути перший важливий крок у рамках управління цим інцидентом (наприклад, фізичний пошук шахрайської точки доступу, логічне підключення до точки доступу)?
2. Який найшвидший спосіб виявити місцезнаходження точки доступу? Який найбільш непомітний чи прихований спосіб виявити місцезнаходження точки доступу?
3. Як змінилося б управління цим інцидентом, якби точку доступу створила стороння сторона (наприклад, підрядник), котра тимчасово працює в офісі організації?
4. Як змінилося б управління цим інцидентом, якби аналітик із виявлення атак/вторгнень повідомив про ознаки підозрілої активності, пов'язаної з деякими робочими станціями на тому самому поверсі будівлі?
5. Як змінилося б управління цим інцидентом, якби точку доступу було видалено, поки команда все ще намагалася фізично знайти її місцезнаходження?

Додаток B — Елементи даних, пов'язані з інцидентами

Організації повинні визначити стандартний набір елементів даних, пов'язаних із інцидентами, котрі слід збирати для кожного інциденту. Це не тільки сприятиме більш ефективній та послідовній обробці інцидентів, але й допоможе організації забезпечити відповідність чинним вимогам щодо звітування про інциденти. Організації необхідно затвердити набір основних елементів (наприклад, ім’я особи, що повідомила / подала звіт про інцидент, номер телефону та місцезнаходження), які будуть зібрані, коли надійде повідомлення/звіт про інцидент, і набір додаткових елементів, які збиратимуть фахівці з управління інцидентами під час реагування. Ці два набори елементів будуть основою для бази даних щодо звітування про інциденти, про яку йшлося в пункті 3.2.5. Наведені нижче списки містять пропозиції щодо того, яку інформацію слід збирати для інцидентів, і вони не є вичерпними. Кожна організація на основі кількох чинників, включаючи модель і структуру команди реагування на інциденти, а також визначення терміну «інцидент», повинна створити свій власний список елементів.

B.1 Основні елементи даних

- Контактні дані особи, яка повідомляє/звітує про інцидент, та особи, яка займається управлінням інцидентами
  - Ім’я
  - Виконувані функції
  - Організація чи структурний підрозділ (наприклад, орган / відомство / установа, управління / відділ, сектор, команда)
  - Адреса електронної поштової скриньки
  - Номер телефону
  - Місцезнаходження (наприклад, поштова адреса, номер кабінету)
- Подробиці щодо інциденту
  - Дата / часові мітки зміни статусу (включаючи часовий пояс): коли інцидент почався, коли інцидент було помічено/виявлено, коли надійшло повідомлення про інцидент, коли інцидент було вирішено/завершено тощо.
  - Фізичне місцезнаходження інциденту (наприклад, місто, штат)
  - Поточний стан справ щодо інциденту (наприклад, атака, що триває)
  - Джерело/причина інциденту (якщо вони відомі), включаючи імена хостів та IP-адреси
  - Опис інциденту (наприклад, як його виявили, що саме сталося)
  - Опис ресурсів, що постраждали (наприклад, мережі, хости, застосунки, дані), включаючи імена хостів, IP-адреси та функції систем
  - Якщо відомо, категорія інциденту, вектори атаки, пов’язані з інцидентом, та індикатори, пов’язані з інцидентом (закономірності трафіку, ключі реєстру тощо)
  - Чинники пріоритезації (функціональні наслідки, інформаційні наслідки інциденту, можливість відновлення після інциденту тощо)
  - Пом’якшувальні чинники (наприклад, викрадений ноутбук із конфіденційними даними використовував повне шифрування диска)
  - Вжиті заходи з реагування (наприклад, вимкнути хост, відключити хост від мережі)
  - Інші організації, до яких зверталися (наприклад, постачальник програмного забезпечення)
- Загальні коментарі

B.2 Елементи даних для куратора інциденту

- Поточний стан справ щодо реагування на інцидент
- Коротка довідка щодо інциденту
- Дії/заходи з управління інцидентами
  - Журнал із діями, що були вжиті всіма особами, які брали участь в управлінні інцидентом
  - Контактні дані всіх залучених сторін
  - Перелік зібраних доказів
- Коментарі та зауваження осіб, які брали участь в управлінні інцидентом
- Причина інциденту (наприклад, неправильно налаштований застосунок, хост без належно налаштованих засобів для усунення вразливостей (патчів)
- Витрати на ліквідацію наслідків інциденту
- Загальний вплив інциденту на бізнес[49]

[49] Загальний вплив інциденту на бізнес може бути або описом наслідків інциденту (наприклад, бухгалтерія не здатна виконувати свої функції протягом двох днів) або категорією наслідків на основі витрат на їх ліквідацію (наприклад, «серйозний» інцидент передбачає витрати на ліквідацію розміром понад 100 000 доларів США).

Додаток С — Термінологічний словник

Окремі скорочення, що використовуються в цьому виданні, визначені нижче.

Оцінювання базової продуктивності мережі (baselining) Моніторинг ресурсів для визначення типових моделей чи закономірностей використання, щоб можна було виявити значні відхилення.

Інцидент, пов’язаний із комп'ютерною безпекою: Див. «інцидент».

Команда реагування на інциденти, пов’язані з комп’ютерною безпекою (CSIRT): Ресурс, створений з метою надання допомоги в реагуванні на інциденти, пов’язані з комп’ютерною безпекою; також називається Командою реагування на комп’ютерні інциденти (CIRT) або CIRC (Центр реагування на комп’ютерні інциденти, Потенціал реагування на комп’ютерні інциденти).

Подія: Будь-яке явище, що спостерігається в системі або мережі.

Помилки першого роду (хибно позитивні): Сповіщення користувача, що відбувається зловмисна діяльність.

Інцидент: Порушення або неминуча загроза порушення політики комп’ютерної безпеки, політики прийнятного користування або стандартних методів забезпечення захисту програм.

Управління інцидентами: Пом’якшення порушень політики безпеки, методичних та практичних рекомендацій.

Реагування на інцидент: Див. «управління інцидентами».

Індикатор: Ознака того, що інцидент, можливо, вже стався або, можливо, відбувається саме зараз.

Система виявлення та запобігання атакам/вторгненням (IDPS): Програмне забезпечення, яке автоматизує процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі, аналізує їх на ознаки можливих інцидентів і намагається зупинити виявлені можливі інциденти.

Шкідливе (зловмисне) програмне забезпечення: Вірус, «хробак», троянська програма (так званий троян, троянець або Троянський кінь) або інше зловмисний об’єкт на основі коду, котрий успішно заражає хост.

Прекурсор: Ознака того, що зловмисник може готуватися до інциденту.

Профілювання: Аналізування та вимірювання динамічних показників очікуваної активності, щоб можна було легше ідентифікувати зміни у ній.

Сигнатура: Доступна для розпізнавання закономірність, яку легко вирізнити, що пов’язана з атакою, наприклад двійковий рядок у вірусі або певний набір натискань на клавіші клавіатури комп'ютера, що використовуються для отримання несанкціонованого доступу до системи.

Соціальна інженерія: Спроба обманом змусити когось розкрити інформацію (наприклад, пароль), яку можна використати для атаки на системи чи мережі.

Загроза: Потенційне джерело небажаної події.

Вразливість: Слабке місце у системі, програмі чи мережі, яке є об’єктом експлуатації або неправильного використання.

Додаток D — Скорочення

Окремі скорочення, що використовуються в цьому виданні, визначені нижче.

CCIPS Відділ комп'ютерної злочинності та злочинності у сфері інтелектуальної власності

CERIAS Центр навчання та досліджень у сфері інформаційної безпеки

CERT®/CC Координаційний центр CERT®

CIO Начальник інформаційного управління (інформаційної служби)

CIRC Потенціал реагування на комп'ютерні інциденти

CIRC Центр реагування на комп'ютерні інциденти

CIRT Команда реагування на комп'ютерні інциденти

CISO Керівник з інформаційної безпеки

CSIRC Потенціал реагування на інциденти, пов'язані з комп'ютерною безпекою

CSIRT Команда реагування на інциденти, пов'язані з комп'ютерною безпекою

DDoS Розподілена атака на відмову в обслуговуванні

DHS Міністерство національної безпеки США (інша назва: Департамент внутрішньої безпеки)

DNS Система доменних імен

DoS Відмова в обслуговуванні / Атака на відмову в обслуговуванні

FAQ Часті запитання

FBI Федеральне бюро розслідувань (ФБР)

FIPS Федеральні стандарти обробки інформації

FIRST Форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою

FISMA Федеральний закон США про управління інформаційною безпекою

GAO Рахункова палата США

GFIRST Урядовий форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою

GRS Порядок ведення загальної документації

HTTP Протокол передачі гіпертекстових документів

IANA Адміністрація адресного простору інтернету (Internet Assigned Numbers Authority)

IDPS Система виявлення та запобігання атакам/вторгненням

IETF Відкрите міжнародне співтовариство проєктувальників, учених, мережевих операторів і провайдерів (Internet Engineering Task Force)

IP Інтернет-протокол

IR Міжвідомчий звіт

IRC Технологія багатокористувацьких конференцій у текстовому режимі через інтернет (Internet Relay Chat)

ISAC Центр обміну й аналізу інформації

ISP Інтернет-провайдери

IT Інформаційні технології

ITL Лабораторія інформаційних технологій

MAC Управління доступом до середовища

MOU Меморандум про взаєморозуміння

MSSP Постачальник послуг з управління інформаційною безпекою

NAT Механізм перетворення мережевих адрес (Network Address Translation)

NDA Угода про нерозголошення інформації

NIST Національний інститут стандартів і технології

NSRL Національна довідкова бібліотека програмного забезпечення

NTP Мережевий протокол часу

NVD Національна база даних вразливостей

OIG Управління генерального інспектора

OMB Відділ із питань управління та бюджету

OS Операційна система

PII Інформація, що дає змогу ідентифікувати особу

PIN Персональний ідентифікаційний номер

POC Контактна установа / особа («точка контакту»)

REN-ISAC Науково-освітній мережевий центр обміну й аналізу інформації

RFC Прохання прокоментувати

RID Міжмережева оборона у режимі реального часу

SIEM Системи управління інформацією та подіями безпеки

SLA Угода про рівень послуг

SOP Типовий порядок дій

SP Спеціальне видання стандарту

TCP Протокол керування передаванням (Transmission Control Protocol)

TCP/IP Протокол керування передаванням (Transmission Control Protocol) / Міжмережевий протокол (Internet Protocol)

TERENA Транс'європейська науково-освітня мережева асоціація

UDP Протокол датаграм користувача (User Datagram Protocol)

URL Уніфікований локатор ресурсів або адреса ресурсу

US-CERT Комп’ютерна команда екстреної готовності Сполучених Штатів

VPN Віртуальна приватна мережа

Додаток E — Ресурси

Наведені нижче списки містять приклади ресурсів, котрі можуть бути корисними у створенні та підтримці потенціалу реагування на інциденти.

Організації реагування на інциденти

Організація	URL-адреса
Робоча група з питань боротьби з фішингом (APWG)	http://www.antiphishing.org/
Відділ комп'ютерної злочинності та злочинності у сфері інтелектуальної власності (CCIPS), Міністерство юстиції США	http://www.cybercrime.gov/
Координаційний центр CERT®, Університет Карнегі-Меллон (CERT®/CC)	http://www.cert.org/
Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA)	http://www.enisa.europa.eu/activities/cert
Форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою (FIRST)	http://www.first.org/
Урядовий форум команд реагування на інциденти, пов'язані з комп'ютерною безпекою (GFIRST)	lhttp://www.us-cert.gov/federal/gfirst.htm
Асоціація розслідувань злочинів у сфері високих технологій (HTCIA)	http://www.htcia.org/
Громадська організація «Infragard» (ППП між ФБР та бізнесом США)	http://www.infragard.net/
Центр «Internet Storm Center» Інституту SANS (ISC)	http://isc.sans.edu/
Національна рада ISAC	http://www.isaccouncil.org/
Команда екстреного реагування на кіберінциденти Сполучених Штатів (US-CERT)	http://www.us-cert.gov/

Видання NIST

Назва ресурсу	URL-адреса
NIST SP 800-53 Третя редакція, *Рекомендовані заходи контролю для федеральних інформаційних систем та організацій*	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NIST SP 800-83, *Керівні настанови щодо запобігання та управління інцидентами з використанням зловмисного програмного забезпечення*	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NIST SP 800-84, *Керівні настанови щодо програм тестування, навчання та тренування для планів і можливостей IT*	http://csrc.nist.gov/publications/PubsSPs.html#800-84
NIST SP 800-86, *Керівні настанови щодо інтегрування методів криміналістики до реагування на інциденти*	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NIST SP 800-92, *Керівні настанови щодо управління журналами, пов'язаними з комп'ютерною безпекою*	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NIST SP 800-94, *Керівні настанови щодо систем виявлення та запобігання атакам / вторгненням (IDPS)*	http://csrc.nist.gov/publications/PubsSPs.html#800-94
NIST SP 800-115, *Технічні керівні настанови щодо тестування та оцінювання інформаційної безпеки*	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NIST SP 800-128, *Керівні настанови з орієнтованого на безпеку управління конфігурацією інформаційних систем*	http://csrc.nist.gov/publications/PubsSPs.html#800-128

Специфікації обміну даними, котрі стосуються управління інцидентами

Назва	Опис	Додаткові відомості
AI	Ідентифікація активів	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7693
ARF	Формат результатів активів	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7694
CAPEC	Загальний реєстр і класифікація схем проведення (закономірностей) атак	http://capec.mitre.org/
CCE	Загальний реєстр конфігурацій	http://cce.mitre.org/
CEE	Загальне вираження подій (Уніфікована мова для надання інформації про події)	http://cee.mitre.org/
CPE	Загальний реєстр платформ	http://cpe.mitre.org/
CVE	Загальновідомі вразливості інформаційної безпеки	http://cve.mitre.org/
CVSS	Загальна система оцінки вразливостей	http://www.first.org/cvss/cvss-guide
CWE	Загальний реєстр слабких місць	http://cwe.mitre.org/
CybOX	Cyber Observable eXpression (Стандартизована мова для опису індикаторів подій безпеки, за якими спостерігають)	http://cybox.mitre.org/
MAEC	Реєстр і характеристики атрибутів зловмисного програмного забезпечення	http://maec.mitre.org/
OCIL	Відкрита інтерактивна мова опису контрольного списку	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7692
OVAL	Відкрита мова оцінювання вразливостей	http://oval.mitre.org/
RFC 4765	Формат обміну повідомленнями про вторгнення (IDMEF)	http://www.ietf.org/rfc/rfc4765.txt
RFC 5070	Формат обміну інформацією з описом інцидентних об’єктів (IODEF)	http://www.ietf.org/rfc/rfc5070.txt
RFC 5901	Розширення до IODEF щодо звітування про фішинг	http://www.ietf.org/rfc/rfc5901.txt
RFC 5941	Обмін даними щодо шахрайства із господарськими операціями	http://www.ietf.org/rfc/rfc5941.txt
RFC 6545	Міжмережева оборона у режимі реального часу (RID)	http://www.ietf.org/rfc/rfc6545.txt
RFC 6546	Передача повідомлень Міжмережевої оборони у режимі реального часу (RID) через HTTP/TLS	http://www.ietf.org/rfc/rfc6546.txt
SCAP	Протокол автоматизації управління даними безпеки	http://csrc.nist.gov/publications/PubsSPs.html #SP-800-126-Rev.%202
XCCDF	Розширюваний формат опису контрольного списку перевірки конфігурації	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7275-r4

Додаток F — Часті запитання

У користувачів, адміністраторів системи, працівників, які займаються питаннями інформаційної безпеки, та інших в організації можуть виникнути запитання щодо реагування на інциденти. Нижче наведено часті запитання (FAQ).
Організаціям рекомендується налаштувати ці часті запитання та надати доступ до них спільноті користувачів.

1. Що таке інцидент?

Загалом, інцидент – це порушення політики комп'ютерної безпеки, політики прийнятного користування або стандартних методів забезпечення захисту комп'ютерних програм. Приклади інцидентів включають:

- Зловмисник дає команду ботнету надсилати до одного з вебсерверів організації велику кількість запитів на з'єднання, що призводить до його збою.
- Користувачів обманом змушують відкрити вкладений до листа «квартальний звіт», надісланий електронною поштою, котрий насправді є шкідливим програмним забезпеченням: запуск цього файлу заразив їхні комп'ютери та встановив з'єднання із зовнішнім хостом.
- Зловмисник отримує несанкціонований доступ до конфіденційних даних та погрожує оприлюднити їх ЗМІ, якщо організація не заплатить визначену суму грошей.
- Користувач надає неліцензійні копії програмного забезпечення стороннім особам за допомогою служб файлообмінних мереж.

2. Що таке управління інцидентами?

Управління інцидентами – це процес виявлення та аналізу інцидентів та обмеження наслідків інциденту. Наприклад якщо зловмисник проникає в систему через інтернет, процес управління інцидентами має виявити злами та порушення у сфері безпеки. Потім фахівці з управління інцидентів аналізують дані та визначають, наскільки серйозною є атака. Інциденту визначають пріоритетність, а фахівці з управління інцидентами вживають заходів, щоб зупинити розвиток інциденту та якнайшвидше відновити нормальну роботу уражених систем.

3. Що таке реагування на інциденти?

Терміни «управління інцидентами» та «реагування на інцидент» є синонімічними у цьому документі.[50]

4. Що таке команда реагування на інциденти?

Команда реагування на інциденти (також відома як Команда реагування на інциденти, пов'язані з комп'ютерною безпекою [CSIRT]) відповідає за надання послуг із реагування на інциденти частині організації або всій організації. Команда отримує інформацію про можливі інциденти, розслідує їх і вживає заходів для мінімізації шкоди, завданої інцидентами.

5. Які послуги надає команда реагування на інциденти?

Детальний перелік послуг, які надають команди реагування на інциденти, значно відрізняються у різних організаціях. Окрім управління інцидентами, більшість команд також беруть на себе відповідальність за моніторинг і керування системою виявлення атак/вторгнень. Команда також може розповсюджувати рекомендації щодо нових загроз і проводити навчання для користувачів та IT-персоналу щодо їхніх функцій під час запобігання інцидентам та управління ними.

6. Кого слід повідомити та кому слід звітувати про інциденти?

Організаціям необхідно чітко визначити контактну особу / установу (так звані контактні особи або POC) для внутрішнього звітування про інциденти. Деякі організації структурують свій потенціал реагування на інциденти так, щоб про всі інциденти повідомляли безпосередньо команді реагування на інциденти, тоді як інші використовують наявні підрозділи, що надають підтримку, такі як служба IT-підтримки, у ролі первинної POC. Організація має усвідомлювати, що зовнішні сторони, такі як інші команди реагування на інциденти, повідомлятимуть/звітуватимуть про деякі інциденти. Відповідно до закону федеральні органи, відомства та агенції зобов'язані повідомляти про всі інциденти до Комп'ютерної команди екстреної готовності Сполучених Штатів (US-CERT). Рекомендується, щоб усі організації повідомляли про інциденти до відповідних Команд реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT). Якщо організація не має власної CSIRT, до якої можна звернутися, вона може повідомляти про інциденти іншим організаціям, включаючи Центри обміну й аналізу інформації (ISAC).

7. Як слід повідомляти/звітувати про інциденти?

Більшість організацій мають кілька методів, щоб повідомити/прозвітувати про інцидент. Перевагу можна надавати різним методам повідомлення/звітування залежно від навичок особи, яка повідомляє про активність, терміновості вжиття заходів через інцидент та конфіденційності інциденту. Слід визначити номер телефону для повідомлення про надзвичайні ситуації. Для неофіційного повідомлення/звітування про інциденти може бути надана адреса електронної поштової скриньки, тоді як для офіційного звітування про інциденти може бути корисною вебформа. Конфіденційну інформацію можна надати команді за допомогою опублікованого командою відкритого ключа для шифрування матеріалів.

8. Яку інформацію слід надати, повідомляючи/звітуючи про інцидент?

Чим точнішою буде інформація, тим краще. Наприклад якщо здається, що робоча станція була заражена зловмисним програмним забезпеченням, повідомлення/звіт про інцидент має містити якомога більше таких даних, наскільки це практично доречно:

- Ім'я користувача, ідентифікатор користувача та контактна інформація (наприклад, номер телефону, адреса електронної пошти)
- Місцезнаходження робочої станції, номер моделі, серійний номер, ім'я хоста та IP-адреса
- Дата і час виникнення інциденту
- Покрокове пояснення того, що сталося, включаючи те, що зробили з робочою станцією після виявлення зараження. Це пояснення має бути детальним, включаючи точні формулювання повідомлень, наприклад тих, які відображаються зловмисним програмним забезпеченням, або сповіщень антивірусного програмного забезпечення.

---

50 Визначення «управління інцидентами» та «реагування на інциденти» дуже відрізняються. Наприклад, CERT®/CC використовує термін «управління інцидентами» для позначення загального процесу виявлення інцидентів, звітування, аналізу та реагування, тоді як «реагування на інциденти» вживається виключно щодо стримування/локалізації інцидентів, відновлення після них та сповіщення інших. Див. http://www.cert.org/csirts/csirt_faq.htmlдля отримання додаткової інформації.

9. Як швидко команда реагування на інцидент реагує на повідомлення/звіт про інцидент?

Час реагування залежить від кількох чинників, таких як тип інциденту, критичність ресурсів і даних, які постраждали, градація інциденту для опису рівня загрози чи небезпеки, чинні Угоди про рівень послуг (SLA) для ресурсів, які постраждали, час і день тижня, а також інші інциденти, якими управляє команда. Як правило, найвищий пріоритет має управління тими інцидентами, які можуть завдати найбільшої шкоди організації чи іншим організаціям.

10. Коли особі, яка була залучена до інциденту, слід звернутися до органів правопорядку?

Комунікації з органами правопорядку мають бути ініційовані учасниками команди реагування на інциденти, начальниками інформаційних управлінь (CIO) або іншою посадовою особою. Користувачам, адміністраторам системи, власникам системи та іншим причетним сторонам не можна ініціювати контакт.

11. Що робити людині, яка виявила атаку на систему?

Цій людині слід негайно припинити використання системи та зв’язатися з командою реагування на інцидент. Людині може знадобитися допомога у первинній обробці інциденту, наприклад у здійсненні фізичного моніторингу системи, поки не прибудуть фахівці з управління інцидентами, щоб захистити докази, які є в системі.

12. Що треба робити людині, до якої звернулися ЗМІ із запитаннями щодо інциденту?

Така особа може відповідати на запитання ЗМІ відповідно до політики організації з питань інцидентів та зовнішніх сторін. Якщо в особи немає повноважень представляти організацію з метою обговорення інциденту, вона не повинна давати жодних коментарів щодо інциденту, окрім того, що перенаправити людину, яка зателефонувала, до служби зі зв’язків із громадськістю організації. Це допоможе службі зі зв’язків із громадськістю надавати ЗМІ та громадськості точну та послідовну інформацію.

Додаток G — Кроки з врегулювання кризи

Це список основних кроків, які слід виконати, якщо технічний фахівець вважає, що стався серйозний інцидент, а організація не має можливості реагувати на інцидент. Це – основний еталон того, що слід робити для тих, хто стикнувся з кризою і не має часу прочитати весь цей документ.

1. **Документуйте все.** Це включає кожну виконану дію, кожен доказ і кожну розмову з користувачами, власниками системи та іншими особами чи організаціями щодо інциденту.
2. **Знайдіть колегу, який зможе надати вам допомогу.** Управління інцидентом стане набагато легшим, якщо двоє або більше людей працюватимуть разом. Наприклад одна людина може виконувати дії, а інша документувати їх.
3. **Проаналізуйте докази, щоб підтвердити, що інцидент дійсно стався.** За потреби проведіть додаткові дослідження (наприклад, пошукові системи в інтернеті, документація до програмного забезпечення), щоб краще зрозуміти докази. Зверніться по додаткову допомогу до інших технічних фахівців в організації.
4. **Повідомте відповідних людей в організації.** Перелік має включати начальника інформаційного управління (CIO), керівника служби інформаційної безпеки та місцевого фахівця з інформаційної безпеки. Пам’ятайте про обережність, обговорюючи деталі інциденту з іншими; розповідайте лише тим людям, яким необхідно знати і використовуйте механізми зв’язку, які мають достатній рівень безпеки. (Якщо зловмисник зламав служби електронної пошти, не надсилайте електронних листів про інцидент.)
5. **Повідомте US-CERT та/або інші зовнішні організації**, що вам потрібна допомога в подоланні інциденту.
6. **Припиніть інцидент, якщо він все ще триває.** Найпоширеніший спосіб зробити це – від’єднати уражені системи від мережі. У деяких випадках може знадобитися змінити конфігурацію брандмауера та маршрутизатора, щоб зупинити мережевий трафік, який є частиною інциденту, наприклад атаки на відмову в обслуговуванні (DoS).
7. **Збережіть докази інциденту.** Зробіть резервні копії (бажано резервні копії образів дисків, а не резервні копії файлової системи) уражених систем. Зробіть копії файлів журналів, які містять докази, пов’язані з інцидентом.
8. **Усуньте всі наслідки інциденту.** Це включає зараження зловмисним програмним забезпеченням, невідповідні матеріали (наприклад, піратське програмне забезпечення), файли троянських програм та будь-які інші зміни, внесені до системи внаслідок інцидентів. Якщо систему було повністю зламано, перебудуйте її з нуля або відновіть із резервної копії, яка є гарантовано справною.
9. **Виявіть і пом’якшіть наслідки всіх вразливостей, котрими скористалися** Інцидент міг статися через використання вразливостей операційних систем або застосунків. Дуже важливо виявити такі вразливості й усунути або в інший спосіб пом’якшити їх, щоб інцидент не повторився.
10. **Переконайтеся, що нормальну роботу відновлено.** Впевніться, що уражені внаслідок інциденту дані, застосунки та інші служби повернули до нормального режиму роботи.
11. **Підготуйте кінцевий звіт** У цьому звіті має бути детально описано процес управління інцидентами. У ньому також має бути представлено короткий огляд того, що сталося, і як офіційний потенціал реагування на інциденти міг би допомогти впоратися з ситуацією, зменшити ризик і швидше обмежити завдану шкоду.

Додаток H — Журнал змін

Друга редакція Проєкт документа № 1 – січень 2012 року Правки від редактора:

- Забезпечено стислість викладу в усьому виданні
- Внесено незначні зміни у форматуванні в усьому виданні

Технічні зміни:

- Розширено матеріал щодо обміну інформацією (скрізь у Розділі 2)
- Оновлено переліки організацій, котрим звітують щодо інцидентів (пункт 2.3.4.3)
- Оновлено перелік поширених послуг команд реагування на інциденти (пункт 2.5)
- Переглянуто діаграми життєвого циклу реагування на інциденти (скрізь у Розділі 3)
- Оновлено перелік векторів атаки (пункт 3.2.1)
- Перероблено чинники для пріоритезації управління інцидентами (пункт 3.2.6)
- Змінено фокус з визначення зловмисника на визначення хоста, що атакує (пункт 3.3.3)
- Розширено перелік можливих показників інцидентів (пункт 3.4.2)
- Оновлено сценарії управління інцидентами, щоб відображати поточні загрози (стара версія Додатку B, нова версія Додатку A)
- Зроблено незначні оновлення пропозицій щодо галузевих даних, пов'язаних із інцидентами (стара версія Додатку C, нова версія Додатку B)
- Оновлено всі переліки інструментів та ресурсів (стара версія Додатку G, нова версія Додатку E)
- Оновлено «Часті запитання» та «Кроки з врегулювання кризи», щоб відобразити зміни, внесені в інших місцях видання (старі версії Додатків H та I, нові версії Додатків F і G)

Видалення:

- Вилучено матеріал із криміналістики, що повторювався, читачам надано посилання на SP 800-86 для отримання цієї інформації (пункт 3.3.2)
- Видалено матеріал, що стосувався старих категорій інцидентів (розділи 4-8)
- Видалено список рекомендацій, що повторювався (стара версія Додатку A)
- Видалено перелік друкованих ресурсів (стара версія Додатку F)
- Видалено категорії звітування про інциденти федеральних органів та відомств (стара версія Додатку J)

Друга редакція Остаточна – серпень 2012 року Правки від редактора:

- Внесено незначні правки до всього видання

Технічні зміни:

- Додано обмін інформацією як послугу команди (пункт 2.5)
- Таблицю 3-1 перетворено на маркерні списки (пункт 3.1.1)
- Додано згадку про тренування/вправи (пункт 3.1.1)
- Переглянуто вектори атак (раніше були категорії інцидентів) (пункт 3.2.1)
- Додано SIEM, потоки трафіку в мережах як поширені джерела прекурсорів та індикаторів (пункт 3.2.3)
- Розширене обговорення ліквідації наслідків та відновлення (пункт 3.3.4)
- Додано пункт про координацію та обмін інформацією (Розділ 4)
- Додано таблицю специфікацій обміну даними, котрі стосуються управління інцидентами (Додаток E)