Додаток
до розпорядження голови
районної в місті ради
від 09.11.2017 № 244-р

Методика
виявлення та реєстрації інцидентів інформаційної безпеки
у виконкомі Довгинцівської районної в місті ради

Зміст

1. Вступ

Методика виявлення та реєстрації інцидентів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради (далі - методика виявлення та реєстрації інцидентів) розроблена відповідно до вимог ДСТУ ISO/IEC 270001:2015 та розповсюджується на всі структурні підрозділи виконкому районної в місті ради.

Цілі впровадження методики виявлення та реєстрації інцидентів:

- оперативний моніторинг стану інформаційної безпеки в рамках дії системи інформаційної безпеки виконкому районної у місті ради;
- виявлення, облік, реагування, розслідування та аналіз інцидентів інформаційної безпеки;
- інформування керівництва виконкому районної в місті ради та зацікавлених осіб про поточний стан інформаційної безпеки.

При здійсненні дій пов’язаних із управлінням інцидентами керуватися даною методикою, а також настановами актуальними стандартами ISO/IEC 27001 та ISO/IEC 27002 (його національними версіями, або іншим нормативним документом, що їх замінюють).

Вимоги методики розповсюджуються на всі структурні підрозділи виконавчого комітету районної в місті ради.

Відповідальність за управління інцидентами, а також за контролювання

дотримання вимогам даного положення несе керуючий справами виконкому Довгинцівської районної в місті ради.

2. Терміни та визначення

В даному положенні використовуються терміни та визначення понять згідно ДСТУ ISO/IEC 27001:2015 та ISO/IEC 27002:2013, а також такі:

Подія інформаційної безпеки - ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідома ситуація, яка може бути істотною для безпеки.

Інцидент інформаційної безпеки - подія, що є наслідком одного або декількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації операції і створення загрози ІБ.

Група реагування на інциденти інформаційної безпеки (ГРІІБ) являється групою (командою) відповідно навчених працівників виконкому районної в місті ради, яка обробляє інциденти ІБ під час їхнього життєвого циклу. Іноді ця група може доповнюватися зовнішніми експертами, наприклад, з офіційно визнаною групи реагування на комп'ютер-ні інциденти або комп'ютерної групи швидкого реагування (КГШР).

Хост (вузол) - будь-який пристрій, що надає сервіси формату «клієнт-сервер» в режимі сервера з будь-якими інтерфейсам і унікально визначене на цих інтерфейсах;

Додаток (застосунок, застосовна програма, прикладна програма) - користувацька комп'ютерна програма, що дає змогу вирішувати конкретні прикладні задачі користувача;

Експлой - комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему.

3. Нормативні посилання

В даній методиці використовуються посилання на наступні нормативні документи:

- ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;
- ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Звід правил по управлінню захистом інформації».

4. Предмет методики та опис дій

4.1. Ознаки інциденту інформаційної безпеки

Припущення того, що в виконкомі районної в місті ради стався інцидент інформаційної безпеки, має базуватися на трьох основних факторах:

- повідомлення про інцидент інформаційної безпеки надходять одночасно з декількох джерел (працівники виконкому, системи виявлення вторгнення (IDS), журнальні файли);

- IDS сигналізують про багаторазове повторення подій;
- аналіз журнальних файлів автоматизованої системи дає підставу для висновку про можливість настання події інциденту.

В загальному випадку, ознаки інциденту поділяються на дві основні категорії, повідомлення про те, що інцидент відбувається в да-ний момент і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому. Нижче перераховані деякі ознаки здійснюваної події:

- IDS фіксує переповнення буферу;
- повідомлення антивірусної програми;
- крах web-інтерфейсу;
- працівники виконкому повідомляють про достатньо низьку швидкість при спробі виходу в Internet;
- посадова особа виконкому, на яку відповідно до розподілу обов'язків покладені обов'язки системного адміністратора фіксує наявність файлів з підозрілими назвами;
- працівники виконкому повідомляють про наявність у своїх поштових скриньках багатьох повторюваних повідомлень;
- хост (вузол) вносить запис до журналу аудиту про зміну конфігурації;
- додаток фіксує в журнальному файлі множинні невдалі спроби авторизації;
- посадова особа виконкому, на яку відповідно до розподілу обов'язків покладені обов'язки адміністратора мережі фіксує різке збільшення мережевого трафіку.

Прикладами подій, які можуть стати джерелами інформаційної безпеки можуть бути:

- журнальні файли сервера, які фіксують сканування портів;
- оголошення про появу нового виду експлойту;
- відкрита заява комп'ютерних злочинців про наміри організації та інше.

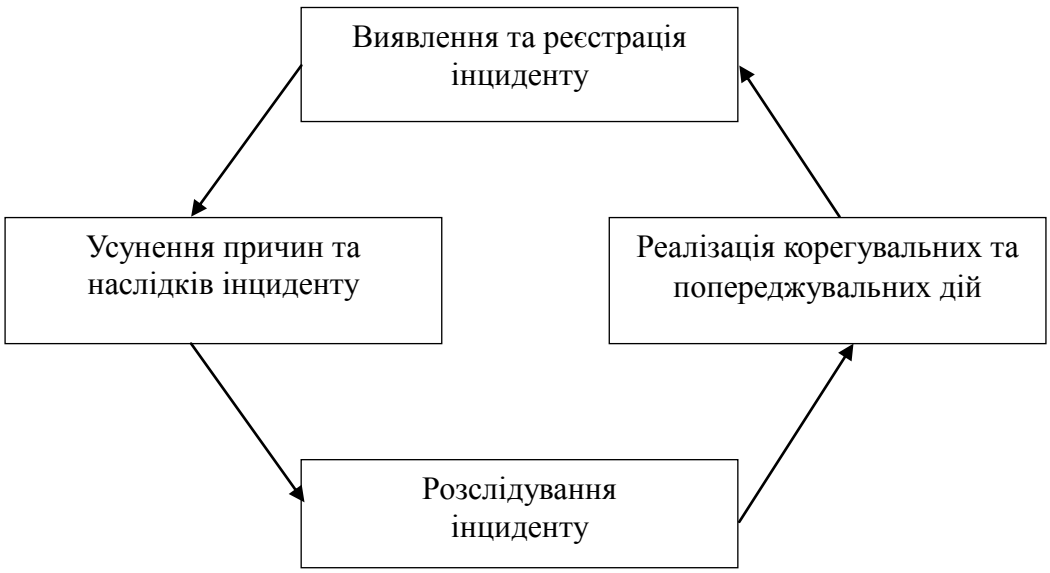
4.2. Виявлення і реєстрація інциденту

Інцидент інформаційної безпеки може помітити працівник виконкому або посадова особа виконкому відповідальна за функціонування системи управління інформаційною безпекою. Для працівників виконкому районної в місті ради має розроблятися інструкція, яка буде містити опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попередити про те, що виконувати які-небудь дії самостійно заборонено). Такий звіт повинен містити докладний опис інциденту, перелік співробітників, залучених до інциденту, прізвище співробітника, що зафіксував інцидент та дату виникнення і реєстрації інциденту. Також повинні бути вказані дії для фахівця, до обов'язків якого входить реєстрація інциденту. Співробітник, що знайшов інцидент, зв'язується із співробітником, відповідальним за реєстрацію інциденту для виконання подальших дій. Також співробітники можуть звернутися напряму до фахівця, який може усунути наслідки й причини інциденту (наприклад, до по-

садової особи виконкому відповідальної за функціонування системи управління інформаційною безпекою, або до посадової особи виконкому на яку відповідно до розподілу обов'язків покладені обов'язки системного адміністратора).

4.3. Управління інцидентами інформаційної безпеки

Процедура управління інцидентами інформаційної безпеки скла-дається із декількох етапів.



Основною метою забезпечення інформаційної безпеки (ІБ) виконкому районної в місті ради є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів ІБ.

5. Ролі та відповідальність

Обов'язки щодо своєчасного реагування та розгляду інцидентів інформаційної безпеки покладаються на групу реагування на інциденти інформаційної безпеки (далі - ГРІІБ), яка створюється розпорядженням голови районної в місті ради.

Основні цілі ГРІІБ:

- забезпечення організації кваліфікованим персоналом для обліку, реагування та аналізу інцидентів;
- забезпечення необхідної координації і управління процесом реагування на інциденти;
- забезпечення належного рівня інформування керівництва і зацікавлених осіб;
- забезпечення максимального зниження наслідків інцидентів, як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи рекомендується включити представників наступних структурних підрозділів виконкому районної в місті ради:

- посадову особу виконкому відповідальну за функціонування системи управління інформаційною безпекою (забезпечення координаційної, адміністративної, експертної і технологічної діяльності);
- працівника, на якого покладено обов'язки служби інформаційних технологій (забезпечення експертної і технологічної діяльності);
- працівника відділу з питань кадрової роботи (забезпечення адміністративної і процедурної діяльності);
- працівника відділу з правових питань (забезпечення експертної і нормативно-правої діяльності);
- працівника відділу, в якому трапився інцидент (залучаються на тимчасовій основі для підтримки забезпечення адміністративної, експертної і технологічної діяльності);
- зовнішніх експертів (забезпечення консультативної, експертної і технологічної діяльності).

6. Документація

Документація повинна містити такі елементи:

- шкалу небезпеки для класифікації інцидентів ІБ (така шкала може складатися, наприклад, з двох положень: "небезпечно" і "безпечно". У будь-якому випадку положення шкали засноване на фактичному або передбачуваному збитку для виконкому районної в місті ради);
- форми звітів про події та інциденти ІБ, відповідні задокументовані методики та дії пов'язані з коректними процедурами використання даних і системи, сервісів і (або) мережевого резервування, планами безперервності управління;
- операційні процедури для ГРІІБ з документованими обов'язками та розподілом функцій серед призначених відповідальних осіб для ведення різних видів діяльності, наприклад таких як:
- відключення ураженої системи, сервісу і (або) мережі, при визначених обставинах за погодженням з відповідним керівництвом і відповідно до попередньої угоди;
- залишення ураженої системи, сервісу і (або) мережі, що знаходиться в працюючому стані;
- ведення моніторингу потоку даних, що виходять, входять або знаходяться в межах ураженої системи, сервісу і (або) мережі;
- активація нормальних дій і процедур планування неперервності управління та резервування згідно політики безпеки системи, сервісу та (або) мережі;
- ведення моніторингу та підтримка безпеки зберігання свідоцтв в електронному вигляді на випадок їх запитання для судового переслідування або внутрішнього дисциплінарного стягнення всередині виконавчого комітету районної в місті ради;
- передача подробиць про інцидент ІБ ГРІІБ, керівництву та стороннім особам або організаціям.

Якщо можливо, документи мають бути в електронній формі (наприклад,

на безпечній веб-сторінці) з посиланням на базу даних, що зберігає електронну інформацію про події/інциденти ІБ. Форма заповнюється особою, що робить повідомлення (тобто необов'язково членом ГРІІБ). Форма звіту про інциденти використовується персоналом менеджменту інцидентів ІБ, заповнюється первісною інформацією про подію ІБ, містить поточні записи оцінки інциденту та інші до повного вирішення інциденту. На кожній стадії в базу даних подій / інцидентів ІБ включаються поновлення. Запис, зроблений у базі даних, що містить "заповнену" форму або відомості про події/інциденти ІБ, потім використовується при розслідуванні інциденту.

7. Коригувальні та превентивні дії

Після усунення наслідків інциденту і відновлення нормального функціонування управлінських процесів виконкому районної в місті ради, виконуються дії щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких дій проводиться аналіз ризиків, в рамках якого визначається доцільність коригувальних і превентивних дій. В деяких випадках, якщо наслідки інциденту незначні в порівнянні з коригувальними і превентивними діями, тоді доцільно не виконувати подальших кроків після усунення наслідків інциденту.

Керуючий справами виконкому ***О.Гижко***

Додаток 1
до Методики виявлення
та реєстрації інцидентів
інформаційної безпеки

Реєстр інцидентів
виконавчого комітету Довгинцівської районної в місті ради

Перелік інцидентів ІБ може включати, але не обмежується, наступне:

- зникнення інтернет-зв'язку;
- порушення строків виконання робіт підрядними організаціями;
- припинення дії електронного ключа;
- пожежа;
- викрадення документів;
- викрадення обладнання;
- втрата ключів від приміщень;
- викрадення ключів від приміщень;
- збої у системі живлення;
- відключення подачі електроенергії;
- спроба ураження;
- ураження вірусами;
- відсутність ліцензій на продукт;
- витік інформації через ПЗ;
- витік інформації через персонал;
- непрацездатність ПЗ електронного документообігу;
- непрацездатність обладнання, систем (апаратної частини);
- пошкодження документів внаслідок невідповідних кліматичних умов (вологості, освітлення);
- викрадення даних із ПК;
- не зроблене резервування даних;
- порушення цілісності ПЗ або ПК;
- несанкціонований доступ до даних,
- несанкціоноване внесення змін до даних;
- збій у системі (-ах) (через неправильне поводження з нею тощо);
- відкриття доступу до секретних даних;
- несанкціоноване обмеження доступу до інформації;
- втрата документів під час переміщення з підрозділу до підрозділу;
- вихід із строю обладнання через природні явища;
- прослуховування телефонних розмов;
- збій у роботі засобів зв'язку;
- неспроможність зберегти дані (через переповнення дискового простору тощо);
- несанкціонований фізичний доступ до інформації;
- перехоплення факсимільних повідомлень.

Додаток 2
до Методики виявлення
та реєстрації інцидентів
інформаційної безпеки

Інструкція
щодо форми звіту про події та інциденти ІБ
та рекомендації по заповненню

Призначенням форм звіту про події та інциденти ІБ - є забезпечення інформації про подію ІБ, а потім, якщо вона визначена як інцидент, то і про інцидент ІБ для певних осіб. Якщо працівник виконкому підозрює, що подія ІБ розвивається або вже відбулася, особливо таке, яке може завдати істотних втрат або шкоди власності або репутації виконкому районної в місті ради, то він повинен негайно заповнити та передати форму звіту про подію ІБ (див. першу частину додатка 1 до інструкції) посадовій особі виконкому відповідальної за функціонування системи управління інформаційною безпекою або безпосередньо-му керівнику.

Представлена інформація використовується для початку відповідного процесу оцінки, яка визначає, чи повинна ця подія бути категорована як інцидент ІБ чи ні, і в разі позитивної відповіді будуть прийняті необхідні коригувальні заходи для запобігання або обмеження втрат або шкоди. Оскільки цей процес за своїм характером є критичним по часу, то необов'язково заповнювати всі поля у формі звіту в даний момент часу. Якщо Ви є членом групи забезпечення експлуатації, переглядаються вже заповнені / частково заповнені форми, то необхідно виріши-ти, чи треба категорувати дану подію як інцидент ІБ. Якщо треба, то необхідно заповнити форму для інциденту ІБ наскільки можливо докладно направити і передати форму для події / інциденту ІБ ГРІІБ. Незалежно від того, чи буде подія ІБ категорована як інцидент чи ні, в будь-якому випадку база даних подій/інцидентів ІБ повинна бути оновлена.

Форма інциденту ІБ повинна далі оновлюватися в міру прогресу в дослідженні, і відповідні оновлення повинні проводитися в базі даних подій / інцидентів ІБ.

При заповненні форм виконуються наступні рекомендації:

- якщо можливо, то форми повинні заповнюватися і передаватися в електронному вигляді[1]. Якщо існують проблеми або вважається, що існують проблеми з встановленими за замовчуванням механізмами електронного оповіщення (наприклад, електронна пошта), включаючи випадки, коли система, можливо, піддається атаці, і форми звіту можуть бути прочитані неавторизованими особами, тоді повинні використовуватися альтернативні засоби зв'язку. Альтернативними засобами зв'язку можуть бути телефон або текстові повідомлення;

---

[1] Якщо можливо, то ці форми повинні бути в електронному вигляді (наприклад, на безпечній web-сторінці) з прив'язкою до електронної бази даних подій / інцидентів ІБ. У сучасному світі, заснована на паперовій документації система є занадто повільною і далеко не найефективнішою в експлуатації.

- уявляйте інформацію, засновану тільки на фактах, в якій Ви впевнені, нічого не придумуйте для того, щоб заповнити всі поля. Де доречно включити інформацію, яку Ви не можете підтвердити, чітко вкажіть, що це непідтверджена інформація і чому Ви вважаєте, що вона вірна;
- Ви повинні докладно вказати, як можна з Вами зв'язатися. Дуже скоро або через деякий час може виникнути необхідність контакту з Вами для подальшої інформації, що стосується Вашого звіту.

Якщо пізніше працівником виконкому буде виявлено, що деяка представлена інформація неточна, неповна або помилкова, то він повинен внести поправки в звіт і надати його повторно.

Звіт про подію ІБ

Дата події
Номер події (назначається керівником ГРІБ):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про особу, що повідомляє:
Прізвище
_____
Адреса
_____
Організація
_____
Телефон
_____
Електронна пошта
_____

Опис події ІБ

Опис події:
· Що сталося
_____
· Як сталося
_____
· Чому відбулося
_____
· Уражені компоненти
_____
· Негативний вплив на службову діяльність
_____
· Будь-які ідентифіковані уразливості
_____

Деталі події ІБ
Дата і час виникнення події

_____

Дата і час виявлення події

_____

Дата і час повідомлення про подію

_____

Чи закінчилася подія? (Зазначити квадрат) [так] [ні]

Якщо «так», то уточнити, як довго тривала подія в днях / годинах / хвилинах.

Звіт про інцидент ІБ

Дата інциденту
Номер інциденту (призначаються керівником ГРІБ і прив'язуються до номера (-ам) відповідних подій):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про співробітника групи забезпечення експлуатації:
Прізвище _____
Адреса _____
Телефон _____
Електронна пошта _____

Інформація про співробітника ГРІБ:
Прізвище _____
Адреса _____
Телефон _____
Електронна пошта _____

Опис інциденту ІБ

Подальший опис інциденту:
· Що сталося _____
· Як сталося _____
· Чому відбулося _____
· Уражені компоненти _____
· Негативний вплив на службову діяльність _____
· Будь-які ідентифіковані уразливості _____

Деталі інциденту ІБ:
Дата і час виникнення інциденту _____
Дата і час виявлення інциденту _____
Дата і час повідомлення про інцидент _____

Закінчився інцидент? (Зазначити квадрат) | так | | ні |
Якщо «так», то уточнити, як довго тривав інцидент в днях / годинах / хвилинах.
Якщо «ні», то уточнити, як довго він уже триває

Тип інциденту ІБ (Відмітити один квадрат, потім заповнити відповідні поля нижче):
Дійсний _____
Спроба _____
Підозра _____

Навмисна (вказати типи загрози) (один з):
Розкрадання (TH) _____
Хакерство / Логічне проникнення (HA) _____
Шахрайство (FR) _____
Неправильне використання ресурсів (MI) _____
Саботаж / фізичний збиток (SA)
Інший збиток (OD)
Шкідлива програма (MC)
Визначити:

Випадкова (вказати типи загрози) (Один з):
Відмова апаратури (HF)
Інші природні події (NE)
Відмова ПО (SF)
Визначити:

Відмова зв'язку (CF)
Втрата істотних сервісів (LE)
Пожежа (HE)
Недостатнє кадрове забезпечення (SS)
Повінь (FL)
Інші випадки (OA)
Визначити:

Помилка (вказати типи загрози) (Один з):
Операційна помилка (OE)
Помилка користувача (UE)
Помилка апаратної підтримки (HE)
Помилка конструкції (DE)
Помилка підтримки ПЗ (SE)
Інші випадки (включаючи справжні омани) (OA)
Визначити:
Невідомо

(Якщо ще не встановлений тип інциденту (навмисний, випадковий, по-милка), то слід зазначити квадрат «невідомо» і, по можливості, вказати тип загрози, використовуючи скорочення, наведені вище)
Визначити:

Уражені активи
Уражені активи (якщо є)
(Дати опису активів, уражених інцидентом, або пов'язаних з ним включаючи серійні, ліцензійні номери та номери версій, по можливості)

Інформація / Дані _____
Апаратура _____
Програмне забезпечення _____
Засоби зв'язку _____
Документація _____
Негативний вплив / вплив інциденту на службову діяльність
Відзначити відповідні квадрати для зазначених нижче порушень, потім в колонці «значимість» вказати рівень негативного впливу за шкалою 1¸ 10, використовуючи скорочення (покажчики категорій): (FD) – фінансові втрати / руйнування бізнес-операцій, (CE) - комерційні і економічні інтереси, (PI) - інформація, що містить персональні дані, (LR) – правові та нормативні зобов'язання (це необхідно звірити з англійським оригіналом), (MO) - менеджмент і службова діяльність, (LG) - втрата престижу. Запишіть кодові букви в колонці «вказівники», а якщо відомі дійсні вартості, то вказати їх у колонці «вартість»

Значимість	Вказівники	Вартість
Порушення конфіденційності (тобто, несанкціоноване розкриття):		
Порушення цілісності (тобто, несанкціонована модифікація):		
Порушення доступності (тобто, недоступність):		
Порушення неспростовності		
Знищення		

Повні вартості відновлення після інциденту

Значимість	Покажчики	Вартість
(Де можливо, необхідно вказати загальні витрати на відновлення після інциденту в цілому по шкалі 1¸ 10 для «значущості» і в грошах для «вартості»)		

Вирішення інциденту

Дата початку розслідування інциденту
_____
Прізвище особи (осіб), що проводив (їх) розслідування інциденту
_____
Дата закінчення інциденту _____
Дата закінчення дії
_____
Дата завершення розслідування інциденту
_____
Посилання та місце зберігання звіту про розслідування
_____

Причетні особи (один з)

Особа (PE)
Легально заснована організація / установа (OI)
Організована група (GR)
Випадковість (AC)
Немає винного (NP)
Наприклад, природні фактори,
Відмова обладнання, помилка людини

Опис порушника
Дійсна або передбачувана мотивація (один з)

Кримінальна / фінансова вигода (CG)
Розвага / хакерство (PH)
Політика / тероризм (PT)
Реванш (RE)
Інші мотиви (OM)
Визначити:

Дії, вжиті для вирішення інциденту
(Наприклад, «ніяких дій», «підручними засобами», «внутрішнє розслідування», «зовнішнє розслідування із залученням ...»)

Дії, заплановані для дозволу інциденту
(Наприклад, див. вище)

Інші дії
(Наприклад, як і раніше потрібне проведення розслідування для іншого персоналу)

Висновок

(Відзначити один з квадратів, чи є інцидент значним чи ні і додати в короткий пояснення для обґрунтування цього висновку)
Значний
Незначний
(Вкажіть будь-які інші висновки) _____

Ознайомлені особи / суб'єкти

(Ця частина звіту заповнюється відповідною особою, на яку покладено обов'язки в області ІБ і яка формулює необхідні дії. Зазвичай цією особою є посадова особа виконкому відповідальна за функціонування системи керування інформаційною безпекою (керівник ІБ).

Керівник ІБ
Керівник ГРІІБ
Місцевий керівник (уточнити, якого підрозділу)
Керівник інформаційних систем
Автор звіту
Керівник автора звіту
Представник РВ МВС(при необхідності)
Інша особа

Визначити:

Залучені особи

Ініціатор
Підпис _____
Прізвище _____
Посада _____
Дата _____

Аналітик
Підпис _____
Прізвище _____
Посада _____
Дата _____